EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CERTIFIKÁCIA KYBERNETICKEJ BEZPEČNOSTI

EUCC, kandidátska schéma certifikácie kybernetickej bezpečnosti, ktorá má slúžiť ako nástupca existujúcej schémy SOG-IS

HISTÓRIA DOKUMENTOV

Dátum	Verzia	Úprava	Poznámky autora
13/12/2019	0.1	Vytvorenie	
28/02/2020	0.2	Integrácia výsledkov prvej pracovnej skupiny AHWG	Poznámka redakcie: súčasná verzia dokumentu sa zaoberá dvoma typmi kapitol: - kapitoly, v ktorých TG (alebo podskupina ECCG) poskytla dostatočné množstvo informácií, aby ENISA mohla navrhnúť text - kapitoly, ktoré TG (alebo podskupina ECCG) musí ešte dodať: v takom prípade sú očakávané témy, ktoré sa majú riešiť, uvedené *kurzívou* vo forme otázok (ďalšie témy vyplývajúce z TG budú zahrnuté)
24/04/2020	0.3	Začlenenie nových výstupov AHWG z 3 zasadnutí a 4 zasadnutých a prvých povinných dokumentov.	Pripravené pre zasadnutie 5th AHWG
18/05/2020	0.4	Začlenenie nových výstupov AHWG zo zasadnutia 5th a priamo z výstupov spravodajcov TG	Pripravené pre zasadnutie 6th AHWG
25/05/2020	0.5	Začlenenie nových výstupov AHWG zo zasadnutia 6th a priamo z výstupov spravodajcov TG	Pripravené pre 2nd dávku preskúmania "užšej skupiny"
02/06/2020	0.6	Integrácia výstupov AHWG zo zasadnutia 6th a priamo z výstupov spravodajcov TG	Zvyšné kapitoly zahrnuté do 3. skupiny "užšieho skupinového" preskúmania
09/06/2020	0.7	Začlenenie pripomienok z preskúmania "užšej skupiny"	Pripravené na preskúmanie pracovnou skupinou AHWG
23/06/2020	0.8	Zapracovanie pripomienok z preskúmania AHWG a príloh	Pripravené na prezentáciu agentúre ENISA MT
01/07/2020	1.0	Zapracovanie posledných pripomienok AHWG	Vypracované pre externú konzultáciu v súlade s článkom 49.3 CSA
07/09/2020	1.1	Aktualizácia na základe výsledkov externej konzultácie a pripomienok ECCG	Pripravené na predloženie stanoviska ECCG
18/05/2021	1.1.1	Kozmetické zmeny a aktualizácia prílohy 10 na základe jej nedávneho vývoja v rámci SOG-IS	Verzia doručená EK ako konsolidovaný kandidátsky program

O AGENTÚRE ENISA

Poslaním Agentúry Európskej únie pre kybernetickú bezpečnosť (ENISA) je dosiahnuť vysokú spoločnú úroveň kybernetickej bezpečnosti v celej Únii aktívnou podporou členských štátov, inštitúcií, orgánov, úradov a agentúr Únie pri zlepšovaní kybernetickej bezpečnosti. Prispievame k tvorbe a implementácii politík, podporujeme budovanie kapacít a pripravenosť, uľahčujeme operačnú spoluprácu na úrovni Únie, zvyšujeme dôveryhodnosť produktov, služieb a procesov IKT zavádzaním systémov certifikácie kybernetickej bezpečnosti, umožňujeme výmenu poznatkov, výskum, inovácie a budovanie povedomia a zároveň rozvíjame cezhraničné komunity. Naším cieľom je posilniť dôveru v prepojené hospodárstvo, zvýšiť odolnosť infraštruktúry a služieb Únie a udržať našu spoločnosť v kybernetickej bezpečnosti. Viac informácií o agentúre ENISA a jej práci nájdete na stránke www.enisa.europa.eu.

KONTAKT

Ak chcete kontaktovať autorov, pošlite e-mail na adresu certification@enisa.europa.eu. Otázky pre médiá zasielajte na e-mailovú adresu press@enisa.europa.eu.

AUTOR

Agentúra Európskej únie pre kybernetickú bezpečnosť (ENISA)

POĎAKOVANIE

Agentúra ENISA ďakuje členom pracovnej skupiny AHWG https://www.enisa.europa.eu/topics/standards/adhoc_wg_calls/ahWG01/ahwg01_members, ako aj zástupcom akreditačných orgánov, členských štátov a Európskej komisie, ktorí od novembra 2019 podporujú agentúru ENISA pri vytváraní tohto kandidátskeho systému.

Agentúra ENISA ďakuje komunite SOG-IS MRA https://www.sogis.eu/uk/status_participant_en.html za možnosť opätovného použitia dostupnej dokumentácie do schémy EUCC.

PRÁVNE UPOZORNENIE

Tento návrh dokumentu predstavuje prípravný právny text, ktorý sa má predložiť na konzultáciu podľa článku 49 zákona o kybernetickej bezpečnosti (nariadenie 2019/881). Predstavuje predbežné názory agentúry ENISA a v žiadnom prípade sa nesmie považovať za vyjadrenie oficiálneho stanoviska agentúry ENISA alebo Komisie. Nepredstavuje právny akt agentúry ENISA alebo Komisie, ani orgánov agentúry ENISA alebo Komisie. Nemožno z neho odvodzovať žiadne práva.

Tento návrh dokumentu nepredstavuje oficiálnu publikáciu agentúry ENISA a nemusí nevyhnutne predstavovať súčasný stav techniky; ide o pracovnú verziu kandidátskeho systému certifikácie kybernetickej bezpečnosti EÚ, ktorá sa šíri výlučne na účely konzultácie podľa článku 49 ods. 3 zákona o kybernetickej bezpečnosti a nesmie sa používať na žiadne iné účely. Agentúra ENISA ju môže po konzultácii zmeniť a doplniť.

Zdroje tretích strán sa majú citovať podľa potreby, ale vzhľadom na to, že ide o pracovnú verziu, môže sa stať, že drobné nezrovnalosti budú predmetom opravy. Agentúra ENISA nezodpovedá za obsah externých zdrojov vrátane externých webových stránok, na ktoré sa v tomto dokumente odkazuje. Vývojové diagramy, modely, matice a štatistiky sa tiež považujú za návrh. Nemožno z nich vyvodzovať žiadne práva.

UPOZORNENIE NA AUTORSKÉ PRÁVA

OBSAH

ZHRNUTIE

Na základe žiadosti Európskej komisie v súlade s článkom 48 ods. 2 Aktu o kybernetickej bezpečnosti[1] (ďalej len "CSA", ako je uvedené v slovníku) agentúra ENISA zriadila ad hoc pracovnú skupinu (AHWG) na podporu prípravy kandidátskej schémy certifikácie kybernetickej bezpečnosti EÚ, ktorá by slúžila ako nástupca existujúcich schém fungujúcich v rámci dohody o vzájomnom uznávaní bezpečnosti informačných systémov skupiny starších úradníkov (SOG-IS MRA).

Na základe výsledkov tejto pracovnej skupiny AHWG, ktorá začala svoju činnosť 27 novembra 2019 a ktorú tvorí dvadsať (20) vybraných členov zastupujúcich priemysel (napr. vývojári, hodnotitelia), ako aj približne dvanásť (12) členov z akreditačných orgánov a členských štátov EÚ, pravidelných diskusií v rámci ECCG a po internom preskúmaní agentúra ENISA skonsolidovala nasledujúcu kandidátsku schému.

Schéma EUCC (Európska schéma certifikácie kybernetickej bezpečnosti založená na spoločných kritériách) sa zaoberá certifikáciou kybernetickej bezpečnosti produktov IKT na základe spoločných kritérií, spoločnej metodiky hodnotenia bezpečnosti informačných technológií a príslušných noriem ISO/IEC 15408 a ISO/IEC 18045.

Spoločné kritériá sa v posledných dvoch desaťročiach v Európe osvedčili najmä pri certifikácii integrovaných obvodov a smart kariet, čím prispeli k zvýšeniu úrovne bezpečnosti zariadení na elektronický podpis, identifikačných prostriedkov, ako sú pasy, bankové karty a tachografy pre nákladné vozidlá.

Okrem toho sa intenzívne používajú na certifikáciu kybernetickej bezpečnosti softvérových produktov IKT.

Táto schéma zlepší podmienky vnútorného trhu Európskej únie pre produkty IKT a v dôsledku toho bude mať pozitívny vplyv aj na služby IKT a procesy IKT, ktoré sa na takéto produkty spoliehajú.

Kandidátska schéma EUCC sa zaoberá potrebnými požiadavkami súvisiacimi s definíciou schémy, ako je vymedzená v článku 49 ods. 1 CSA, pričom predpisuje, že musia byť splnené požiadavky článkov 51, 52 a 54 CSA.

Okrem toho obsahuje základné informácie súvisiace s požiadavkami, ktoré poskytujú objasnenie požiadaviek a umožňujú ilustrovať konkrétnu voľbu alebo odôvodniť konkrétny prípad, ako to očakáva CSA.

Na záver sa na základe skúseností členov AHWG venuje niektorým odporúčaniam pre ECCG na prijatie a udržanie novej schémy.

Táto verzia schémy bola aktualizovaná na základe pripomienok získaných v rámci verejnej konzultácie a od ECCG. Významné zmeny sa týkajú:

- doplnenie a objasnenie definícií;
- systematická spolupráca s ECCG pri vypracúvaní sprievodných dokumentov na podporu schémy;
- objasnenie činností súvisiacich s udržiavaním certifikácie;
- objasnenie lehôt súvisiacich s riešením nezhôd, nesúladov a zraniteľností;
- úprava stavu nového procesu správy záplat, ktorý je teraz v prílohe a na skúšobné používanie;
- úprava loga spojeného s certifikátmi, ktorá umožní vytvoriť ďalšie špecifické logo pre schému a uvádzať okrem úrovne záruky CSA aj dosiahnutú úroveň hodnotenia;
- objasnenie požiadaviek na vzájomné posudzovanie a zjednodušenie súvisiacej prílohy;
- aktualizácia príloh 7 a 9 na základe ich nedávneho vývoja v rámci SOG-IS a doplnenie jednej prílohy týkajúcej sa anonymizácie ST

[1]NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie) o kybernetickej bezpečnosti) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (zákon o kybernetickej bezpečnosti).

SLOVNÍK

Na účely tejto schémy sa uplatňujú nasledujúce definície, ktoré dopĺňajú a podporujú definície stanovené v článku 2 CSA a definície uvedené v hlavnom dokumente podporujúcom túto schému, Spoločných kritériách hodnotenia bezpečnosti informačných technológií.

Termín alebo pojem	Skratka	Definícia
Autorizácia		Potvrdenie NCCA, že CAB spĺňa osobitné alebo dodatočné požiadavky týkajúce sa jeho odbornej kompetentnosti na hodnotenie definované v článku 54 ods. 1 písm. f).
Skupina záruk "Analýza zraniteľnosti"	AVA_VAN	Skupina záruk týkajúca sa analýzy zraniteľnosti definovaná v časti 3 CC. Analýza zraniteľnosti je posúdenie s cieľom určiť, či potenciálne zraniteľnosti identifikované počas hodnotenia vývoja a predpokladanej prevádzky TOE alebo inými metódami (napr. hypotézami chýb alebo kvantitatívnou či štatistickou analýzou bezpečnostného správania základných bezpečnostných mechanizmov) by mohli útočníkom umožniť porušenie SFR. Analýza zraniteľnosti sa zaoberá hrozbami, že útočník bude schopný objaviť chyby, ktoré umožnia neoprávnený prístup k údajom a funkciám, umožnia zasahovať do TSF alebo ho meniť, alebo zasahovať do autorizovaných možností iných používateľov. Pre túto schému úroveň AVA_VAN určuje úroveň hodnotenia podľa článku 52.8.
Tím pre reakciu na počítačové núdzové situácie	CERT	Historický termín pre skupinu expertov, ktorá sa zaoberá incidentmi v oblasti počítačovej bezpečnosti.
Udržiavanie certifikácie		Proces analýzy, či súbor jednej alebo viacerých zmien ovplyvňuje bezpečnostnú záruku certifikovaného produktu IKT, a následné rozhodnutie na základe zhromaždených dôkazov.
Certifikačný orgán	CB	Orgán posudzovania zhody tretej strany prevádzkujúci certifikačné schémy [ISO/IEC 17065]. POZNÁMKA1: CB je zodpovedný za certifikačné činnosti súvisiace s vydávaním certifikátov; činnosti súvisiace s hodnotením a testovaním vykonáva ITSEF (pozri súvisiacu definíciu). POZNÁMKA2: Podľa ustanovení čl. 58 ods. 4 môže NCCA konať ako CB. Pojem CB sa potom vzťahuje tak na súkromný orgán spojený s CB, ako aj na NCCA, ktorý koná ako CB. POZNÁMKA3: Vydavateľ certifikátov sa pre túto schému považuje za ekvivalent CB.
Spoločné kritériá	CC	Spoločné kritériá pre hodnotenie bezpečnosti informačných technológií, ktoré pozostávajú z: Časť 1: Úvod a všeobecný model Časť 2: Komponenty bezpečnostných funkcionalít Časť 3: Komponenty bezpečnostných záruk POZNÁMKA: CC označujú Spoločné kritériá pre hodnotenie bezpečnosti informačných technológií podľa ich platnej verzie ISO/IEC 15408 alebo podľa ich platnej verzie uverejnenej na https://www.commoncriteriaportal.org/cc/.
Spoločná metodika hodnotenia	CEM	Spoločná metodika hodnotenia bezpečnosti informačných technológií. POZNÁMKA: CEM označuje Spoločnú metodiku hodnotenia bezpečnosti informačných technológií podľa jej platnej verzie ISO/IEC 18045 alebo podľa jej platnej verzie uverejnenej na https://www.commoncriteriaportal.org/cc/.

Termín alebo pojem	Skratka	Definícia
Spoločné zraniteľnosti a vystavenia	CVE	Zoznam záznamov, z ktorých každý obsahuje identifikačné číslo, opis a aspoň jeden verejný odkaz, pre verejne známe zraniteľnosti kybernetickej bezpečnosti.
Hodnotenie/certifikácia zloženého produktu		Postupy hodnotenia a certifikácie zavedené s cieľom umožniť, aby sa pri hodnotení produktu (napr. smart karty) ako kombinácie viacerých častí (napr. hardvérovej časti integrovaného obvodu (IC) a softvérovej časti pozostávajúcej z platformy a aplikácie), ktoré často vyvíjajú rôzne subjekty so špecifickými cieľmi, priamo zohľadnili výsledky hodnotenia jednej časti (napr. certifikácie IC) pri hodnotení ostatných častí.
Orgán posudzovania zhody	CAB	Orgán posudzovania zhody podľa článku 2 bodu 13 nariadenia (ES) č. 765/2008. POZNÁMKA: CAB označuje certifikačný orgán (CB) aj interné alebo externé skúšobné laboratórium (ITSEF). Ak sú v tejto schéme definované požiadavky na CAB, vzťahujú sa na oba. Ak sa vzťahujú len na CB alebo ITSEF, potom sa používajú termíny CB alebo ITSEF.
Akt o kybernetickej bezpečnosti	CSA	Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií, ktorým sa zrušuje nariadenie (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti).
Hodnotenie		Kombinácia funkcií výberu a určovania činností posudzovania zhody [ISO/IEC 17065]. POZNÁMKA1: Úlohy hodnotenia môžu zahŕňať činnosti, ako je preskúmanie návrhu a dokumentácie, odber vzoriek, skúšanie, inšpekcia a audit [ISO/IEC 17065]. POZNÁMKA2: V kontexte schémy možno hodnotenie definovať ako posúdenie produktu IKT alebo ochranného profilu na základe kritérií hodnotenia bezpečnosti a metód hodnotenia bezpečnosti s cieľom určiť, či sú uvedené výroky opodstatnené [CC časť 1]. POZNÁMKA3: Činnosti hodnotenia vykonáva ITSEF
Hodnotenie úrovne záruky	EAL	Vhodne vytvorený balík požiadaviek bezpečnostných záruk [CC časť 3]. POZNÁMKA: EAL sa vzťahuje na úrovne záruky definované v CSA, ako je opísané v časti 4.
Technická správa hodnotenia	ETR	Správa vypracovaná ITSEF, ktorá slúži ako hlavný podklad pre správu o certifikácii. POZNÁMKA: Cieľom ETR je prezentovať všetky verdikty, ich odôvodnenia a všetky zistenia vyplývajúce z práce vykonanej počas hodnotenia vrátane chýb zistených počas vývoja produktu IKT alebo ochranného profilu a všetkých zraniteľností, ktoré sa dajú zneužiť a ktoré sa zistili počas hodnotenia. ETR môže obsahovať chránené informácie, ak je to potrebné na zdôvodnenie výsledkov hodnotenia.
Správa z analýzy vplyvu	IAR	Dokument zaznamenávajúci analýzu vplyvu zmien certifikovaného produktu IKT.
Správa o udržiavaní		Verejne dostupný dokument, ktorý opisuje výsledky procesu udržiavania aplikovaného na certifikovaný produkt IKT. POZNÁMKA: Správa o udržiavaní odôvodňuje rozhodnutie týkajúce sa súvisiaceho certifikátu.
Výrobca alebo poskytovateľ certifikovaného produktu IKT		Výrobca alebo poskytovateľ produktu IKT zodpovedá vývojárovi v terminológii spoločných kritérií, pokiaľ ide o poskytovanie časti dôkazov podľa požiadaviek metodiky (CC časť 3).
Dohľad nad trhom		Činnosti vykonávané a opatrenia prijímané orgánmi verejnej moci s cieľom zabezpečiť, aby produkty spĺňali požiadavky stanovené v príslušných harmonizačných právnych predpisoch Spoločenstva a neohrozovali zdravie, bezpečnosť alebo akýkoľvek iný aspekt ochrany verejného záujmu (NARIADENIE (ES) č. 765/2008).

Termín alebo pojem	Skratka	Definícia
Národná autorita pre certifikáciu kybernetickej bezpečnosti	NCCA	Národná autorita pre certifikáciu kybernetickej bezpečnosti vymedzená v článku 58.7 CSA. Ak to nie je výslovne uvedené, NCCA sa má chápať ako orgán dozoru, a nie ako CAB, ktorý vydáva certifikáty na úrovni "vysoká", ako sa uvádza v článku 56.6 CSA.
Nesúlad / nezhoda		Nesúlad: nesplnenie požiadavky súvisiacej s ustanoveniami schémy alebo certifikátu. Nezhoda: nesplnenie požiadavky týkajúcej sa technických noriem alebo bezpečnostných cieľov definovaných v článku 51 CSA.
Ochranný profil	PP	Implementácia nezávislého súboru bezpečnostných požiadaviek pre kategóriu produktov IKT, ktoré spĺňajú špecifické potreby spotrebiteľov
preskúmavanie/preskúmanie		Overenie vhodnosti, primeranosti a efektívnosti hodnotenia a výsledkov tejto činnosti, pokiaľ ide o splnenie špecifikovaných požiadaviek predmetom posudzovania zhody [prevzaté z normy ISO/IEC 17000].
Udržiavanie schémy		Proces aktualizácie certifikačnej schémy
Požiadavky bezpečnostných záruk	SAR	Činnosti súvisiace s posudzovaním bezpečnosti produktu IKT, ktorý sa má certifikovať. Katalóg SAR je definovaný v časti 3 CC.
Požiadavky bezpečnostných funkcionalít	SFR	Bezpečnostné ciele produktu IKT, ktorý sa má certifikovať. Katalóg SFR je definovaný v časti 2 CC.
Bezpečnostný zámer	ST	v závislosti od implementácie, vyhlásenie o bezpečnostných potrebách pre špecifický identifikovaný TOE [CC časť 1].
Skupina starších úradníkov pre bezpečnosť informačných systémov	SOG-IS	Výbor s dlhodobým mandátom poskytovať Komisii poradenstvo v oblasti bezpečnosti informačných systémov, zriadený rozhodnutím Rady EÚ z 31. marca 1992 (92/242/EHS) v oblasti bezpečnosti informačných systémov a následným odporúčaním Rady zo 7. apríla 1995 (1995/144/ES) o spoločných kritériách hodnotenia bezpečnosti informačných technológií.
Dohoda o vzájomnom uznávaní SOG-IS	SOG-IS MRA	Dohoda o vzájomnom uznávaní certifikátov hodnotenia bezpečnosti informačných technológií (platná verzia 3.0, január 2010).
subdodávka (úloh hodnotenia)		Zadanie úlohy hodnotenia CB externému skúšobnému laboratóriu podľa bodu 9 prílohy k nariadeniu (EÚ) 2019/881.
Objekt hodnotenia	TOE	Súbor softvéru, firmvéru a/alebo hardvéru, ku ktorému je prípadne pripojené usmernenie [CC časť 1], ktorý je predmetom hodnotenia v rámci produktu IKT. TOE môže byť podmnožinou produktu IKT.
Technická doména		Spoločný technický rámec definovaný pre vyššie úrovne záruky certifikácie zodpovedajúce AVA_VAN.4 a 5 a spojené s konkrétnou technológiou. Umožňuje okrem iného definovať spoločné chápanie potenciálu útoku a súvisiacich metód útoku pre danú technológiu. Jeho aplikácia sa týka aj schopností CAB vykonávať takéto hodnotenia.

Termín alebo pojem	Skratka	Definícia
Skúšobné laboratórium / hodnotiace zariadenie	ITSEF	Orgán posudzovania zhody tretej strany, ktorý vykonáva jednu alebo viacero z týchto činností: - kalibrácia - testovanie - odber vzoriek spojený s následnou kalibráciou alebo testovaním [prevzaté z ISO/IEC 17025]. POZNÁMKA1: V kontexte tejto schémy skúšobné laboratórium vykonáva funkcie určovania a výberu ako súčasť činností posudzovania zhody. POZNÁMKA2: ITSEF (IT Security evaluation facility) je ekvivalentom testovacieho laboratória/hodnotiaceho zariadenia. Môže to byť a) interný subjekt CAB alebo b) externý subjekt, ktorému CAB konajúci ako CB zadá hodnotenie v subdodávke. Ak sú v schéme EUCC definované požiadavky na ITSEF, vzťahujú sa na interný aj externý subjekt. POZNÁMKA3: V kontexte schémy EUCC je ITSEF z hľadiska prevádzky oddelený od CB.

1. PREDMET A ROZSAH PÔSOBNOSTI

ODKAZ(-Y) NA ČLÁNOK(-KY) CSA

Článok 1.2 (Predmet a rozsah pôsobnosti): Týmto nariadením nie sú dotknuté kompetencie členských štátov týkajúce sa činností v oblasti verejnej bezpečnosti, obrany, národnej bezpečnosti a činností štátu
v oblasti trestného práva.

Článok 54 1. *Európska schéma certifikácie kybernetickej bezpečnosti obsahuje aspoň tieto prvky:*

a) predmet a rozsah certifikačnej schémy vrátane typu alebo kategórií produktov IKT, služieb IKT a procesov IKT, na ktoré sa vzťahuje.

Európska schéma certifikácie kybernetickej bezpečnosti založená na spoločných kritériách (ďalej len "schéma EUCC") umožňuje certifikáciu kybernetickej bezpečnosti produktov IKT podľa normy ISO/IEC 15408 a spoločných kritérií (CC), ako je vymedzené v kapitole 3, NORMY POUŽITÉ PRI HODNOTENÍ.
Schéma EUCC sa môže vzťahovať na akýkoľvek typ produktu IKT, ktorý je určený pre vnútorný trh Európskej únie, pričom platí, že produkt IKT, na ktorý sa vzťahuje táto schéma musí:

- obsahovať súbor významných požiadaviek bezpečnostných funkcionalít, ako je opísané v časti 2 CC;
- mať za cieľ dosiahnuť úrovne záruky "významná" alebo "vysoká" CSA.

Schéma EUCC zahŕňa posudzovanie zraniteľnosti kryptografických implementácií do bezpečnostných funkcionalít produktu IKT v súlade s požiadavkami kritérií a metodiky hodnotenia definovaných v kapitole 3, NORMY POUŽITÉ PRI HODNOTENÍ.

Uplatňujú sa potenciálne podmienky týkajúce sa dosiahnuteľných úrovní certifikácie, ako je opísané v kapitole 4, ÚROVNE ZÁRUKY.

EUCC okrem toho poskytuje možnosť pokryť ďalšie prvky, ako sa predpokladá v článku 54 CSA, za podmienok vymedzených v kapitole 24, ĎALŠIE PRVKY SCHÉMY:
- certifikáciu ochranných profilov[2];
- pravidlá ochrany informácií súvisiacich s certifikáciou kybernetickej bezpečnosti.

ZÁKLADNÉ INFORMÁCIE

Podľa časti 1 CC: *"Spoločné kritériá (CC) umožňujú porovnateľnosť výsledkov nezávislých hodnotení bezpečnosti. CC poskytuje spoločný súbor požiadaviek na bezpečnostné funkcionality IT produktov a na opatrenia bezpečnostných záruk, ktoré sa na tieto IT produkty uplatňujú počas hodnotenia bezpečnosti. Tieto IT produkty môžu byť implementované v hardvéri, firmvéri alebo softvéri."*

Aj keď by sa táto schéma teoreticky mohla použiť na certifikáciu akéhokoľvek produktu IKT, najvhodnejšia je pre tie, ktoré sa snažia dosiahnuť úroveň záruky CSA "významnú" a "vysokú". Na certifikáciu produktov IKT, ktoré sú menej náročné z hľadiska úrovní záruky, môžu byť vhodnejšie iné schémy.

V súvislosti s kryptografiou sa v časti 1 CC uvádza, že: *"Predmetom kritérií na posúdenie prirodzených vlastností kryptografických algoritmov sa CC nezaoberá. Ak by sa vyžadovalo nezávislé posúdenie matematických vlastností kryptografie, schéma hodnotenia, v rámci ktorého sa CC uplatňuje, musí takéto posúdenie zabezpečiť. "*Komunita SOG-IS vytvorila dokumentom SOGIS Agreed Cryptographic Mechanisms v1.1 prvý stavebný prvok na analýzu vhodnosti kryptografických mechanizmov.

Potrebu rozšíriť rozsah pôsobnosti schémy EUCC o certifikáciu ochranného profilu a pravidlá bezpečnosti informácií stanovila pracovná skupina AHWG na základe súčasných postupov v rámci

[2] Ochranné profily (PP) umožňujú definovať súbor bezpečnostných požiadaviek nezávislých od implementácie pre kategórie produktov IKT, ktoré spĺňajú špecifické potreby spotrebiteľov; PP sú široko využívané skupinami spotrebiteľov a záujmovými spoločenstvami, môžu sa stať normami a môžu byť zahrnuté do nariadení EÚ.

MRA SOG-IS a naliehavých potrieb.

Súvisiace podmienky a podrobnejšie základné informácie sú uvedené v kapitole 24, ĎALŠIE PRVKY SCHÉMY.

2. ÚČEL SCHÉMY

ODKAZ(-Y) NA ČLÁNOK(-KY) CSA

Článok 54 1. *Európska schéma certifikácie kybernetickej bezpečnosti obsahuje aspoň tieto prvky:*

b) jasný opis účelu schémy a toho, ako vybrané normy, metódy hodnotenia a úrovne záruky zodpovedajú potrebám zamýšľaných používateľov schémy.

Schéma EUCC môže slúžiť ako nástupca národných schém EÚ fungujúcich v rámci MRA SOG-IS, ktoré sú uvedené v kapitole 16, NÁRODNÉ ALEBO MEDZINÁRODNÉ SCHÉMY.

Môže umožniť zlepšiť podmienky vnútorného trhu a zvýšiť úroveň bezpečnosti produktov IKT týkajúcich sa bezpečnosti (napr. firewallov, šifrovacích zariadení, brán, zariadení na elektronický podpis, identifikačných prostriedkov, ako sú pasy, ...), ako aj všetkých produktov IKT, ktoré obsahujú bezpečnostnú funkcionalitu (napr. smerovače, smartfóny, bankové karty, zdravotnícke zariadenia, tachografy pre nákladné vozidlá, ...).

Tým, že ponúka dve (2) úrovne bezpečnostnej záruky, "významnú" a "vysokú", pokrýva veľkú škálu náročných bezpečnostných požiadaviek, hoci sa nevenuje základnej úrovni, ktorú môžu ponúkať schémy, ktoré sú menej náročné z hľadiska dôkazov hodnotenia a pokrývajú menej prísne bezpečnostné požiadavky.

Používateľmi schémy môžu byť:

- výrobcovia alebo poskytovatelia, ktorí chcú posúdiť kvalitu bezpečnosti svojich produktov IKT prostredníctvom certifikácie treťou stranou;
- poskytovatelia služieb IKT alebo procesov IKT, ktorí chcú pre svojich klientov využívať dôkazy o bezpečnosti certifikovaných produktov IKT;
- regulačné orgány, ktoré chcú v rámci svojich nariadení a smerníc stanoviť bezpečnostné požiadavky a požiadavky bezpečnostných záruk produktov IKT;
- koncoví používatelia, ktorí chcú dodržiavať predpisy alebo získať dôkazy o bezpečnosti produktov IKT, ktoré chránia ich citlivé aktíva.

Na vyjadrenie svojich bezpečnostných požiadaviek, a to tak hľadiska funkcionalít, ako aj bezpečnostných záruk, môžu tieto komunity použiť metodiku opísanú v kapitole 24, ĎALŠIE PRVKY SCHÉMY, aby vytvorili ochranný profil pre kategóriu produktov, ktoré sa majú certifikovať, alebo môžu vytvoriť individuálny bezpečnostný zámer pre jednotlivé produkty, ktoré sa majú certifikovať.

S cieľom znížiť zložitosť pri hodnotení a zároveň zachovať potrebnú úroveň dôvery umožňuje schéma EUCC certifikáciu zložených produktov[3]. Takéto certifikácie musia spĺňať podmienky stanovené v kapitole 9, INFORMÁCIE POTREBNÉ NA CERTIFIKÁCIU.

Pri zvažovaní certifikácie kybernetickej bezpečnosti produktu IKT alebo používania certifikovaného produktu IKT musia rôzne zainteresované strany vrátane orgánov verejnej moci a súkromného sektora zohľadniť tieto charakteristiky schémy EUCC:

- európska harmonizovaná kvalita certifikátov pre produkty IKT, ktorej cieľom je dosiahnuť úroveň záruky "významná" a "vysoká" podľa CSA, a to prostredníctvom hodnotenia nezávislou treťou stranou, zapojením národných orgánov a v prípade potreby vzájomným posudzovaním;
- niekoľko podúrovní záruky, ktoré umožňujú nájsť kompromis medzi bezpečnostnými zárukami a nákladmi na hodnotenie a certifikáciu;
- rozsiahly katalóg dostupných a štandardizovaných bezpečnostných funkcionalít a požiadaviek bezpečnostných záruk, ktoré ponúka CC a ktoré sú bližšie opísané v kapitole 4, ÚROVNE ZÁRUKY, ktoré možno vybrať na definovanie harmonizovaných bezpečnostných požiadaviek EÚ prostredníctvom ochranných profilov v mnohých oblastiach bezpečnosti a sektoroch;
- životný cyklus produktu IKT s jeho podpornou dokumentáciou zahrnutou do rozsahu hodnotenia a možným opakovaným použitím výsledkov medzi certifikáciami, čo uľahčuje úsporný

[3] napr. aplikácie nad certifikovanou platformou alebo platformy nad certifikovaným integrovaným obvodom.

harmonogram a štruktúru nákladov;
- široká dostupnosť podporných dokumentov, ktoré umožňujú dobrú prípravu certifikačných činností;
- nový súbor harmonizovaných činností týkajúcich sa udržiavania certifikátov a monitorovania a riešenia nesúladu a nezhôd;
- nové harmonizované podmienky pre zaobchádzanie so zraniteľnosťami a zrýchlený postup posudzovania záplat;
- nové bezpečnostné podmienky ochrany informácií používaných na certifikáciu;
- kontinuita s predchádzajúcimi národnými certifikačnými schémami, a to tak z hľadiska kvality certifikátov, ako aj z hľadiska kompatibility metodiky, čo umožní hladký prechod na novú schému, a to tak z hľadiska certifikátov, ako aj orgánov zapojených do certifikácie (CB a ITSEF), najmä na úrovni záruky "vysoká";
- nová možnosť pre súkromné subjekty zapojiť sa do certifikačných činností v oblasti kybernetickej bezpečnosti na úrovni záruky "významná" a kombinovať ich s inými sektorovými certifikačnými činnosťami;
- celoeurópske udržiavanie schémy EUCC s cieľom neustáleho zlepšovania.

ZÁKLADNÉ INFORMÁCIE

V časti 1 CC sa uvádza, že: "*Výsledky hodnotenia môžu spotrebiteľom pomôcť určiť, či tieto IT produkty spĺňajú ich bezpečnostné potreby. CC je užitočný ako návod na vývoj, hodnotenie a/alebo obstarávanie IT produktov s bezpečnostnými funkcionalitami. CC je zámerne flexibilný, čo umožňuje použiť celý rad metód hodnotenia na celý rad bezpečnostných vlastností celého radu IT produktov [...] Zatiaľ čo ST vtedy opisuje konkrétny TOE (napr. Firewall MinuteGap v18.5), PP je určený na opis typu TOE (napr. firewallov). Ten istý PP sa preto môže použiť ako šablóna pre mnoho rôznych ST, ktoré sa majú použiť pri rôznych hodnoteniach. [...] Vo všeobecnosti ST opisuje požiadavky na TOE a píše ho vývojár tejto TOE, zatiaľ čo PP opisuje všeobecné požiadavky na typ TOE, a preto ho zvyčajne píše:*
- *Komunita používateľov, ktorá sa snaží dosiahnuť konsenzus pri požiadavkách na daný typ TOE;*
- *Vývojár TOE alebo skupina vývojárov podobných TOE, ktorí chcú stanoviť minimálnu základnú úroveň pre daný typ TOE;*
- *Vláda alebo veľká korporácia, ktorá špecifikuje svoje požiadavky v rámci procesu obstarávania."*

Pokiaľ ide o výhody, ktoré treba zvážiť pri výbere tejto schémy pre kybernetickú bezpečnosť produktov IKT, niektoré z nich priamo súvisia s vlastnosťami schémy (napr. opakovaná použiteľnosť certifikačných činností, možnosť vytvoriť ochranné profily).

Okrem toho:

- Udržiavanie certifikátov a monitorovanie súladu boli široko rozvinuté pre schému EUCC s cieľom poskytnúť bezpečnostnú záruku, že bezpečnosť produktu je zachovaná.
- Spoločné kritériá sú harmonizované kritériá uznané medzinárodnými normalizačnými výbormi ISO a IEC, ktoré sú neustále udržiavané širokou medzinárodnou a európskou štruktúrovanou komunitou zloženou technických z expertov, ktorí spolupracujú s jediným cieľom, a to zdokonaľovať normu.
- CC poskytuje (akýsi pseudo-formálny) jazyk na stanovenie bezpečnostných funkcionalít, mechanizmov a činností na ich hodnotenie. CC sú flexibilné, pretože poskytujú katalóg skupín a funkcií a ich použitie a rozšírenie, aby bolo možné opísať akýkoľvek druh produktu IKT, či už ide o hardvér, firmvér alebo softvér, alebo ich kombináciu.
- CC má najväčší katalóg vzájomne preskúmaných a na produkte nezávislých požiadaviek bezpečnostných funkcionalít (SFR) a požiadaviek bezpečnostných záruk (SAR) použiteľných pre širokú škálu produktov IKT.
- CC umožnili vytvoriť rozsiahly katalóg základných požiadaviek schválených odvetvím prostredníctvom ochranných profilov.
- Okrem bezpečnosti produktu umožňuje CC kontrolovať aj bezpečnosť vývojárskej lokality a bezpečnosť procesu vývoja.
- Certifikácia v rámci tejto schémy na úrovni záruky "vysoká" je podmienená autorizáciou NCCA.
- Mnohé krajiny a používatelia oceňujú certifikáciu podľa CC: CC má dlhoročnú históriu, pokiaľ ide o jej uznanie pätnástimi krajinami EÚ a celkovo viac ako tridsiatimi krajinami na ich federálnej a vládnej úrovni. Okrem toho už viac ako 4500 produktov získalo certifikát CC a používajú ich miliardy používateľov na celom svete.
- CC umožňujú spotrebiteľom nestranné posúdenie produktu IKT: takéto posúdenie je zároveň hodnotením bezpečnosti, keďže CC zahŕňajú analýzu a testovanie produktu z hľadiska jeho súladu

s konkrétnymi bezpečnostnými požiadavkami. Tým sa zvyšuje úroveň záruky spotrebiteľa v bezpečnosť certifikovaného produktu IKT a spoliehanie sa na ňu.

- Flexibilný súbor hodnotenia úrovní záruky: v CC je definovaných viacero úrovní bezpečnostnej záruky, ktoré boli priradené k dvom úrovniam záruky CSA. To umožňuje pokryť veľký počet rôznych potrieb trhov v oblasti bezpečnostných záruk, pretože čím vyššiu úroveň záruky produkt má, tým viac dôkazov o jeho bezpečnosti existuje so stále prísnejšou metódou testovania.
- Schéma zahŕňa špecifické opatrenia, ktoré umožňujú rýchle uznávanie certifikovaných produktov IKT, keďže obsahuje pravidlá na zavedenie a používanie osobitného rámca označovania. Tento rámec bol navrhnutý tak, aby podporoval umiestňovanie certifikovaných produktov na jednotnom trhu EÚ aj mimo neho.

3. NORMY POUŽITÉ PRI HODNOTENÍ

ODKAZ(-Y) NA ČLÁNOK(-KY) CSA

Článok 54 1. *Európska schéma certifikácie kybernetickej bezpečnosti obsahuje aspoň tieto prvky:*

c) odkazy na medzinárodné, európske alebo národné normy použité pri hodnotení alebo, ak takéto normy nie sú k dispozícii alebo nie sú vhodné, na technické špecifikácie, ktoré spĺňajú požiadavky stanovené v prílohe II k nariadeniu (EÚ) č. 1025/2012, alebo, ak takéto špecifikácie nie sú k dispozícii, na technické špecifikácie alebo iné požiadavky kybernetickej bezpečnosti vymedzené v európskej schéme certifikácie kybernetickej bezpečnosti.

Hodnotenie sa zakladá na týchto normách:

- Spoločné kritériá pre hodnotenie bezpečnosti informačných technológií podľa ich platnej verzie ISO/IEC 15408 alebo podľa ich platnej verzie uverejnenej na stránke https://www.commoncriteriaportal.org/cc/ a pozostávajú z:
  - CC Časť 1: Úvod a všeobecný model;
  - CC časť 2: Komponenty bezpečnostných funkcionalít;
  - CC časť 3: Komponenty bezpečnostných záruk;
- v tejto kandidátskej schéme označované ako Spoločné kritériá alebo CC;
- Spoločná metodika hodnotenia bezpečnosti informačných technológií podľa jej platnej verzie ISO/IEC 18045 alebo podľa jej platnej verzie uverejnenej na https://www.commoncriteriaportal.org/cc/, v tejto kandidátskej schéme označovaná ako CEM.

Vo vydaných certifikátoch sa uvedie, ktorá verzia/vydanie CC a CEM boli použité na hodnotenie a certifikáciu.

Pri hodnotení sa zohľadňujú aj podporné prvky stanovené tak, aby umožňovali harmonizovaný výklad týchto noriem. Ako je bližšie vymedzené v kapitole 8, ŠPECIFICKÉ KRITÉRIA A METÓDY HODNOTENIA, takéto prvky sú buď povinnými podpornými prvkami začlenenými ako prílohy tejto schémy, alebo usmerňujúcimi podpornými dokumentmi vypracovanými v spolupráci s ECCG a poskytovanými agentúrou ENISA na jej webovej stránke venovanej certifikácii kybernetickej bezpečnosti.

V prípade potreby môžu rôzne zainteresované strany certifikácie kybernetickej bezpečnosti produktov IKT definovať ochranné profily ako technické špecifikácie. Takéto technické špecifikácie môžu byť prijaté ako normy vnútroštátnou, európskou alebo medzinárodnou normalizačnou organizáciou (nariadenie 1025/2012[4]) a certifikované podľa požiadaviek tejto schémy. Agentúra ENISA na svojej webovej stránke venovanej certifikácii kybernetickej bezpečnosti poskytne zoznam týchto ochranných profilov.

Okrem toho sa na akreditáciu orgánov posudzovania zhody, ktoré vykonávajú činnosti posudzovania a certifikácie, vzťahujú tieto normy na podporu článkov 60.1-2 a prílohy 19-20 CSA:

- ISO/IEC 17065 pre orgán posudzovania zhody alebo národný orgán zodpovedný za certifikačné činnosti, ďalej označovaný ako certifikačný orgán (CB);
- ISO/IEC 17025 pre časť orgánu posudzovania zhody alebo národného orgánu tretej strany, alebo subdodávateľa CAB alebo národného orgánu, ktorý je zodpovedný za činnosti hodnotenia, ďalej označované ako skúšobné laboratórium (ITSEF).

ZÁKLADNÉ INFORMÁCIE

Normy ISO/IEC 15408 a ISO/IEC 18045 boli od vytvorenia a prijaté ako súčasť Spoločných kritérií

[4] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1025/2012 z 25. októbra 2012 o európskej normalizácii.

(CC) a Spoločnej metodiky hodnotenia bezpečnosti informačných technológií (CEM), vnímané komunitou Spoločných kritérií ako technické špecifikácie v rámci CCRA.

Prebiehajúca revízia oboch noriem v ISO umožní zaviesť pokročilé kritériá, ktoré ponúka piate vydanie CC v súvislosti so zavedením pojmov Base-PP, PP-Module a PP-Configuration. Preto keď sa do definície produktu IKT na účely jeho hodnotenia zavedú PP-moduly, okrem noriem sa v súčasnosti uplatňujú aj technické špecifikácie.

Spoločná metodika hodnotenia bezpečnosti informačných technológií (CEM) vo svojom úvode uvádza nasledovné: "*CEM uznáva, že v tomto dokumente nie sú zodpovedané všetky otázky týkajúce sa hodnotenia bezpečnosti IT a že budú potrebné ďalšie výklady. Jednotlivé schémy určia, ako sa s takýmito výkladmi vysporiadať, hoci tieto môžu byť predmetom dohôd o vzájomnom uznávaní.*"

S cieľom harmonizovať postupy hodnotenia a certifikácie a uľahčiť vzájomné uznávanie certifikátov preto komunita SOG-IS vytvorila dlhý rad podporných dokumentov, ktoré spresňujú požiadavky oboch hlavných noriem. Väčšina týchto dokumentov nebola predložená na normalizáciu a sú kľúčové aj pre novú schému CC, a preto budú po povinnom uplatnení pridané do schémy EUCC.

Určité spoločenstvá zainteresovaných strán v EÚ alebo regulačné orgány EÚ sa môžu rozhodnúť vytvoriť ochranné profily, ktoré sú vypracované v rámci normalizačných orgánov EÚ alebo medzinárodných normalizačných orgánov a na ktoré sa ďalej odkazuje ako na platné normy alebo technické špecifikácie v rámci nariadenia. Tieto PP by mali byť certifikované, ako to ponúka schéma v kapitole 24, ĎALŠIE PRVKY SCHÉMY, a potom by sa malo zvážiť ich zverejnenie na webovej stránke agentúry ENISA venovanej certifikácii kybernetickej bezpečnosti.

4. ÚROVNE ZÁRUKY

ODKAZ (-Y) NA ČLÁNOK(-KY) CSA

Článok 52.6 *Európsky certifikát kybernetickej bezpečnosti, ktorý odkazuje na úroveň záruky "významná", poskytuje bezpečnostnú záruku, že produkty IKT, služby IKT a procesy IKT, pre ktoré sa tento certifikát vydáva, spĺňajú príslušné bezpečnostné požiadavky vrátane bezpečnostných funkcionalít a že boli hodnotené na úrovni určenej na minimalizáciu známych rizík kybernetickej bezpečnosti a rizika incidentov a kybernetických útokov vykonávaných subjektmi s obmedzenými zručnosťami a zdrojmi. Činnosti hodnotenia, ktoré sa majú vykonať, zahŕňajú aspoň tieto činnosti: preskúmanie s cieľom preukázať neprítomnosť verejne známych zraniteľností a testovanie s cieľom preukázať, že produkty IKT, služby IKT alebo procesy IKT správne implementujú potrebné bezpečnostné funkcionality. Ak takéto činnosti hodnotenia nie sú vhodné, vykonajú sa náhradné činnosti hodnotenia s rovnocenným účinkom.*

Článok 52.7 Európsky certifikát kybernetickej bezpečnosti, ktorý odkazuje na úroveň záruky "vysoká", poskytuje bezpečnostnú záruku, že produkty IKT, služby IKT a procesy IKT, pre ktoré sa tento certifikát vydáva, spĺňajú príslušné bezpečnostné požiadavky vrátane bezpečnostných funkcionalít a že boli vyhodnotené na úrovni určenej na minimalizáciu rizika najmodernejších kybernetických útokov, ktoré vykonávajú subjekty so značnými zručnosťami a zdrojmi. Činnosti hodnotenia, ktoré sa majú vykonať, zahŕňajú aspoň tieto činnosti: preskúmanie s cieľom preukázať neprítomnosť verejne známych zraniteľností; testovanie s cieľom preukázať, že produkty IKT, služby IKT alebo procesy IKT správne implementujú potrebné bezpečnostné funkcionality na úrovni state-of-the-art; a posúdenie ich odolnosti voči kvalifikovaným útočníkom pomocou penetračného testovania. Ak takéto činnosti hodnotenia nie sú vhodné, vykonajú sa náhradné činnosti hodnotenia s rovnocenným účinkom.

Článok 52.8 Európska schéma certifikácie kybernetickej bezpečnosti môže stanoviť niekoľko hodnotení úrovní v závislosti od prísnosti a hĺbky použitej metodiky hodnotenia. Každá z hodnotení úrovní zodpovedá jednej z úrovní záruky a je definovaná vhodnou kombináciou komponentov záruk.

Článok 54 1. Európska schéma certifikácie kybernetickej bezpečnosti obsahuje aspoň tieto prvky:

d) prípadne jednu alebo viacero úrovní záruky.

Certifikácia v rámci tejto schémy sa vzťahuje na úrovne záruky "významná" a "vysoká" CSA.

Priradenie k úrovniam záruky CSA sa zakladá na použití komponentov záruk pre hodnotenie zraniteľnosti definovaných v časti 3 CC takto:

- AVA_VAN.1 a AVA_VAN.2 sa vzťahujú na úroveň záruky "významná" CSA;
- AVA_VAN.3 až AVA_VAN.5 zodpovedajú úrovni záruky "vysoká" CSA.

Všetky závislosti, ako sú definované v časti 3 CC, ktoré sa vzťahujú na zvolenú úroveň AVA_VAN, sa pri hodnotení uplatnia[5] a zahrnú do aplikovaných požiadaviek bezpečnostných záruk.

Prednostne všetky komponenty záruk z hodnotenia úrovne záruky (EAL) definovanej v časti 3 CC, ktorá je spojená so zvolenou úrovňou AVA_VAN, sa použijú, v súlade s príslušnou tabuľkou.

***Tabuľka 1**: Zhrnutie hodnotenia úrovne záruky (výňatok z časti 3 CC)*

[5] Ako príklad z časti 3 CC uvádzame priame závislosti, ktoré sa vzťahujú na analýzu zraniteľnosti zameranú na AVA_VAN.3:
ADV_ARC.1 Opis bezpečnostnej architektúry
ADV_FSP.4 Úplná funkčná špecifikácia
ADV_TDS.3 Základný modulárny dizajn
ADV_IMP.1 Zobrazenie implementácie TSF
AGD_OPE.1 Používateľské pokyny
AGD_PRE.1 Postup prípravy
ATE_DPT.1 Skúšanie: základný návrh

Trieda záruk *Assurance class*	**Skupina záruk** *Assurance Family*	**Komponenty záruk podľa hodnotenia úrovne záruky** *Assurance Components by Evaluation Assurance Level*						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Vývoj *Development*	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Sprievodná dokumentácia *Guidance documents*	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Podpora životného cyklu *Life-cycle support*	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	1	1
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Hodnotenie bezpečnostného zámeru *Security target evaluation*	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1		1		1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Skúšky *Tests*	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Posudzovanie zraniteľnosti *Vulnerability Assessment*	AVA_VAN	1	2	2	3	4	5	5

ADV_ARC	Security Architecture	Bezpečnostná architektúra
ADV_FSP	Functional Specification	Funkčná špecifikácia
ADV_IMP	Implementation Representation	Zobrazenie implementácie
ADV_INT	TSF Internals	Vnútorné TSF (Trusted Security Functions)
ADV_SPM	Security Policy modelling	Modelovanie bezpečnostnej politiky
ADV_TDS	TOE design	TOE návrh
AGD_OPE	Operational user guide	Používateľská príručka
AGD_PRE	Preparative procedures	Postup prípravy
ALC_CMC	CM Capabilities	Schopnosti CM
ALC_CMS	CM Scope	Rozsah CM
ALC_DEL	Delivery	Doručovanie
ALC_DVS	Development Security	Bezpečnosť vývoja
ALC_FLR	Flaw remediation	Odstraňovanie chýb
ALC_LCD	Life-cycle definition	Definícia životného cyklu
ALC_TAT	Tools and Techniques	Nástroje a techniky
ASE_CCL	Conformance Claims	Potvrdenie zhody
ASE_ECD	Extended Component Definition	Definícia
ASE_INT	ST Introduction	Predstavenie bezpečnostného zámeru
ASE_OBJ	Security Objectives	Bezpečnostné ciele
ASE_REQ	Security Requirements	Bezpečnostné požiadavky
ASE_SPD	Security Problem Definition	Definícia bezpečnostného problému
ASE_TSS	TOE Summary Specification	Súhrnná špecifikácia TOE
ATE_COV	Coverage	Pokrytie

ATE_DPT	Depth	Hĺbka
ATE_FUN	Functional test	Funkčná skúška
ATE_IND	Independent testing	Nezávislé skúšanie
AVA_VAN	Vulnerability Assessment	Posudzovanie zraniteľností

Ak je úroveň AVA_VAN spojená s viacerými EAL, možno vybrať ktorýkoľvek z nich.

Výber nižšej úrovne EAL, ako je úroveň priradená k úrovni AVA_VAN v predchádzajúcej tabuľke, môže byť naďalej možný za podmienok, že:

- Zvolená EAL nesmie byť o viac ako dve úrovne nižšia ako najnižšia EAL priradená k úrovni AVA_VAN;
- Výsledná úroveň záruky sa považuje za rozšírenie zvolenej EAL, ako je definované v časti 3 CC a v súlade s prílohou 1, VYHLÁSENIE O BALÍKU ZÁRUKY V CERTIFIKÁTE.

Zvolená úroveň AVA_VAN určuje príslušnú úroveň záruky CSA pre produkt IKT a pravidlá, ktoré sa majú uplatňovať pri certifikácii príslušného produktu IKT.

Preto ako dôsledky na ilustráciu na niekoľkých vzorových prípadoch:

- pri výbere AVA_VAN.2, ktorá je v súlade s CC Časť 3 v oboch hodnoteniach úrovní záruky EAL2 a EAL3:
    - uplatňujú sa všetky závislosti AVA_VAN.2 definované v časti 3 CC;
    - pri hodnotení by sa aspoň mali brať do úvahy všetky činnosti bezpečnostných záruk EAL2 ;
- certifikát týkajúci sa hodnotenia úrovne záruky EAL3, ktorý podľa definície obsahuje AVA_VAN.2, sa považuje za certifikát na "významnej" úrovni záruky CSA;
- certifikát na úrovni EAL3 rozšírený o AVA_VAN.3 a súvisiace závislosti je možný a považuje sa za certifikát na "vysokej" úrovni záruky CSA.

Možnosť hodnotenia a certifikácie pomocou komponentov záruk pre posudzovanie zraniteľnosti AVA_VAN.1 a AVA_VAN.2 vychádza zo všeobecných ustanovení tejto schémy.

Možnosť hodnotenia a certifikácie pomocou komponentov záruk pre posudzovanie zraniteľnosti AVA_VAN.3 vychádza zo všeobecných ustanovení tejto schémy s pridaním požiadaviek stanovených pre úroveň záruky CSA "vysoká" v rámci tejto schémy.

Možnosť hodnotenia a certifikácie pomocou komponentov záruk pre hodnotenie zraniteľnosti AVA_VAN.4 a AVA_VAN.5 vychádza zo všeobecných ustanovení tejto schémy s doplnením požiadaviek stanovených pre:

- Úroveň záruky CSA "vysoká" v rámci tejto schémy;
- Technické domény, ako sú definované v kapitole 8, ŠPECIFICKÉ KRITÉRIA A METÓDY HODNOTENIA.

Vo všeobecnosti platí, že ak pre technológiu produktov IKT nebola definovaná žiadna technická doména, súvisiace certifikáty nesmú deklarovať vyššiu úroveň posúdenia zraniteľnosti ako komponent AVA_VAN.3.

Certifikácia nad AVA_VAN.3 pre produkty IKT, na ktoré sa nevzťahuje technická doména, je možná len na základe osobitného ochranného profilu definovaného a certifikovaného v rámci tejto schémy, ktorý obsahuje usmernenia pre osobitnú metodiku hodnotenia a je na tento účel prílohou k schéme. Požiadavky na usmernenie pre PP sa môžu vynechať len vtedy, ak s tým súhlasí vlastník rizika (napr. zástupca prevádzkovateľa, tvorca národnej politiky, regulačný orgán) koncovej aplikácie prípadu opísaného v PP.

Produktom IKT certifikovaným podľa týchto ochranných profilov sa venuje veľká pozornosť v rámci mechanizmu vzájomného posudzovania, ktorý je súčasťou tejto schémy.

V certifikáte vydanom podľa tejto schémy sa uvádza úroveň záruky CSA a úrovne CC AVA_VAN a EAL, ktoré boli potvrdené pri hodnotení produktu IKT, ako aj komponentov SAR. Uvádza sa v ňom akékoľvek obmedzenie týkajúce sa maximálnych úrovní, ktoré môže CAB dosiahnuť v súlade s touto schémou.

Agentúra ENISA môže v spolupráci s ECCG poskytnúť usmernenie, ako vybrať správnu úroveň záruky na základe posúdenia rizika.

ZÁKLADNÉ INFORMÁCIE

CC vo svojej časti 3 definovali skupinu záruk "Posúdenie zraniteľnosti", ktorá sa zaoberá možnosťou zneužitia zraniteľností zavedených pri vývoji alebo prevádzke TOE.
Pri vykonávaní analýzy zraniteľnosti existujú tri hlavné faktory, a to:

1. identifikácia potenciálnych zraniteľností:
   a. Vyhľadávanie vo verejnej oblasti (CVE, CERT atď.);
   b. Vyhľadávanie dôkazov o hodnotení (v rámci projektovej dokumentácie, usmernení pre používateľov atď.);
2. posúdenie s cieľom určiť, či by identifikované potenciálne zraniteľnosti mohli umožniť útočníkovi s príslušným potenciálom útoku narušiť SFR:
   a. Hypotéza chýb (analytický prístup k hľadaniu potenciálnych zraniteľností, definovanie priorít);
3. penetračné testovanie s cieľom určiť, či sú identifikované potenciálne zraniteľnosti zneužiteľné v operačnom prostredí TOE.

Pre túto triedu záruk bolo definovaných päť rôznych úrovní, pričom "*úroveň je založená na zvyšujúcej sa prísnosti analýzy zraniteľností hodnotiteľom a na zvyšujúcej sa úrovni potenciálu útoku, ktorý útočník potrebuje na identifikáciu a využitie potenciálnych zraniteľností*."

- AVA_VAN.1 Prieskum zraniteľnosti
  - Odolnosť TOE proti základnému potenciálu útoku
- AVA_VAN.2 Analýza zraniteľnosti (neštruktúrovaná)
  - Odolnosť TOE proti základnému potenciálu útoku
- AVA_VAN.3 Zameraná (neštruktúrovaná) analýza zraniteľnosti
  - Odolnosť TOE proti rozšírenému základnému potenciálu útoku
- AVA_VAN.4 Metodická analýza zraniteľnosti
  - Odolnosť TOE proti strednému potenciálu útoku
- AVA_VAN.5 Pokročilá metodická analýza zraniteľností
  - Odolnosť TOE proti vysokému potenciálu útoku

Táto trieda bola preto vybraná ako najreprezentatívnejšia trieda na splnenie požiadaviek článku 52.1 a jeho všeobecnej požiadavky v oddiele 1: "*Úroveň záruky musí zodpovedať úrovni rizika spojeného so zamýšľaným používaním produktu IKT, služby IKT alebo procesu IKT z hľadiska pravdepodobnosti a vplyvu incidentu*."

Podľa CEM *by sa pri analýze potenciálu útoku potrebného na zneužitie zraniteľnosti mali zohľadniť tieto faktory*:
a) Čas potrebný na identifikáciu a zneužitie (uplynulý čas);
b) Požadované odborné technické znalosti (odborná expertíza);
c) Znalosť konštrukcie a prevádzky TOE (znalosť TOE);
d) Okno pre príležitosť;
e) IT hardvér/softvér alebo iné vybavenie potrebné na zneužívanie."

CEM definoval tabuľku na výpočet potenciálu útoku:

Tabuľka 2: *Výpočet potenciálu útoku (výňatok z CEM)*

faktor ***factor***	**hodnota** ***value***
uplynulý čas ***elapsed time***	
<=*one day*	0
<=*one week*	1
<=two weeks	2
<=*one month*	4
<=*two months*	7
<=*three months*	10
<=*forth months*	13
<=*five months*	15
<=*six months*	17
>*six months*	19
Expertise	
laik *Laymen*	0
zdatný *proficient*	3*(1)
expert *expert*	6
viacnásobný expert *multiple expert*	8
znalosti experta ***Knowledge of TOE***	
verejné *public*	0
vyhradené *restricted*	3
citlivé *sensitive*	7
kritické *critical*	11
okno pre príležitosť ***Window of opportunity***	
zbytočný/neobmedzený prístup *unnecessary/unlimited access*	0
jednoduchý *easy*	1
stredný *moderate*	4
zložitý *difficult*	10
žiadny *none*	**(2)
zariadenie ***Equipment***	
štandard *standard*	0
špecializovaný *specialised*	4(3)
na mieru *bespoke*	7

faktor ***factor***	**hodnota** ***value***
uplynulý čas ***elapsed time***	
viacnásobne na mieru *multiple bespoke*	9

(1) Keď je potrebných niekoľko zdatných osôb na dokončenie cesty útoku, výsledná úroveň expertízy zostane „zdatný“ (čo vedie k ratingu 3)

(2) Naznačuje, že cesta útoku nie je zneužiteľná vzhľadom na ďalšie opatrenia v zamýšľanom operačnom prostredí TOE

(3) Ak sa na jednotlivé kroky útoku vyžadujú zreteľne odlišné skúšobné zariadenia pozostávajúce zo špecializovaného vybavenia, malo by sa to hodnotiť ako na mieru

Na základe týchto prvkov pre výpočet potenciálu útoku CEM definuje hodnotenie odolnosti produktu pomocou nasledujúcej tabuľky:

Tabuľka 3: *Hodnotenie zraniteľností a odolnosti TOE (výňatok z CEM)*

hodnota *value*	potenciál útoku potrebný na scenár zneužitia *attack potential required to exploit scenario*	odolnosť TOE voči útočníkom s potenciálom útoku: *TOE resistant to attackers with attack potential of:*	spĺňanie komponentov záruk *meets assurance components*	zlyhanie komponentov *failure of components*
0-9	základný *Basic*	bez ratingu *No rating*	-	AVA_VAN1 AVA_VAN2 AVA_VAN3 AVA_VAN4 AVA_VAN5
10-13	rozšírený-základný *Enhanced-Basic*	základný *Basic*	AVA_VAN1 AVA_VAN2	AVA_VAN3 AVA_VAN4 AVA_VAN5
14-19	stredný *Moderate*	*rozšírený-základný* *Enhanced-Basic*	AVA_VAN1 AVA_VAN2 AVA_VAN3	AVA_VAN4 AVA_VAN5
20-24	vysoký *High*	*stredný* *Moderate*	AVA_VAN1 AVA_VAN2 AVA_VAN3 AVA_VAN4	AVA_VAN5
=>25	veľmi vysoký *Beyond High*	vysoký *High*	AVA_VAN1 AVA_VAN2 AVA_VAN3 AVA_VAN4 AVA_VAN5	-

Okrem toho sa v CC zavádza pojem závislosti medzi komponentami záruk, čo znamená, že pri výbere jedného komponentu záruk sa na splnenie požiadaviek normy použijú aj súvisiace komponenty. Tieto závislosti sa požadujú aj na mapovanie s úrovňami záruky CSA.

Norma definuje pre prvú úroveň triedy hodnotenia zraniteľnosti, AVA_VAN.1, nasledovné: "*Hodnotiteľ vykoná prieskum zraniteľností na základe verejne dostupných informácií s cieľom zistiť potenciálne zraniteľnosti, ktoré môže útočník ľahko nájsť. Hodnotiteľ vykoná penetračné testovanie, aby potvrdil, že potenciálne zraniteľnosti nie je možné využiť v operačnom prostredí TOE. Penetračné testovanie vykonáva hodnotiteľ za predpokladu, že potenciál útoku je základný*."

Pojem *Základný potenciál útoku* používaný v CC je pri porovnaní s úrovňou záruky základná v CSA zavádzajúci, pretože:

- na dosiahnutie tejto úrovne je potrebné získať aspoň 10 bodov vzhľadom na predchádzajúcu tabuľku;
- typ činností vykonaných na posúdenie zhody s AVA_VAN.1 už spĺňa nasledujúcu požiadavku CSA

pre úroveň záruky "významná", ako je definovaná v článku 52.6:
- "Preskúmanie s cieľom preukázať, že neexistujú verejne známe zraniteľnosti".

S cieľom splniť dodatočné požiadavky článku 52.6 pre úroveň záruky "významná":

- "overenie súladu bezpečnostných funkcionalít produktu IKT, služby IKT alebo procesu IKT s jeho technickou dokumentáciou" (odôvodnenie 89) alebo "testovanie s cieľom preukázať, že produkty IKT, služby IKT alebo procesy IKT správne implementujú potrebné bezpečnostné funkcionality" (článok 52 ods. 6 CSA);

bola stanovená potreba zohľadniť celý balík komponentov záruk súvisiacich s úrovňou EAL priamo vrátane úrovne AVA_VAN.

EAL1, ktorá obsahuje AVA_VAN.1, si vyžaduje aj funkčné nezávislé skúšanie produktu IKT prostredníctvom jeho komponentu ATE_IND.1.

Toto všeobecné pravidlo zohľadnenia všetkých závislostí alebo celého balíka EAL však môže podliehať výnimke, ako sa predpokladá v časti 3, 6.1.3.4 CC: "*V špecifických situáciách sa uvedené závislosti nemusia uplatniť. Autor PP/ST sa môže na základe zdôvodnenia, prečo daná závislosť nie je uplatniteľná, rozhodnúť **nie** na splnenie tejto závislosti*."

Keďže AVA_VAN.2 vychádza z rovnakého potenciálu útoku ako AVA_VAN.1, považuje sa za rovnakú úroveň záruky CSA "významná".

AVA_VAN.3 umožňuje riešiť ďalšiu kategóriu potenciálu útoku, ktorá je v CC definovaná ako rozšírená-základná, a pridáva nasledujúcu činnosť pre hodnotiteľa: "*Hodnotiteľ vykoná nezávislú, cielenú analýzu zraniteľnosti TOE s použitím riadiacej dokumentácie, funkčnej špecifikácie, návrhu TOE, opisu bezpečnostnej architektúry a zobrazenia implementácie s cieľom identifikovať potenciálne zraniteľnosti TOE*."

Na základe rozpätia 14-19 bodov na riešenie tejto úrovne rozšírená-základná sa táto úroveň zaoberá potrebou odolávať útočníkom:

- so značnými zručnosťami a prostriedkami: odborná úroveň zdatný s vybavením na mieru alebo odborníka na špecializované vybavenie, čo by v oboch prípadoch "pripísalo" desať bodov;
- útok počas pomerne dlhého obdobia (viac ako jeden (1) mesiac), čo by znamenalo sedem bodov.

Považuje sa to za splnenie požiadaviek článku 52.7 pre CSA úroveň záruky "vysoká".

Na základe vyššie uvedenej definície to zároveň znamená, že hodnotiteľovi s minimálne rovnakou úrovňou zručností a vybavenia, ako je opísané vyššie, je nariadené vykonať cielenú analýzu zraniteľností s použitím citlivých informácií o produkte, ku ktorým by sa "skutočný" útočník nemal dostať. To je jednoznačne nad rámec požiadavky spojenej s "významnou" úrovňou, ktorá má zabezpečiť "*preskúmanie s cieľom preukázať neprítomnosť verejne známych zraniteľností*".

Pokiaľ ide o ešte vyššie úrovne AVA_VAN (4 a 5), komunita SOG-IS predstavila potrebu definovať spoločný rámec, ktorý by umožnil harmonizovať posúdenie odborníkov, aby sa zohľadnil kontext hodnotenia uvedený v časti 3 CC, kapitola 5.5:

"V záujme *dosiahnutia väčšej porovnateľnosti výsledkov hodnotenia by sa hodnotenia mali vykonávať v rámci autoritatívneho systému hodnotenia, ktorý stanovuje normy, monitoruje kvalitu hodnotení a spravuje predpisy, ktoré musia dodržiavať skúšobné laboratóriá a hodnotitelia. V CC sa neuvádzajú požiadavky na regulačný rámec. Na dosiahnutie cieľa vzájomného uznávania výsledkov takýchto hodnotení však bude potrebný súlad medzi regulačnými rámcami rôznych hodnotiacich orgánov. Druhým spôsobom dosiahnutia väčšej porovnateľnosti výsledkov hodnotenia je používanie spoločnej metodiky na dosiahnutie týchto výsledkov. V prípade CC je táto metodika uvedená v CEM. Používanie spoločnej metodiky hodnotenia prispieva k opakovateľnosti a objektívnosti výsledkov, ale samo osebe nie je postačujúce. Mnohé z hodnotiacich kritérií si vyžadujú uplatnenie odborného posúdenia a základných znalostí, pri ktorých sa konzistentnosť dosahuje ťažšie. S cieľom zvýšiť konzistentnosť výsledkov hodnotenia sa konečné výsledky hodnotenia môžu predložiť na certifikačný proces. Certifikačný proces je nezávislá kontrola výsledkov hodnotenia, ktorá vedie k vypracovaniu konečného certifikátu alebo schválenia, ktoré je zvyčajne verejne dostupné. Proces certifikácie je prostriedkom na dosiahnutie väčšej konzistentnosti pri uplatňovaní kritérií bezpečnosti IT. Za hodnotiace schémy a certifikačné procesy sú zodpovedné hodnotiace orgány, ktoré tieto schémy a procesy prevádzkujú, a nepatria do pôsobnosti CC*."

Takýto spoločný rámec bol definovaný prostredníctvom vývoja technických domén, ktoré okrem iného umožňujú definovať spoločné chápanie potenciálu útoku a súvisiacich metód útoku pre vyššie úrovne certifikácie (vrátane AVA_VAN.4 a 5) a pre konkrétne typy produktov IKT. Jeho uplatnenie sa týka aj možnosti CAB vykonávať takéto hodnotenia, ktoré sú bližšie definované v kapitole 6, ŠPECIFICKÉ POŽIADAVKY VZŤAHUJÚCE SA NA CAB.

Ak pre produkt IKT, ktorý sa má certifikovať, nebola definovaná žiadna špecifická technická doména nad úrovňou AVA_VAN.3 alebo ak neexistuje príslušné oprávnenie CAB certifikovať príslušnú špecifickú technickú doménu produktu IKT, ktorý sa má certifikovať, certifikát vydaný v rámci tejto schémy by sa mal obmedziť na úroveň AVA_VAN.3.

Zaviedla sa možnosť odchýliť sa od tohto všeobecného pravidla, že certifikácia nad úrovňou AVA_VAN.3 si vyžaduje technickú doménu, a to len prostredníctvom definície a certifikácie ochranného profilu, ktorý sa stane neoddeliteľnou súčasťou povinných požiadaviek pre túto schému a bude tvoriť neoddeliteľnú prílohu k schéme. Silná motivácia na zahrnutie súvisiacich certifikovaných produktov do rozsahu vzájomného posudzovania umožní vzájomnú kontrolu metodiky, nástrojov a zručností používaných na hodnotenie týchto produktov a ešte lepšiu pozíciu na ďalšie definovanie technických domén odvodených od týchto špecifických PP.

5. POSUDZOVANIE ZHODY SAMOHODNOTENÍM

ODKAZ (-Y) NA ČLÁNOK(-KY) CSA

Článok 54 1. *Európska schéma certifikácie kybernetickej bezpečnosti obsahuje aspoň tieto prvky:*

e) údaj o tom, či je v rámci schémy povolené posudzovanie zhody samohodnotením.

Schéma EUCC neumožňuje *posudzovanie* zhody *samohodnotením*.

ZÁKLADNÉ INFORMÁCIE

Schéma sa nevzťahuje na základnú úroveň záruky CSA, ktorá je jedinou úrovňou, ktorá umožňuje posudzovanie zhody samohodnotením v súlade s článkom 53.1 CSA.

Okrem toho sa v § 8.2.3 CEM vyžaduje oddelenie úloh (napr. zadávateľa, hodnotiteľa, orgánu hodnotenia), aby sa zabránilo nevhodnému ovplyvňovaniu hodnotenia.

6. ŠPECIFICKÉ POŽIADAVKY VZŤAHUJÚCE SA NA CAB

ODKAZ (-Y) NA ČLÁNOK(-KY) CSA

Článok 54 1. *Európska schéma certifikácie kybernetickej bezpečnosti obsahuje aspoň tieto prvky:*

f) prípadne špecifické alebo dodatočné požiadavky, ktorým podliehajú orgány posudzovania zhody, aby sa zaručila ich odborná kompetentnosť posudzovať požiadavky kybernetickej bezpečnosti.

Príloha, POŽIADAVKY, KTORÉ MUSIA SPLNIŤ ORGÁNY POSUDZOVANIA ZHODY:

19. Orgány posudzovania zhody musia spĺňať požiadavky príslušnej normy harmonizovanej podľa nariadenia (ES) č. 765/2008 na akreditáciu orgánov posudzovania zhody vykonávajúcich certifikáciu produktov IKT, služieb IKT alebo procesov IKT.

20. Orgány posudzovania zhody zabezpečia, aby skúšobné laboratóriá používané na účely posudzovania zhody spĺňali požiadavky príslušnej normy harmonizovanej podľa nariadenia (ES) č. 765/2008 na akreditáciu laboratórií vykonávajúcich skúšky.

V súlade s prílohou CSA musí byť certifikačný orgán (CB) akreditovaný podľa príslušnej normy ISO/IEC 17065. Okrem toho musí mať autorizáciu od svojej NCCA na vydávanie certifikátov na úrovni záruky "vysoká" podľa CSA.

Skúšobné laboratórium (ITSEF) vrátane jeho zamestnancov vykonávajúcich hodnotenia pre certifikačný orgán, či už ide o interné skúšobné laboratórium orgánu posudzovania zhody alebo externé skúšobné laboratórium v prípade, že skúšky vykonáva subdodávateľ, musí byť odborne kompetentné na príslušné úlohy.

V prípade úroveň záruky "významná" sa táto odborná kompetentnosť posudzuje prostredníctvom akreditácie skúšobného laboratória podľa ISO/IEC 17025 pre hodnotenia podľa ISO/IEC 18045 v spojení s ISO/IEC 15408.

Agentúra ENISA môže s podporou Európskej spolupráce pre akreditáciu a v spolupráci s ECCG poskytnúť usmernenia pre harmonizovaný výklad normy ISO/IEC 17025 pre schému EUCC, pričom zohľadní súvisiace normy, ako je ISO/IEC 19896-3.

Pre úroveň záruky "vysoká" sa v schéme EUCC okrem akreditácie skúšobného laboratória podľa normy ISO/IEC 17025 stanovujú tieto osobitné požiadavky, ktorým podliehajú orgány posudzovania zhody, aby sa zaručila ich odborná kompetentnosť posudzovať požiadavky kybernetickej bezpečnosti:

- špecifické požiadavky sa týkajú odbornej kompetentnosti súvisiacej s konkrétnymi skúšobnými činnosťami a uplatňujú sa len na certifikáty vydané na úrovni záruky "vysoká";
- požiadavky sa vzťahujú na interné skúšobné laboratóriá orgánov posudzovania zhody, ako aj na externé laboratóriá v prípadoch, keď skúšky vykonáva subdodávateľ.

Od týchto ITSEF a ich príslušných pracovníkov sa vyžaduje, aby spĺňali tieto požiadavky:

(a) mať potrebné odborné znalosti a skúsenosti s vykonávaním špecifických testovacích činností na určenie odolnosti produktu voči špecifickým útokom (penetračné testovanie) za predpokladu potenciálu útoku "rozšírená-základná", ako je opísané v CC (AVA_VAN.3 Zameraná analýza zraniteľnosti).

(b) Pre technické domény definované v kapitole 8, ŠPECIFICKÉ KRITÉRIA A METÓDY HODNOTENIA:
- mať potrebné odborné znalosti a skúsenosti s vykonávaním špecifických testovacích činností potrebných na metodické určenie odolnosti produktu voči útokom vykonávaným v prevádzkovom prostredí produktu za predpokladu zodpovedajúceho potenciálu útoku "stredný" alebo "vysoký", ako je opísané v CC (AVA_VAN.4 Metodická analýza zraniteľnosti, AVA_VAN.5 Pokročilá metodická analýza zraniteľnosti);
- byť schopný preukázať tieto špecifické odborné kompetentnosti:
  - pre technickú doménu "smart karty a podobné zariadenia" požadované spôsobilosti

prílohy 8;

- pre technickú doménu "Hardvérové zariadenia s bezpečnostnými skrinkami" požadované spôsobilosti z prílohy 10.

ZÁKLADNÉ INFORMÁCIE

Požiadavky, ktoré sa vzťahujú na CB v súvislosti s ich schopnosťou vydávať certifikáty, sú tu len zhrnuté, pretože sú už definované vo všeobecných podmienkach CSA.

SOG-IS MRA a CCRA požadujú ako základ akreditáciu podľa normy ISO/IEC 17025 pre ITSEF, ktoré vykonávajú hodnotenia. To sa považuje za dostatočné pre úroveň "významná", ktorá je spojená s AVA_VAN.1 a 2, podľa opisu mapovania hodnotenia úrovní v kapitole 4, ÚROVNE ZÁRUKY.

Mohla by však byť potrebná vzájomne schválená interpretácia akreditačných noriem pre činnosti certifikačných a skúšobných laboratórií, ktorá by sa potom mala definovať ako usmernenie pre schému (s podporou európskej spolupráce v oblasti akreditácie). Agentúra ENISA môže v spolupráci s ECCG navrhnúť súvisiace vylepšenia, pričom by sa mali opätovne využiť skúsenosti rôznych členov SOG-IS MRA, ktorí takéto výklady vypracovali, a použiť tieto potenciálne relevantné normy:

- ISO/IEC 19896, Požiadavky na kompetentnosť testerov a hodnotiteľov informačnej bezpečnosti, najmä:
  - Časť 1: Úvod, koncepty a všeobecné požiadavky
  - Časť 3: Požiadavky na znalosti, zručnosti a efektívnosť hodnotiteľov CC
- ISO/IEC 2nd WD 23532-1, Požiadavky na kompetentnosť laboratórií na testovanie a hodnotenie bezpečnosti IT, najmä:
  - Časť 1: Hodnotenie pre CC

POZNÁMKA: Norma ISO/IEC 19896-3 poskytuje požiadavky na kompetentnosť hodnotiteľov CC, ktoré možno použiť ako podporu v procese hodnotenia. Zaoberá sa však len základnými metodickými kompetenciami a nerieši spôsob hodnotenia technologicky špecifických znalostí a zručností, ako sú tie, ktoré sa vyžadujú na vykonanie hodnotenia ADV, ATE alebo AVA_VAN na danom type produktu, ani sektorové znalosti, ktoré sa zvyčajne vyžadujú na vykonanie hodnotenia ASE, APE alebo ACE. Okrem toho si špecifické zručnosti vyžadované pri hodnotení CC môžu vyžadovať ďalšie metódy hodnotenia kompetentnosti. Napríklad na hodnotenie zručností súvisiacich s formálnymi metódami.

Na posúdenie schopností ITSEF vykonávať hodnotenia na úrovni AVA_VAN.3 nebol doteraz stanovený žiadny podrobný harmonizovaný rámec, hoci certifikačné orgány pri tomto posudzovaní vo všeobecnosti postupujú podľa:

- skúsenosti ITSEF a príslušného personálu;
- ich schopnosti na určenie odolnosti produktu voči konkrétnym útokom (penetračné testovanie) za predpokladu potenciálu útoku "rozšírený-základný", ako je opísané v CC (AVA_VAN.3 Zameraná analýza zraniteľností);
- potrebných rozhovoroch a/alebo testoch hodnotiteľov a prípadné podrobné monitorovanie pilotných hodnotení na uvažovanej úrovni zo strany CB.

V dôsledku toho sa má harmonizácia spôsobu vykonávania tohto hodnotenia pre túto prvú verziu schémy EUCC dosiahnuť prostredníctvom mechanizmov vzájomného preskúmania a vzájomného posudzovania a agentúra ENISA môže v spolupráci s ECCG ďalej vypracovať usmernenia založené na týchto vzájomných preskúmaniach/posudzovaniach.

Pre každú technickú doménu stanovil SOG-IS MRA osobitné požiadavky, ktoré musí ITSEF spĺňať, aby mohol byť vyhlásený za spôsobilého vykonávať takéto hodnotenia:

- Minimálne požiadavky ITSEF na hodnotenie bezpečnosti smart kariet a podobných zariadení v prílohe 8;
- Minimálne požiadavky ITSEF na hodnotenia bezpečnosti hardvérových zariadení s bezpečnostnými skrinkami v prílohe 10,

Príklady v rámci prílohy 8, ktoré požiadavky sú zakotvené pre hodnotiteľov IC z hľadiska zručností a vedomostí v týchto technických doménach:

- porozumenie návrhu bezpečného integrovaného obvodu (ako je smart karta, bezpečný prvok atď.) a výrobného procesu vo všeobecnosti návrhu a výroby integrovaného obvodu;

- pochopenie technológie bezpečných integrovaných obvodov, jej základných princípov a vývojových zariadení používaných výrobcami bezpečných integrovaných obvodov;
- pochopenie bezpečného ekosystému založeného na integrovaných obvodoch s dobrými znalosťami súvisiacich hrozieb a techník útokov.
- znalosti a skúsenosti v oblasti techník fyzického útoku na hardvér, ktoré by mohli ohroziť zabezpečený integrovaný obvod, a schopnosť používať súvisiace zariadenia na zaťaženie hardvérových vrstiev. To zahŕňa pochopenie základných fyzikálnych princípov IC;
- znalosti a skúsenosti s fyzickými narušeniami, ktoré by mohli zmeniť bezpečné správanie integrovaného obvodu s cieľom následne znížiť bezpečnosť zariadenia založeného na integrovanom obvode. Schopnosť používať súvisiace zariadenia na vykonávanie fyzických narušení a pochopenie súvisiacich fyzických účinkov na hardvér;
- znalosti a skúsenosti v oblasti techník kryptografických útokov a schopnosť vykonávať analýzu (vrátane postupov zachytávania údajov a spracovania signálov).

Okrem toho sa v prípade ostatných technických domén definovaných pre schému EUCC na zručnosti a znalosti hodnotiteľov týkajúce sa logickej architektúry vzťahujú tieto požadované schopnosti pre zložené hodnotenia:

- revízia zdrojového kódu, špecifikácie rozhraní (natívnych aj protokolov), správa obsahu a zdrojov;
- aspekty integrácie dodávateľského reťazca v prostredí aplikácie;
- kryptografický softvér s použitím špecializovaného hardvéru alebo bez neho;
- virtuálne počítače;
- útoky súvisiace so softvérom.

7. NOTIFIKÁCIA A AUTORIZÁCIA CAB, FUNGOVANIE CAB A SUBDODÁVATEĽOV

ODKAZ (-Y) NA ČLÁNOK(-KY) CSA

Článok 2.18: *"orgán posudzovania zhody" je orgán posudzovania zhody vymedzený v článku 2 bode 13 nariadenia (ES) č. 765/2008.*

Článok 54 ods. 1 písm. f): *prípadne špecifické alebo dodatočné požiadavky, ktorým podliehajú orgány posudzovania zhody s cieľom zaručiť ich odbornú kompetentnosť na posudzovanie požiadaviek kybernetickej bezpečnosti.*

Článok 56.6.: *Ak európska schéma certifikácie kybernetickej bezpečnosti prijatá podľa článku 49 vyžaduje úroveň záruky "vysoká", európsky certifikát kybernetickej bezpečnosti podľa tejto schémy vydáva len národná autorita pre certifikáciu kybernetickej bezpečnosti alebo v nasledujúcich prípadoch orgán posudzovania zhody:*

(a) národná autorita pre certifikáciu kybernetickej bezpečnosti najprv schváli každý jednotlivý európsky certifikát kybernetickej bezpečnosti, ktorý vydal orgán posudzovania zhody, alebo

(b) národná autorita pre certifikáciu kybernetickej bezpečnosti poverila úlohou vydávať takéto európske certifikáty kybernetickej bezpečnosti orgán posudzovania zhody na základe všeobecného delegovania.

Článok 60.2.: *Ak národná autorita pre certifikáciu kybernetickej bezpečnosti vydala v súlade s článkom 56 ods. 5 písm. a) a článkom 56 ods. 6 európsky certifikát kybernetickej bezpečnosti, certifikačný orgán národnej autority pre certifikáciu kybernetickej bezpečnosti sa akredituje ako orgán posudzovania zhody podľa odseku 1 tohto článku.*

Článok 60.3.: Ak sa v európskych schémach certifikácie kybernetickej bezpečnosti stanovujú osobitné alebo dodatočné požiadavky podľa článku 54 ods. 1 písm. f), národná autorita pre certifikáciu kybernetickej bezpečnosti autorizuje na vykonávanie úloh podľa týchto schém len tie orgány posudzovania zhody, ktoré spĺňajú uvedené požiadavky.

Nariadenie 765/2008.13: "orgán posudzovania zhody" je orgán, ktorý vykonáva činnosti posudzovania zhody vrátane kalibrácie, skúšania, certifikácie a inšpekcie.

Notifikácia

Pre každý CAB vydávajúci certifikáty (označený ako certifikačný orgán alebo CB podľa slovníka pojmov), ktorý je notifikovaný v súlade s článkom 61 CSA, notifikácia obsahuje:

- stanovenú úroveň záruky CSA ("významná" alebo "vysoká");
- ak je úroveň záruky CSA "vysoká", úroveň AVA_VAN, do ktorej môže CB vydávať certifikáty, a prípadne technické domény, pre ktoré sa certifikácia ponúka;
- prípadne zoznam ITSEF, ktoré vykonávajú hodnotenia pre CB, vrátane úrovne AVA_VAN, do ktorej môže každý ITSEF hodnotiť, a prípadne technické domény, pre ktoré sa hodnotenie ponúka.

Autorizácia

NCCA autorizuje CAB vykonávať úlohy v rámci schémy EUCC. Na tento účel musí posúdiť schválenia CAB, vykonávané v súlade so špecifickými požiadavkami opísanými v kapitole 6 ŠPECIFICKÉ POŽIADAVKY VZŤAHUJÚCE SA NA CAB, interného skúšobného laboratória (ITSEF) tohto CAB a v prípadoch, keď skúšky vykonáva subdodávateľ, externého skúšobného laboratória (ITSEF).

Toto hodnotenie môže pre každý ITSEF zahŕňať:

- vykonanie štruktúrovaných rozhovorov s cieľom zistiť, či ITSEF a jeho zamestnanci majú potrebné odborné znalosti a skúsenosti v príslušných činnostiach;
- preskúmanie dôkazov dvoch pilotných hodnotení, ktoré vykonal ITSEF v rámci schvaľovacieho

postupu CAB, a zhodnotenie ich výkonu.

V prípadoch, keď testovanie vykonáva subdodávateľ, autorizované certifikačné orgány poskytujú svojej NCCA potrebnú technickú podporu pri posudzovaní ITSEF a pravidelne (minimálne raz za dva (2) roky) sa zúčastňujú na ich audite.

Táto podpora zahŕňa aj posúdenie, či ITSEF spĺňajú prísne bezpečnostné požiadavky potrebné na ochranu citlivých alebo chránených informácií týkajúcich sa hodnotených produktov IKT alebo ochranných profilov a samotného procesu hodnotenia, ako sa vyžaduje v kapitole 24, ĎALŠIE PRVKY SCHÉMY.

Pokiaľ to nie je riadne odôvodnené, autorizované CB a pridružené ITSEF sa zúčastňujú na údržbe schémy a poskytujú mu technickú podporu.

Pri vypracovaní žiadosti o certifikáciu podľa tejto schémy na úrovni záruky "vysoká" CSA sa výrobca alebo poskytovateľ môže poradiť s ktorýmkoľvek ITSEF pridruženým k autorizovanému CAB o dostupnosti a odhade zdrojov a nákladov na hodnotenie a môže uzavrieť zmluvu priamo s jedným alebo viacerými z týchto ITSEF. Uplatňujú sa však tieto určenia:

- uzavrie zmluvu len s ITSEF, ktorý bol riadne oznámený CB na príslušnej úrovni;
- ITSEF informuje CB o zdrojoch (človekodňoch) pridelených na hodnotenie;
- CB zostáva hlavným zodpovedným orgánom za výsledný certifikát.

Uzatváranie subdodávateľských zmlúv a využívanie zariadení tretích strán

Subdodávky sú povolené v súlade s požiadavkami stanovenými v akreditačných normách, ktoré sa vzťahujú na činnosti CB a ITSEF, t. j. ISO/IEC 17065 a ISO/IEC 17025.

ITSEF, ktorý sa považuje za spôsobilý pre technickú doménu, môže zadať svoju prácu subdodávateľom v rámci technickej domény len za týchto podmienok:

- činnosti prevezme iba ITSEF príslušný pre danú technickú doménu;
- ďalšie uzatváranie subdodávateľských zmlúv je možné len so súhlasom CB, NCCA a výrobcu alebo poskytovateľa produktu IKT;
- činnosti sa vykonávajú pod plnou kontrolou a zodpovednosťou subdodávateľského ITSEF;
- je povolené len zadávanie čiastočných činností AVA_VAN subdodávateľom.

Ďalšie uzatváranie subdodávateľských zmlúv nesmie mať vplyv na dôvernosť, objektívnosť alebo nestrannosť hodnotiacich činností v súlade s požiadavkami odsekov 7, 9 a 16 prílohy k dohode o partnerstve. Uvedený súhlas CB si vyžaduje, aby ITSEF a jeho subdodávateľ dodali potrebný obsah na posúdenie, či je subdodávateľ schopný splniť všetky potrebné požiadavky.

Ak ITSEF využíva iné zariadenia (napr. tretie strany nezávislé od ITSEF aj od spoločnosti(-í) vyvíjajúcej(-ich) a vyrábajúcej(-ich) TOE), uplatňujú sa vhodné bezpečnostné opatrenia na ochranu informácií a vzoriek dodávateľa a know-how ITSEF. To si môže vyžadovať dodatočné opatrenia, ak by TOE musel zostať v zariadení tretej strany bez dozoru. To si môže vyžadovať aj dôkladné zváženie získania opakovateľnosti výsledkov testov, ak bola vzorka odstránená z miesta alebo sa zmenili nastavenia zariadenia pred dokončením analýzy TOE.

Využitie zariadenia tretej strany sa uvedie v pláne hodnotenia a schváli ho výrobca alebo poskytovateľ a CB, pričom ITSEF zostáva zodpovedný za vykonanú prácu.

Ak ITSEF používa v zariadení tretej strany zariadenie na mieru, hodnotiteľ musí byť prítomný a inštruovať obsluhujúci personál. Na inštruktáž prevádzkového personálu musí mať hodnotiteľ dostatočné znalosti o TOE, zariadení a účele testu.

ZÁKLADNÉ INFORMÁCIE

Certifikačná schéma sa spolieha na viacero činností vrátane certifikačných a hodnotiacich činností. Vzhľadom na to, že CB môže svoje hodnotiace činnosti vo veľkej miere zadávať externým dodávateľom, najmä na úrovni záruky "vysoká", notifikácia umožňuje uvádzať úroveň, ktorú môže každý jednotlivý člen dosiahnuť, a pri udeľovaní autorizácie plne zohľadniť základné schopnosti ITSEF.

Tým sa umožní potrebná hospodárska súťaž, a teda žiadatelia budú môcť konzultovať a vybrať si subdodávateľa(-ov) podľa vlastného výberu za podmienok vymedzených v tomto oddiele.

Pri posudzovaní ITSEF by sa mali zapojiť odborné zručnosti CB a mali by byť prínosom pre ich NCCA.

8. ŠPECIFICKÉ KRITÉRIÁ HODNOTENIA A METÓDY

ODKAZ (-Y) NA ČLÁNOK(-KY) CSA

Článok 54 1. *Európska schéma certifikácie kybernetickej bezpečnosti obsahuje aspoň tieto prvky*

g) špecifické kritériá hodnotenia a metódy, ktoré sa majú použiť, vrátane typov hodnotenia, aby sa preukázalo, že sa dosiahli bezpečnostné ciele uvedené v článku 51.

Okrem niektorých špecifických ustanovení tejto schémy CC výrazne prispieva k plneniu bezpečnostných cieľov definovaných v článku 51 CSA. Deje sa tak prostredníctvom výberu príslušných komponentov
v rámci nasledujúcich tried/skupín katalógu požiadaviek bezpečnostných funkcionalít (SFR)
a požiadaviek bezpečnostných záruk (SAR):

***Tabuľka 4:** Kandidátsky SFR a/alebo SAR na splnenie bezpečnostných cieľov definovaných v článku 51*

Bezpečnostné ciele definované v Článku 51	Kandidátske triedy/skupiny SFR a/alebo SAR z CC
(a) chrániť uložené, prenášané alebo inak spracované údaje pred náhodným alebo neoprávneným uložením, spracovaním, prístupom alebo zverejnením počas celého životného cyklu produktu IKT, služby IKT alebo procesu IKT;	- SFR Trieda FCO: Komunikácia - SFR Trieda FCS: FCS_COP: kryptografická operácia - SFR Trieda FDP: FDP_UCT: Ochrana dôvernosti prenosu používateľských údajov medzi jednotlivými FSF
(b) chrániť uložené, prenášané alebo inak spracúvané údaje pred náhodným alebo neoprávneným zničením, stratou alebo zmenou alebo nedostatočnou dostupnosťou počas celého životného cyklu produktu IKT, služby IKT alebo procesu IKT;	- SFR Trieda FDP: FDP_SDI: Integrita uložených údajov a Skupina SFR FDP_UIT: Ochrana prenosu integrity používateľských údajov medzi TF - SFR Skupina FCS_COP: Kryptografická operácia
(c) aby oprávnené osoby, programy alebo stroje mali prístup len k údajom, službám alebo funkciám, na ktoré sa vzťahujú ich prístupové práva;	- SFR Trieda FDP: FDP_SDI: Integrita uložených údajov a skupina SFR FDP_UIT: Ochrana prenosu integrity používateľských údajov medzi TF - SFR Skupina FCS_COP: Kryptografická operácia - SFR Skupina FMT_MSA Správa bezpečnostných atribútov - SFR Skupina FMT_SMF Špecifikácia funkcií riadenia
(d) identifikovať a zdokumentovať známe závislosti a zraniteľnosti;	- SFR Trieda FDP: Ochrana údajov používateľa - SAR Skupina ALC_FLR: Náprava chýb - SAR Skupiny ALC_CMS: CM Rozsah pôsobnosti - SAR Trieda ASE: Bezpečnostný zámer
(e) zaznamenávať, ku ktorým údajom, službám alebo funkciám sa pristupovalo, ktoré sa používali alebo inak spracúvali, v akom čase a kto ich spracúval;	- Trieda SFR FAU: Bezpečnostný audit vrátane skupiny SFR FAU_GEN: Generovanie údajov bezpečnostného auditu - SFR Trieda FTA: prístup k TOE
(f) umožniť kontrolu toho, ku ktorým údajom, službám alebo funkciám sa pristupovalo, ktoré sa používali alebo inak spracúvali, v akom čase a kto ich spracúval;	- SFR Trieda FAU: Bezpečnostný audit vrátane SFR Skupiny FAU_SAR: Preskúmanie údajov bezpečnostného auditu - SFR Skupina FMT_MSA Správa bezpečnostných atribútov - SFR Skupina FMT_SMF Špecifikácia funkcií riadenia
(g) overiť, či produkty IKT, služby IKT a procesy IKT neobsahujú známe zraniteľnosti;	- SAR Trieda AVA: posúdenie zraniteľnosti vrátane skupiny SAR AVA_VAN: analýza zraniteľnosti
(h) včasné obnovenie dostupnosti a prístupu k údajom, službám a funkciám v prípade fyzického alebo technického incidentu;	- SFR Trieda FPT ochrana FPT vrátane SFR Skupiny FPT_RCV: dôveryhodné obnovenie
(i) aby produkty IKT, služby IKT a procesy IKT boli štandardne a dizajnovo bezpečné;	- SAR Skupina ALC_TAT: Nástroje a techniky - SAR Skupina ADV_ARC: Bezpečnostná architektúra - SAR Skupina ADV_TDS: TOE Design - SAR Skupina ASE_SPD: Definícia bezpečnostného problému

Bezpečnostné ciele definované v článku 51	Kandidátske triedy/skupiny SFR a/alebo SAR z CC
(j) aby produkty IKT, služby IKT a procesy IKT boli vybavené aktuálnym softvérom a hardvérom, ktoré neobsahujú verejne známe zraniteľnosti, a aby boli vybavené mechanizmami bezpečných aktualizácií.	- SAR Trieda AVA: Posúdenie zraniteľnosti - SAR Skupina ALC_FLR: Náprava chýb

V súlade s CC sa môžu v prípade potreby definovať rozšírené komponenty existujúceho katalógu SFR a SAR, aby lepšie vyhovovali uvedeným cieľom v konkrétnom produkte IKT.

Používateľ certifikovaných produktov alebo žiadateľ o certifikáciu sa rozhodne, na základe ktorých bezpečnostných cieľov sa rozhodne hodnotiť produkt(-y) IKT, a vyberie príslušné požiadavky buď v ochrannom profile, alebo v bezpečnostnom zámere jednotlivých produktov IKT. Agentúra ENISA môže
v spolupráci s ECCG poskytnúť súvisiace usmernenia pre tento výber na základe metód alebo nástrojov posudzovania rizík.

Štandardne sa však každé hodnotenie zakladá na použití SAR triedy AVA: Posúdenie zraniteľnosti a SAR skupiny ALC_FLR: Odstránenie chýb, aby sa zabezpečilo, že produkty IKT sú vybavené aktuálnym softvérom a hardvérom, ktoré neobsahujú verejne známe zraniteľnosti, a sú vybavené mechanizmami na bezpečné aktualizácie.

Ako je uvedené v kapitole 3, NORMY POUŽITÉ PRI HODNOTENI, dve platné normy pre hodnotenie, ISO/IEC 15408 a ISO/IEC 18405, sú podporené povinnými podpornými prvkami a podpornými dokumentmi s usmerneniami:

- Povinné podporné prvky sú opísané v prílohách tohto dokumentu a sú určené na povinné použitie (rozsah ich použitia však môže byť obmedzený). Obsahujú konzistentný súbor výkladov, ktoré špecifikujú použitie kritérií a metodiky v rámci konkrétnej oblasti alebo technologickej domény, a musia sa používať, ak je to relevantné. V technickej správe z hodnotenia a správe z certifikácie sa uvádza, ktoré povinné podporné prvky boli použité;
- Vysvetľujúce podporné dokumenty obsahujú nezáväzné rady a odporúčania, ktorých používanie nie je povinné, hoci sa to odporúča. Cieľom vysvetľujúcich dokumentov je, aby vývojári, hodnotitelia a vydavatelia certifikátov zlepšili proces hodnotenia a certifikácie. Vysvetľujúce dokumenty môžu obsahovať podkladový materiál na podporu pochopenia prístupu k hodnoteniu alebo akékoľvek iné informácie a nevyplývajú z nich žiadne povinnosti pre žiadneho zo zúčastnených aktérov. Ak sú však relevantné pre produkty IKT, ktoré sa majú certifikovať, vždy sa zváži možnosť odkazovať na ne a použiť ich pri hodnotení.

Povinné podporné prvky môžu byť určené na skúšobné používanie na určité obdobie: v prípade potreby sa takýto stav uvedie, ako aj príslušné obdobie skúšobného používania.

Cieľom obdobia skúšobného používania je získať skúsenosti s uplatňovaním požiadaviek prvkov v kontexte hodnotenia produktu. Uplatňovanie prvkov skúšobného používania je povinné pre certifikáciu príslušných produktov IKT, ale počas obdobia skúšobnej fázy sa môže v jednotlivých prípadoch stať, že na výklad prvkov skúšobného používania bude potrebná dodatočná podpora zo strany orgánu alebo subjektu zodpovedného za certifikáciu, ak by sa vyskytli problémy s ich uplatňovaním.

Ak sa počas fázy skúšobného používania zistia potrebné výklady, zdieľajú ich špecializované štruktúry ECCG, ktoré budú podporovať udržiavanie schémy s cieľom zlepšiť prvky v ďalšej verzii príslušnej dokumentácie, a ECCG stanoví, ktoré prvky môže ENISA poskytnúť na svojej webovej stránke pred prijatím akejkoľvek formálnej revízie dokumentácie.

Všetky vysvetľujúce dokumenty na podporu tejto schémy sa vypracujú v spolupráci s ECCG a uverejnia sa na webovej stránke agentúry ENISA venovanej certifikácii kybernetickej bezpečnosti.

Nasledujúce prvky sa uplatňujú ako povinné podporné prvky, ktoré sa používajú pri hodnotení produktov IKT bez ohľadu na typ produktov IKT alebo ich úroveň záruky:

- Príloha 1, ktorá obsahuje podmienky pre vyhlásenie o balíku záruky v certifikáte.

Nasledujúce dve technické domény umožňujú certifikáciu produktov IKT súvisiacich s technológiami na úrovniach záruky AVA_VAN.4 a AVA_VAN.5 za predpokladu, že sa na ich hodnotenie použijú špecifické dodatočné metódy, techniky a nástroje. Tieto technické domény sú:

- Smart karty a podobné zariadenia - kde významná časť požadovanej bezpečnostnej funkcionality závisí od hardvérových funkcií na úrovni integrovaných obvodov (napr. hardvér/IC smart kariet, zložené produkty smart kariet, TPM[6] používané v dôveryhodných počítačoch, karty digitálnych tachografov atď.)
- Hardvérové zariadenia s bezpečnostnými skrinkami - kde významná časť požadovanej bezpečnostnej funkcionality závisí od hardvérového fyzického obalu s protiopatreniami (tzv. "bezpečnostná skrinka") proti priamym fyzickým útokom (napr. platobné terminály, tachografy vo vozidlách, smart merače, taxametre, terminály kontroly prístupu, hardvérové bezpečnostné moduly atď.).

Poznámka: V prípadoch, keď sa požiadavky na fyzickú ochranu ("bezpečnostnú skrinku") definované v ochrannom profile vypracovanom normalizačným orgánom uznaným EÚ líšia od požiadaviek všeobecne platných v danej oblasti (či už sú väčšie alebo menšie), majú prednosť požiadavky PP a súvisiaca metodika.

Nasledujúce prvky sa uplatňujú ako povinné podporné prvky pre hodnotenie produktov IKT súvisiacich s týmito technickými doménami:

- pre obe technické domény, príloha 2, ktorá obsahuje minimálne bezpečnostné požiadavky na lokalitu;
- pre technickú doménu smart karty a podobné zariadenia, ďalšie metódy, techniky a nástroje hodnotenia zahrnuté v:
  - Príloha 3, ktorá obsahuje podmienky týkajúce sa uplatňovania CC na integrované obvody;
  - Príloha 4, ktorá obsahuje požiadavky na bezpečnostnú architektúru (ADV_ARC) pre smart karty a podobné zariadenia;
  - Príloha 5, ktorá obsahuje podmienky týkajúce sa certifikácie produktov "otvorených" smart kariet
  - Príloha 6, ktorá obsahuje podmienky týkajúce sa hodnotenia zložených produktov pre smart karty a podobné zariadenia;
  - Príloha 7, ktorá obsahuje podmienky týkajúce sa uplatňovania potenciálu útoku na smart karty;
  - Príloha 8, ktorá obsahuje minimálne požiadavky na ITSEF pri hodnotení bezpečnosti smart kariet a podobných zariadení;
- pre technickú doménu Hardvérové zariadenia s bezpečnostnými skrinkami, ďalšie metódy hodnotenia, techniky a nástroje zahrnuté v:
  - Príloha 9, ktorá obsahuje podmienky týkajúce sa uplatňovania potenciálu útoku na HW zariadenia s bezpečnostnými skrinkami;
  - Príloha 10, ktorá obsahuje minimálne požiadavky na ITSEF pri hodnotení bezpečnosti hardvérových zariadení s bezpečnostnými skrinkami.

V iných kapitolách tohto dokumentu sa môže požadovať uplatnenie ďalších povinných podporných prvkov na podporu požiadaviek súvisiacich so schémou EUCC. Tieto prvky sa tiež uvádzajú v prílohách k tejto schéme.

Ak sa produkt IKT podrobuje hodnoteniu zloženého produktu, citlivé informácie sa vymieňajú medzi fórom ITSEF, ktorý pristúpil k hodnoteniu, ktorého výsledky sa opätovne použijú, a fórom ITSEF, ktorý pristúpil k hodnoteniu zloženého produktu. Toto zdieľanie informácií sa uskutočňuje prostredníctvom štruktúrovanej dokumentácie, technickej správy o hodnotení (ETR) zloženého produktu. Agentúra ENISA poskytne vzor ETR[7].

ZÁKLADNÉ INFORMÁCIE

Mapovanie medzi bezpečnostnými cieľmi definovanými v článku 51 CSA a vybranými triedami SFR alebo SAR možno ďalej kontrolovať prostredníctvom preskúmania CC. Agentúra ENISA môže v spolupráci s ECCG poskytnúť podporný vysvetľujúci dokument k tomuto mapovaniu.

Na podporu potrebného vývoja a evolúcie povinných podporných prvkov bola zavedená koncepcia skúšobného používania. Umožňuje na určité obdobie overiť platnosť požiadaviek, ktoré stanovujú, pričom možnosť odchýliť sa a stále certifikovať a potom informovať spoločenstvo o potrebných úpravách, skôr ako sa podporné prvky začnú plne uplatňovať.

---

[6] Moduly dôveryhodnej platformy.

[7] https://www.sogis.eu/documents/cc/domains/sc/JIL-ETR-template-for-composition-v1-1.pdf je aktuálne platná šablóna pre hodnotenia súvisiace s SOG-IS MRA, ktorá môže slúžiť ako technický základ pre šablónu ETR schémy EUCC pre zloženie.

Technické domény boli vytvorené na základe týchto charakteristík:

- v technológiách, na ktoré sa vzťahuje rozsah pôsobnosti smart kariet a podobných zariadení, bude útočník často schopný získať fyzický prístup k zariadeniu (alebo k súboru zariadení); zariadenie môže obsahovať kritické informácie, ako sú bezpečnostné prístupové údaje/kľúče, a časť bezpečnostných funkcií požadovaných od zariadenia sa bude týkať vlastnej ochrany buď aktívnymi (detekcia neoprávnenej manipulácie), alebo pasívnymi prostriedkami (ako sú nátery odolné voči neoprávnenej manipulácii). To je v protiklade so štandardným viacúčelovým hardvérom, ktorý sa používa vo všeobecných zariadeniach na spracovanie údajov (napríklad v PC).

Prístup k hodnoteniu musí zohľadňovať všetky hardvérovo špecifické aspekty analýzy zraniteľnosti vrátane tých, ktoré si vyžadujú značné dodatočné vybavenie a zdroje. Takéto zariadenia sú často zložené z prvkov vyrobených rôznymi vývojármi (napr. hardvér, operačný systém smart karty a aplikácia) a môžu zahŕňať výrobu na rôznych vývojových miestach (napr. návrh integrovaného obvodu, výroba masky, výroba, charakterizácia atď.) Tieto faktory sa musia dôsledne zohľadňovať aj pri hodnotení a certifikácii.

- v technológiách, na ktoré sa vzťahuje rozsah pôsobnosti pre hardvérové zariadenia s bezpečnostnými skrinkami, bude útočník často schopný získať fyzický prístup k zariadeniu (alebo k súboru zariadení). Zariadenie môže obsahovať kritické informácie, ako sú bezpečnostné prístupové údaje/kľúče, alebo by sa mohlo používať aj na bezpečné zadávanie prístupových údajov/kľúčov a významná časť bezpečnostnej funkcie požadovanej od zariadenia sa bude týkať vlastnej ochrany proti fyzickým útokom. Tieto protiopatrenia vlastnej ochrany alebo "bezpečnostná skrinka" takýchto zariadení pozostáva z protiopatrení fyzickej ochrany založených na hardvérových a softvérových aktívnych mechanizmoch. Zvyčajne tieto mechanizmy zahŕňajú aj pasívnu ochranu ako neoddeliteľnú súčasť poskytovanej bezpečnostnej funkcie (napr. kovové štíty alebo pancierovanie, drôtené pletivo, chemická ochrana, ako je epoxidová živica atď.) v spojení so senzormi a elektronickými mechanizmami proti neoprávnenej manipulácii (ako je bezpečné vymazanie údajov, generovanie alarmu alebo núdzové zničenie komponentov).

Prístup k hodnoteniu musí zohľadňovať všetky softvérové, firmvérové a hardvérové špecifické aspekty analýzy zraniteľnosti vrátane tých, ktoré si môžu vyžadovať značné dodatočné vybavenie a zdroje. Takéto zariadenia sa často skladajú aj z diskrétnych častí vyrobených rôznymi vývojármi. Aj tieto faktory sa musia dôsledne zohľadniť počas hodnotenia a certifikácie.

9. INFORMÁCIE POTREBNÉ NA CERTIFIKÁCIU

ODKAZ (-Y) NA ČLÁNOK(-KY) CSA

Článok 54 1. *Európska schéma certifikácie kybernetickej bezpečnosti obsahuje aspoň tieto prvky:*

h) prípadne informácie, ktoré sú potrebné na certifikáciu a ktoré má žiadateľ poskytnúť alebo inak sprístupniť orgánom posudzovania zhody.

Článok 55 *Doplňujúce informácie o kybernetickej bezpečnosti certifikovaných produktov IKT, služieb IKT a procesov IKT*

Každý žiadateľ poskytne orgánu posudzovania zhody informácie potrebné na hodnotenie kybernetickej bezpečnosti.

To musí zahŕňať všetky relevantné dôkazy, ako sa vyžaduje v rámci *prvkov činnosti vývojára,* a v príslušnom formáte, ako sa vyžaduje v *prvkoch obsahu a prezentácie,* podľa časti 3 CC pre zvolenú úroveň záruky a súvisiace požiadavky bezpečnostných záruk. Dôkazy musia v prípade potreby obsahovať podrobné informácie o produkte IKT a jeho zdrojovom kóde.

V rámci novej certifikácie je možné opätovne použiť výsledky hodnotenia z inej certifikácie produktov IKT. Žiadateľ preto môže poskytnúť CAB predchádzajúce výsledky hodnotenia vrátane tých, ktoré sa týkajú životného cyklu produktu alebo prístupu žiadateľa k riadeniu opráv, ktoré sa majú opätovne použiť ako dôkaz. CAB opätovne použije takéto výsledky na svoje úlohy, ak poskytnuté dôkazy spĺňajú požiadavky na takéto dôkazy požadované CAB a ak je možné potvrdiť autentickosť dôkazov.

Ak CAB schváli, aby sa produkt IKT podrobil certifikácii zloženého produktu, všetky potrebné prvky vymedzené v kapitole 8, ŠPECIFICKÉ KRITÉRIA A METÓDY HODNOTENIA, sa sprístupnia CAB vykonávajúcemu hodnotenie zloženého produktu, prípadne v súlade s povinnými podpornými prvkami stanovenými pre technickú doménu.

Potrebné informácie sa poskytnú CAB, pokiaľ CAB nesúhlasí s prístupom k týmto informáciám iným spôsobom[8].

Okrem toho v prípade tejto schémy každý žiadateľ poskytne orgánu posudzovania zhody v súlade s pravidlami vymedzenými v kapitole 23 DOPLŇUJÚCE INFORMÁCIE O KYBERNEBEZPEČNOSTI - ČLÁNOK 55 odkaz na doplňujúce informácie o kybernetickej bezpečnosti vymedzené v článku 55 CSA. To umožní orgánu posudzovania zhody integrovať odkaz do certifikátu kybernetickej bezpečnosti, ako sa vyžaduje v kapitole 17, OBSAH A FORMÁT CERTIFIKÁTOV.

Schéma EUCC môže požadovať, aby časť alebo všetky takéto doplňujúce informácie podliehali posúdeniu CAB; to sa uvedie v príslušnej kapitole (kapitolách).

Všeobecné pravidlá týkajúce sa ochrany informácií poskytnutých žiadateľom musia byť v súlade s požiadavkami stanovenými v kapitole 24, ĎALŠIE PRVKY SCHÉMY.

ZÁKLADNÉ INFORMÁCIE

Informácie, ktoré žiadateľ požaduje na základe tej istej základnej normy (CC), uľahčia migráciu z MRA SOG-IS do novej schémy, a ak je to možné, opätovné použitie za podmienok definovaných pre danú schému. Takéto opätovné použitie sa môže týkať životného cyklu produktu IKT (napríklad miest, kde sa produkt vyvíja alebo vyrába) alebo postupov (napríklad správa záplat), ktoré sa vzťahujú na viaceré produkty a ktoré už boli posúdené v rámci predchádzajúcich hodnotení a certifikácií.

Okrem predloženia odkazu na doplňujúce informácie o kybernetickej bezpečnosti, ako sa vyžaduje v článku 55 CSA, ktoré sa vložia do certifikátu (pozri kapitolu 17, OBSAH A FORMÁT CERTIFIKÁTOV), sa zabezpečila potreba sprístupniť časť obsahu týchto informácií CAB. Umožní to v prípade potreby skontrolovať, či sú tieto informácie platné, úplné, presné a aktuálne v súlade s požiadavkami príslušných kapitol, ako sú pravidlá zaobchádzania so zraniteľnými miestami.

Pravidlá týkajúce sa bezpečnosti informácií boli stanovené s cieľom umožniť harmonizovanú ochranu

[8] CAB môže napríklad súhlasiť s prístupom k informáciám v priestoroch výrobcu alebo poskytovateľa

citlivých a chránených informácií vývojárov, ktorí sa podrobujú certifikácii.

10. ZNAČKY A ŠTÍTKY

ODKAZ (-Y) NA ČLÁNOK(-KY) CSA

Článok 54 1. *Európska schéma certifikácie kybernetickej bezpečnosti obsahuje aspoň tieto prvky:*

i) ak schéma stanovuje značky alebo štítky, podmienky, za ktorých sa tieto značky alebo štítky môžu používať.

Európsky rámec certifikácie kybernetickej bezpečnosti môže stanoviť štítok a súvisiacu značku.

Ak je takéto označenie k dispozícii, musí sa zaviesť osobitne pre túto schému, aby sa umožnilo jeho použitie na každom certifikáte, certifikovanom produkte IKT a súvisiacej dokumentácii.

Štítok a súvisiaca značka sa používajú len pri udelení certifikátu a do skončenia jeho platnosti: nedodržanie tejto podmienky sa považuje za nezrovnalosť, ako je definované v kapitole 11, PRAVIDLÁ MONITOROVANIA SÚLADU.

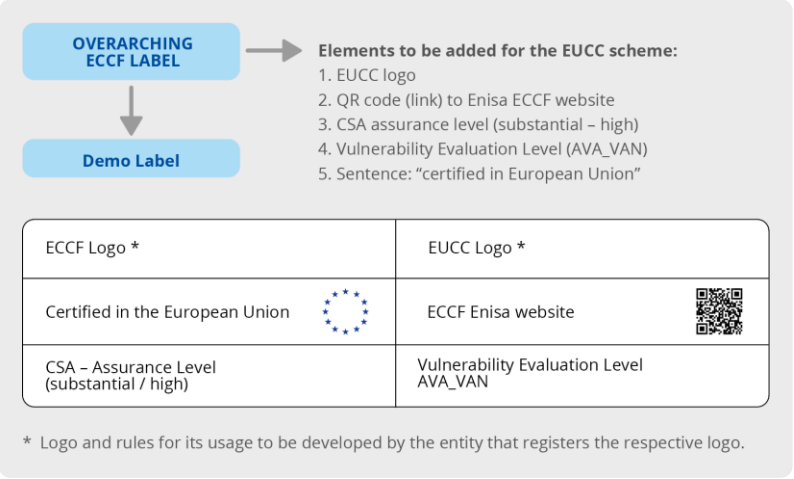
Bez toho, aby boli dotknuté pravidlá monitorovania dodržiavania predpisov opísané v kapitole 11, PRAVIDLÁ MONITOROVANIA SÚLADU, môže mať v závislosti od okolností povaha a vplyv nerešpektovania, nesprávneho používania, zneužívania, zneužívania značky a/alebo označenia ďalšie právne dôsledky v oblasti ochrany práv duševného vlastníctva, prípadných obvinení z trestných činov (napr. podvod, klamanie), predpisov o dohľade nad trhom súvisiacich s ochranou spotrebiteľa (napr. klamlivá a/alebo nezákonná porovnávacia reklama alebo distribúcia produktov). Tieto právne dôsledky sú mimo rozsahu pôsobnosti tejto schémy EUCC.

ZÁKLADNÉ INFORMÁCIE

Štítok a súvisiaca značka, ktoré boli vytvorené pre Európsky rámec certifikácie kybernetickej bezpečnosti a zavedené špeciálne pre tento systém, umožnia:

- zdôrazniť, že produkt IKT bol certifikovaný v Európskej únii, a poskytnúť okamžité informácie o certifikáte odkazom na rámec (ECCF), schéma hodnotenia a úroveň záruky;
- aby bola certifikácia ľahko rozpoznateľná, keďže štítok aj príslušná značka môžu byť vytlačené na obale produktov, v technickej dokumentácii a na letákoch používaných na marketingové účely;
- poskytnúť priamy odkaz (vo forme QR kódu) na webovú stránku agentúry ENISA (podľa článku 50), kde sú zverejnené všetky informácie týkajúce sa certifikátu vrátane aktuálneho stavu certifikátu.

***Obrázok 1** Ukážkový štítok schémy EUCC*



"Ukážkový štítok" zobrazuje základné informácie, ktoré môže obsahovať štítok spojený so schémou:

- logo ECCF (registrované, regulované a chránené subjektom zodpovedným za presadzovanie rámca označovania);
- logo EUCC (ktoré má byť registrované, regulované a chránené subjektom zodpovedným za presadzovanie rámca označovania);

- QR kód smerujúci na webový portál agentúry ENISA - podľa článku 50 CSA - a na stránku, kde je možné vyhľadať platný stav certifikátu produktov a informácie o jeho životnom cykle;
- úroveň záruky CSA (so zavedením špecifickej farby označujúcej každú úroveň) a súvisiace hodnotenie úrovne zraniteľnosti AVA_VAN;
- vetu "Certifikované v Európskej únii" spolu s vlajkou EÚ.

Uvedenie QR kódu bude vyžadovať, ako je definované v kapitole 20, POLITIKA ZVEREJŇOVANIA CERTIFIKÁTOV, postup pre zverejnenie QR kódu.

11. PRAVIDLÁ MONITOROVANIA SÚLADU

ODKAZ(-Y) NA ČLÁNOK(-KY) CSA

Článok 54 1. *Európska schéma certifikácie kybernetickej bezpečnosti obsahuje aspoň tieto prvky:*

i) pravidlá monitorovania súladu produktov IKT, služieb IKT a procesov IKT s požiadavkami európskych certifikátov kybernetickej bezpečnosti alebo EÚ vyhlásení o zhode vrátane mechanizmov na preukázanie trvalého súladu s určenými požiadavkami kybernetickej bezpečnosti.

Článok 58 7. *Národné autority pre certifikáciu kybernetickej bezpečnosti:*

a) podľa článku 54 ods. 1 písm. j) týkajúce monitorovania súladu produktov IKT, služieb IKT a procesov IKT dozerajú a v spolupráci v spolupráci s ďalšími príslušnými orgánmi trhového dohľadu presadzujú pravidlá uvedené v európskych schémach certifikácie kybernetickej bezpečnosti s požiadavkami európskych certifikátov kybernetickej bezpečnosti vydanými na ich územiach;

b) monitorujú a presadzujú dodržiavanie povinností výrobcov alebo poskytovateľov produktov IKT, služieb IKT alebo procesov IKT usadených na ich územiach, ktorí vykonali posúdenie zhody samohodnotením uvedené v článku 53 ods. 2 a 3, príslušnej európskej schéme certifikácie kybernetickej bezpečnosti;

c) bez toho, aby bol dotknutý článok 60 ods. 3, na účely tohto nariadenia aktívne pomáhajú národným akreditačným orgánom a podporujú ich pri monitorovaní činností orgánov posudzovania zhody a dozore nad týmito činnosťami;

d) monitorujú a dozerajú na činnosti verejných orgánov uvedených v článku 56 ods. 5 ;

e) vybavujú sťažnosti fyzických alebo právnických osôb v súvislosti s európskymi certifikátmi kybernetickej bezpečnosti vydanými národnými autoritami pre certifikáciu kybernetickej bezpečnosti alebo v súvislosti s európskymi certifikátmi kybernetickej bezpečnosti vydanými orgánmi posudzovania zhody v súlade s článkom 56 ods. 6 alebo v súvislosti s EÚ vyhláseniami o zhode vydanými podľa článku 53 a v primeranom rozsahu prešetrujú predmet takýchto sťažností a v primeranej lehote informuje sťažovateľa o pokroku a výsledku prešetrovania;

f) poskytujú agentúre ENISA a ECCG výročnú súhrnnú správu o činnostiach vykonávaných podľa písmen b), c) a d) tohto odseku alebo podľa odseku 8;

g) spolupracujú s inými národnými autoritami pre certifikáciu kybernetickej bezpečnosti alebo inými i orgánmi verejnej moci, čo zahŕňa poskytovanie informácií o možnom nesúlade produktov IKT, služieb IKT a procesov IKT s požiadavkami tohto nariadenia alebo s požiadavkami osobitných európskych schém certifikácie kybernetickej bezpečnosti.

Článok 58 8. *Každá národná autorita pre certifikáciu kybernetickej bezpečnosti má aspoň tieto právomoci:*

a) žiadať od orgánov posudzovania zhody, držiteľov európskych certifikátov kybernetickej bezpečnosti a vydavateľov EÚ vyhlásení o zhode akékoľvek informácie, ktoré potrebuje na plnenie svojich úloh;

b) viesť vyšetrovanie v podobe auditov orgánov posudzovania zhody, držiteľov európskych certifikátov kybernetickej bezpečnosti a vydavateľov EÚ vyhlásení o zhode na overenie, či dodržiavajú ustanovenia tejto hlavy;

c) prijať primerané opatrenia v súlade s vnútroštátnym právom s cieľom zabezpečiť, aby orgány posudzovania zhody, držitelia európskych certifikátov kybernetickej bezpečnosti a vydavatelia EÚ vyhlásení o zhode dodržiavali toto nariadenie alebo európsku schému certifikácie kybernetickej bezpečnosti;

d) získať prístup do priestorov akýchkoľvek orgánov posudzovania zhody alebo držiteľov európskych certifikátov kybernetickej bezpečnosti na účely vykonávania vyšetrovaní v súlade s procesným právom Únie alebo členského štátu;

e) v súlade s vnútroštátnym právom zrušiť európske certifikáty kybernetickej bezpečnosti, ktoré vydali národné autority pre certifikáciu kybernetickej bezpečnosti alebo európske certifikáty kybernetickej bezpečnosti, ktoré v súlade s článkom 56 ods. 6 vydali orgány posudzovania zhody ak takéto

certifikáty nie sú v súlade s týmto nariadením alebo európskou schémou certifikácie kybernetickej bezpečnosti;

f) ukladať v súlade s vnútroštátnymi právom sankcie podľa článku 65, a vyžadovať okamžité ukončenie porušovania povinností stanovených v tomto nariadení.

Bez toho, aby boli dotknuté činnosti NCCA vymedzené v článkoch 58.7 a 58.8 CSA, monitorovanie súladu produktov IKT s požiadavkami európskych certifikátov kybernetickej bezpečnosti preukazuje ich trvalý súlad so stanovenými požiadavkami kybernetickej bezpečnosti.

Toto monitorovanie umožní, ak je to možné, zabrániť a v prípade potreby odhaliť najmä tieto všeobecné prípady nesúladu:

- nedodržanie pravidiel a povinností súvisiacich s certifikátom vydaným na ich produkt IKT zo strany výrobcu alebo poskytovateľa;
- nesúlad s podmienkami, za ktorých sa certifikácia vykonáva a ktoré sa netýkajú jednotlivých produktov IKT;
- nezhodu certifikovaného produktu IKT s jeho bezpečnostnými požiadavkami, ktorý zahŕňa:
  - zmeny v prostredí hrozieb po vydaní certifikátu, ktoré majú nepriaznivý vplyv na bezpečnosť certifikovaného produktu IKT[9];
  - identifikovaná zraniteľnosť súvisiaca s certifikovaným produktom IKT, ktorá má nepriaznivý vplyv na bezpečnosť certifikovaného produktu IKT.

Všeobecné monitorovanie certifikovaných produktov IKT je založené na výbere vzoriek s použitím všeobecných kritérií, ako je typ produktu, úroveň hodnotenia, výrobca alebo poskytovateľ, CAB a všetky relevantné informácie, ktoré sa NCCA dozvie (napr. sťažnosti, bezpečnostné udalosti). NCCA na svojich územiach a v spolupráci s ostatnými príslušnými orgánmi trhového dohľadu každoročne odoberú vzorky minimálne 5 % produktov a aspoň jedného produktu ročne, ktoré získali certifikáty v predchádzajúcom roku.

NCCA zapojí do monitorovania CB a v prípade potreby ITSEF certifikovaného produktu IKT. Monitorovanie pozostáva z opätovného posúdenia produktu IKT, ako je definované v prílohe 11, v prípade potreby spolu s auditom na potvrdenie alebo vyvrátenie vyššie uvedených relevantných informácií (napr. sťažností, bezpečnostných udalostí), ktoré sa NCCA dozvedela.

Ak sa vyberie produkt, výrobca alebo vývojár musí byť informovaný o dôvodoch výberu.

Opakované posúdenia a audity, ak sú potrebné, finančne podporuje výrobca alebo poskytovateľ. Okrem tohto všeobecného monitorovania sa vykonávajú nižšie opísané činnosti.

Nasledujúce odchýlky a nezrovnalosti sa považujú za potenciálny nesúlad pri uplatňovaní pravidiel a povinností súvisiacich s certifikátom vydaným na ich produkt IKT zo strany výrobcu alebo poskytovateľa:

- akúkoľvek odchýlku od požiadaviek, ktoré sa vzťahujú na informácie poskytnuté alebo sprístupnené CB alebo ITSEF a ktoré by mohli byť zistené po vydaní certifikátu, ako napr:
  - verzia dodaných informácií, ktorá nezodpovedá certifikovanému produktu IKT;
  - vlastné dôkazy, ktoré neboli v súlade s realitou produktu;
- akúkoľvek odchýlku od požiadaviek týkajúcich sa obsahu certifikátu a doplňujúcich informácií, ako sa vyžaduje v kapitole 9, INFORMÁCIE POTREBNÉ PRE CERTIFIKÁCIU, kapitole 17, OBSAH A FORMÁT CERTIFIKÁTOV, kapitole 18, DOSTUPNOSŤ INFORMÁCIÍ a kapitole 23, DOPLŇUJÚCE INFORMÁCIE O KYBERNETICKEJ BEZPEČNOSTI - ČLÁNOK 55, vrátane a bez obmedzenia na:
  - odchýlku od odkazovania na správne identifikátory produktov IKT;
  - nesprávne zosúladenie opisu rozsahu TOE[10];
- odchýlku od obmedzení certifikátu vrátane obmedzení uvedených v kapitole 12, PODMIENKY VYDÁVANIA, UDRŽIAVANIA, POKRAČOVANIA A OBNOVOVANIA CERTIFIKÁTOV[11];
- odchýlok od podmienok používania značiek a štítkov schémy, ako sú definované v kapitole 10, ZNAČKY A ŠTÍTKY;
  - neoprávnené úpravy alebo zmeny dokumentu certifikátu, ako je vymedzené v kapitole 17,

[9] Nezamieňajte s prevádzkovým prostredím, za ktoré nesú zodpovednosť výlučne používatelia.
[10] napr. naznačenie, že certifikát sa vzťahuje na celý produkt, a nie na skutočný TOE, použitím rovnakého alebo podobného názvu pre TOE a celý produkt.
[11] napr. reklama certifikovaného produktu po uplynutí platnosti certifikátu produktu

OBSAH A FORMÁT CERTIFIKÁTOV;
  - opomenutie poskytnúť alebo neoprávnená zmena špecifikácie produktu a doplňujúcich informácií v zmysle kapitoly 18, DOSTUPNOSŤ INFORMÁCIÍ a kapitoly 23, DOPLŇUJÚCE INFORMÁCIE O KYBERNETICKEJ BEZPEČNOSTI - ČLÁNOK 55;
- akékoľvek odchýlky od požiadaviek na povinnosti držiteľa certifikátu týkajúce sa zachovania platnosti certifikátu, ako napr.:
  - neuplatňovanie povinných činností údržby;
  - nezavedenie a nevykonávanie povinných postupov, ako to vyžadujú podmienky certifikátu a značky;
  - v prípade potreby neoznámenie zmien vývojového cyklu a prostredia[12];
  - odchýlky od rozsahu certifikovaného produktu vrátane povinností vyplývajúcich z článku 56.8 CSA, vrátane: nedeklarovaných úprav produktu IKT, jeho dodávateľských procesov, rozvojového prostredia[13], zoznamu CMC komponentov TOE[14]alebo použitých nástrojov[15].

Takéto nedodržiavanie požiadaviek týkajúcich sa certifikátu vydaného na ich produkt IKT zo strany výrobcu alebo poskytovateľa sa monitoruje:

1) požadovaním, aby sa každý žiadateľ o certifikát zaviazal CB k viacerým povinnostiam, okrem iného:
   - odovzdávať CB a ITSEF informácie, ktoré považujú za spoľahlivé a pri ktorých nehrozí riziko falšovania úsudku CB a ITSEF;
   - nevyhlasovať predmet za certifikovaný, kým ešte prebieha hodnotenie;
   - deklarovať predmet ako certifikovaný len pre rozsah uvedený v certifikáte;
   - v prípade pozastavenia alebo odobratia certifikátu okamžite zastaviť používanie akejkoľvek reklamy, v ktorej sa uvádza certifikát;
   - zabezpečiť, aby produkty vyrábané v sérii a predávané v spojení s vydaným certifikátom boli prísne identické s produktom, ktorý bol predmetom certifikácie;
   - zaviazať sa, že bude dôsledne dodržiavať pravidlá používania značky stanovenej pre túto schému;
2) s použitím nasledujúceho dostupného dispozitívneho práva na sledovanie nedodržania predchádzajúcich záväzkov:
   a. činnosti dohľadu nad trhom ustanovené podľa článku 58 ods. 7 písm. a) CSA so správou pre CB, ktorá vydala certifikát;
   b. opatrenia na zabezpečenie kvality zavedené v rámci CB a možnosť podávať a vybavovať sťažnosti;
3) posúdením závažnosti nezrovnalosti zo strany CB s prípadnou podporou ITSEF;
4) využitím možnosti dialógu medzi CB a výrobcom alebo poskytovateľom s cieľom pokúsiť sa vyriešiť drobné problémy a v prípade potreby aj ustanovenia kapitoly 13, PRAVIDLÁ TÝKAJÚCE SA NEDODRŽIAVANIA PREDPISOV.

O výsledkoch týchto činností sa informuje NCCA.

Okrem činností dohľadu nad trhom môže NCCA stanoviť pravidlá pravidelného dialógu medzi vydavateľmi certifikátov a vlastníkmi certifikátov s cieľom formálne skontrolovať a oznámiť dodržiavanie vopred stanovených záväzkov.

Agentúra ENISA môže na účely harmonizácie so schémou EUCC poskytnúť v spolupráci s ECCG usmernenie k záväzkom, ktoré môžu byť súčasťou žiadosti, s uvedením súvisiacej závažnosti.

Nasledujúce odchýlky sa považujú za potenciálne problémy súvisiace s nedodržiavaním podmienok, za ktorých sa certifikácia vykonáva, a ktoré sa netýkajú jednotlivých produktov IKT:

- nesplnenie povinností týkajúcich sa vybavovania sťažností na zachovanie platnosti certifikátu vrátane:
  - povinnosti auditu dodržiavania systému CB, ITSEF a držiteľov certifikátov v súvislosti s používaním certifikátov, ako to implicitne vyžaduje článok 58.8 písm. b) CSA;
  - povinnosti dohľadu a presadzovania dodržiavania systému CB, ITSEF a držiteľov certifikátov, ako sa implicitne vyžaduje v čl. 58 ods. 7 písm. a) CSA;

[12] napr. zmena zlievarne čipov.
[13] napr. aktualizácia CMC.
[14] napr. prejsť na iné komponenty, keď sa prestane používať niektorý z uvedených komponentov.
[15] napr. úprava nástrojov súvisiacich s ALC_TAT.

- povinnosti pri vybavovaní sťažností, ako to implicitne vyžaduje čl. 58.7.(f);
- odchýlky od požiadaviek na hodnotenie:
  - neodôvodnená odchýlka od metodiky hodnotenia a príslušných podporných dokumentov opísaných v kapitole 3, NORMY POUŽITÉ PRI HODNOTENÍ;
  - odchýlky od očakávanej hodnotiacej kompetentnosti, ako je opísané v kapitole 6, ŠPECIFICKÉ POŽIADAVKY VZŤAHUJÚCE SA NA CAB.

Takýto nesúlad podmienok, za ktorých sa certifikácia vykonáva a ktoré sa netýkajú jednotlivého produktu IKT, sa má:

1) vyhnúť, ak je to možné, prostredníctvom:
   a. auditu povoleným podľa článku 58 ods. 8 písm. b) a c);
   b. trvalým monitorovaním ITSEF ich akreditačnými orgánmi a CB, ako sa požaduje v kapitolách 6 a 23;
2) zistiť prostredníctvom:
   a. procesu kvality CB a ITSEF vrátane správy o zistenom probléme pre NCCA a požiadavky spojenej s ich akreditáciou na vybavovanie sťažností.

Za potenciálne problémy nesúladu certifikovaného produktu IKT s jeho bezpečnostnými požiadavkami sa považujú tieto prípady:

- zmena v prostredí hrozieb, ktorá má nepriaznivý vplyv na bezpečnosť certifikovaného produktu IKT;
- identifikovaná zraniteľnosť súvisiaca s certifikovaným produktom IKT, ktorá má nepriaznivý vplyv na bezpečnosť certifikovaného produktu IKT.

Takáto nezhoda certifikovaného produktu IKT s jeho bezpečnostnými požiadavkami sa monitoruje v rámci týchto povinností:

1) výrobcovia a poskytovatelia produktov IKT:
   - monitorujú všetky zraniteľnosti, ktoré by sa týkali ich produktu IKT, buď zverejnením alebo prijatím od koncových používateľov a výskumných pracovníkov v oblasti bezpečnosti, ako je definované v článku 55.1 písm. c), alebo zistením výrobcom/poskytovateľom, a informovať CB, ktorá vydala certifikát, o zmenách týkajúcich sa vyhlásení príslušného certifikátu;
   - monitorujú známe závislosti a zraniteľnosti identifikované akýmkoľvek iným zdrojom, ktoré sa môžu týkať certifikovaného produktu, a v prípade potreby predložiť ich CB analýzu vplyvu;
   - spolupracujú s CB a v prípade potreby s NCCA s cieľom podporiť ich monitorovacie činnosti;
   - môžu posudzovať takéto činnosti v rámci procesu certifikácie produktu IKT prostredníctvom príslušnej skupiny záruk CC časť 3 ALC_FLR;
2) certifikačné orgány a ITSEF;
   - monitorujú všetky zraniteľnosti z akéhokoľvek zdroja, ktoré by boli relevantné pre ich rozsah hodnotenia a certifikácie;
   - nahlasujú svojmu NCCA každú zistenú zraniteľnosť, ktorá ovplyvňuje zhodu certifikovaného produktu IKT s požiadavkami súvisiacimi s certifikáciou.

Ak to CB považuje za potrebné alebo podľa uváženia NCCA, môže sa požadovať vykonanie série úloh hodnotenia s podporou[16] výrobcu alebo poskytovateľa certifikovaného produktu IKT s cieľom potvrdiť vplyv nezhody.

Tieto činnosti súvisiace s monitorovaním dodržiavania súladu sú súčasťou výročnej súhrnnej správy NCCA.

ZÁKLADNÉ INFORMÁCIE

Požiadavky boli stanovené s ohľadom na:

- prípadné nezrovnalosti (podľa článku 56.8 CSA): Nezrovnalosť ovplyvňujúca súlad produktu vyplýva z bezpečnostného výroku uvedeného v certifikáte a/alebo jeho základnej špecifikácie

[16] V prípade potreby podpora znamená finančnú podporu opísaných činností.

(ciele, predpoklady, funkcie, atď.), rozvojového prostredia (ALC), Doručenia produktu (ALC_DEL), skúšania produktu (ATE), posúdenia zraniteľnosti (AVA) a/alebo v prípade zvolenia odstraňovania chýb (ALC_FLR). Hoci sa takéto nezrovnalosti riešia ako nesúlad produktu po certifikácii, môžu sa objaviť kedykoľvek;

- potenciálne medzery v odborných kompetentnostiach CAB;
- potenciálne zraniteľnosti a úpravy produktu alebo jeho prostredia.

Identifikovali sa súvisiace problémy nesúladu a zaviedli sa protiopatrenia na ich predchádzanie a odhaľovanie.

Tento proces využíva ustanovenia CSA:

- dohľadu nad trhom zavedený podľa článku 58 ods. 7 písm. a);
- povinnosti vykonávať audit dodržiavania schémy CAB a držiteľov certifikátov podľa článku 58 ods. 8 písm. b);
- práva napadnúť certifikáty (článok 63 ods. 1) a potrebu, aby zodpovedné orgány alebo úrady vybavovali sťažnosti týkajúce sa platnosti certifikátu vydaného na úrovni záruky "vysoká" (článok 58 ods. 7 písm. f), a teda súlad produktu, ako sa vyžaduje v článku 54 ods. 1 písm. j);
- NCCA môže - prostredníctvom právomoci podľa článku 58 ods. 8 písm. b) - prešetriť sťažnosť týkajúcu sa súladu produktu auditom držiteľa a vydavateľa certifikátu a predísť tak súdnemu sporu. Táto právna konštrukcia zasa ponecháva certifikáty na úrovni záruky "významná" bez akéhokoľvek preventívneho opatrenia na mimosúdne vybavenie sťažnosti;
- takéto sťažnosti sa preto musia riešiť na úrovni CAB a jeho NAB. Keďže v článku 54 ods. 1 písm. j) sa požadujú pravidlá pre súlad produktu a žiadna takáto právna požiadavka na vybavovanie sťažností na úrovni záruky "významná" neexistuje, bola zahrnutá povinnosť vybavovať takéto sťažnosti. V dôsledku toho bolo vybavovanie sťažností zrovnoprávnené so všetkými úrovňami záruky schémy;
- nutnosti zahrnúť do schémy riešenie zraniteľnosti a prijať nové postupy opravovania.

Pokiaľ ide o úlohu výrobcov alebo poskytovateľov monitorovať známe závislosti a zraniteľnosti: Podmienky certifikátu vyžadujú, aby výrobca alebo poskytovateľ monitoroval prostredie hrozieb a informoval CAB o každej zraniteľnosti svojho certifikovaného produktu. ITSEF môže výrobcom alebo poskytovateľom navrhnúť takúto službu.

V prípade potreby boli uvedené podmienky na podporu nových hodnotiacich činností, keďže môžu mať finančný vplyv.

12. PODMIENKY VYDÁVANIA, UDRŽIAVANIA, POKRAČOVANIA A OBNOVOVANIA CERTIFIKÁTOV

ODKAZ(-Y) NA ČLÁNOK(-KY) CSA

Článok 54 1. *Európska schéma certifikácie kybernetickej bezpečnosti obsahuje aspoň tieto prvky:*

k) prípadne podmienky vydávania, udržiavania, pokračovania a obnovovania platnosti európskych certifikátov kybernetickej bezpečnosti, ako aj podmienky pre rozšírenie alebo zúženie rozsahu certifikácie.

Úvod do procesov súvisiacich s vydávaním a udržiavaním certifikátu

S vydávaním a udržiavaním certifikátu súvisí niekoľko procesov: prehľad na vysokej úrovni je uvedený na nasledujúcom obrázku:

Obrázok 2: *Prehľad procesov súvisiacich s vydávaním a udržiavaním certifikátu na vysokej úrovni*

Referenčnou normou pre tieto činnosti je norma ISO/IEC 17065 a najmä jej článok 7.10, kde sa hovorí o "zmenách ovplyvňujúcich certifikát"[17].

Zmeny ovplyvňujúce certifikát môžu byť rôzneho charakteru a môžu sa týkať jeho technického obsahu, ktorý by mohol viesť k nezhodám, alebo môžu súvisieť s inými faktormi vrátane nesúladov[18]. Všimnite si, že príloha 11, KONTINUITA ZÁRUKY, sa vzťahuje len na časť činností údržby súvisiacich s certifikáciou: berie do úvahy zmeny technickej povahy, ktoré sa priamo týkajú bezpečnostnej záruky osvedčenou certifikátom.

Podmienky vydania certifikátu

Certifikačný orgán (CB) vydá certifikát len vtedy, ak:

- žiadateľ sa zaviazal splniť všetky povinnosti, ktoré je potrebné splniť v rámci tejto schémy na získanie certifikátu;
- hodnotenie produktu IKT je v súlade s požiadavkami na hodnotenie stanovenými v tejto schéme pre požadovaný výber komponentov záruk a je úspešné;
- preskúmanie výsledkov hodnotenia zo strany CB je úspešné a v súlade s požiadavkami normy ISO/IEC 17065.

[17] Všimnite si, že v norme sa nepoužíva pojem "údržba".

[18] pozri diskusiu o nezhode/nesúlade v kapitole 11, PRAVIDLÁ MONITOROVANIA SÚLADU.

CB monitoruje všetky správy z hodnotenia poskytnuté ITSEF (vrátane technických správ o hodnotení), aby zabezpečil, že závery sú v súlade s predloženými dôkazmi a že sa správne uplatnili prijaté hodnotiace kritériá a metódy hodnotenia.

Certifikát sa vzťahuje na verziu hodnoteného produktu IKT vrátane jeho sprievodnej dokumentácie.

CB stanoví dobu platnosti certifikátu, ktorá nesmie presiahnuť maximálnu dobu definovanú v kapitole 19, DOBA PLATNOSTI CERTIFIKÁTOV.

Podmienky na udržiavanie, pokračovanie a obnovovanie certifikátu

Certifikovaný produkt IKT môže počas platnosti certifikátu zostať stabilný a využívať nezmenené prostredie hrozieb; v takom prípade certifikát platí až do dátumu jeho platnosti. Túto skutočnosť potvrdí CAB v rámci svojich monitorovacích činností, ako sa uvádza v kapitole 11, PRAVIDLÁ MONITOROVANIA SÚLADU.

Vo všetkých ostatných prípadoch sa na certifikovaný produkt IKT vzťahujú činnosti údržby v reakcii na zmeny, ktoré majú vplyv na jeho certifikáciu. Činnosti údržby zahŕňajú preskúmanie a rozhodnutie, ktoré vykonáva CB, a ak sa takáto činnosť považuje za potrebnú, aj hodnotenie, ktoré vykonáva ITSEF.

Údržbové činnosti sa môžu začať na žiadosť vlastníka certifikátu za týchto podmienok:
- čoskoro uplynie doba platnosti certifikátu;
- zmena certifikovaného produktu IKT vrátane zmeny v jeho životnom cykle, ktorá sa neočakáva a mohla by mať vplyv na jeho bezpečnostnú funkčnosť;
- žiadosť o obnovenie posúdenia zraniteľnosti, aby sa preukázalo, že výroky o odolnosti spojené s certifikátom stále platia v porovnaní so „state of he art“ útokov.

Iniciuje sa za týchto podmienok:
- ak bol produkt IKT vybraný prostredníctvom pravidla výberu vzoriek zavedeného na všeobecné monitorovanie certifikovaných produktov IKT, ako je vymedzené v kapitole 11, PRAVIDLÁ MONITOROVANIA SÚLADU;
- po potenciálnej alebo skutočnej nezhode s bezpečnostnými požiadavkami, ktorý zahŕňa okrem iného:
- zmenu v prostredí hrozieb, ktorá by mohla mať nepriaznivý vplyv na bezpečnosť certifikovaného produktu IKT;
- potenciálna zraniteľnosť identifikovaná a súvisiaca s certifikovaným produktom IKT, ktorá by mohla mať nepriaznivý vplyv na bezpečnosť certifikovaného produktu IKT;
- po zistení nesúladu s akreditačnými požiadavkami CAB, ustanoveniami CSA alebo požiadavkami schémy, ktorý ovplyvňuje certifikáciu.

V závislosti od povahy predchádzajúcich podmienok a v súlade s požiadavkami stanovenými v kapitole 11, PRAVIDLÁ MONITOROVANIA SÚLADU, kapitole 13, PRAVIDLÁ TÝKAJÚCE SA NEDODRŽIAVANIA PREDPISOV a kapitole 14, PRAVIDLÁ TÝKAJÚCE SA RIEŠENIA ZRANITEĽNOSTÍ, sa činnosti údržby spúšťajú na základe rozhodnutia výrobcu alebo poskytovateľa produktu IKT, CB alebo NCCA. Národný akreditačný orgán môže spustiť činnosti údržby aj v prípade, že bola vydaná sťažnosť.

Ak činnosti údržby iniciuje výrobca alebo poskytovateľ produktu IKT, k žiadosti o údržbu predloženej CB sa priloží správa o analýze vplyvu (IAR) v súlade s prílohou 11, KONTINUITA ZÁRUKY.

Ak činnosti údržby iniciuje akákoľvek iná strana (CB, NCCA a akákoľvek zainteresovaná strana, ktorá vystupuje ako sponzor súvisiacich činností údržby), žiadosť musí byť podložená odôvodnením údržby, ktoré obsahuje opis potenciálnej alebo skutočnej nezhody alebo identifikovaného nesúladu a jej možný vplyv na certifikát.

Na základe IAR alebo odôvodnenia údržby CB pred svojím preskúmaním a rozhodnutím overí, či sú niektoré úlohy hodnotenia považované za potrebné, a zodpovedajúcim spôsobom s podporou ITSEF overí rozsah a pracovné zaťaženie spojené s týmito úlohami. CB tiež overí výsledok potrebných úloh hodnotenia po ich dokončení zo strany ITSEF.

Výrobca alebo poskytovateľ produktu IKT podporí[19] ITSEF pri úlohách hodnotenia, ktoré považuje za potrebné, pokiaľ nie je v kapitole 13, PRAVIDLÁ TÝKAJÚCE SA NEDODRŽIAVANIA PREDPISOV, uvedené inak.

V žiadosti o činnosti údržby sa môže identifikovať vysoká úroveň naliehavosti zmien/opráv certifikovaného produktu IKT: CB môže prípadne rozhodnúť o povolení uplatnenia procesu riadenia opráv, ako je definovaný v kapitole 14, PRAVIDLÁ TÝKAJÚCE SA RIEŠENIA ZRANITEĽNOSTÍ.

Ak bola správa záplat zavedená v súlade s požiadavkami prílohy 15, SPRÁVA ZÁPLAT, ktorá je určená na skúšobné použitie[20] , CB môže tiež rozhodnúť o povolení jeho použitia ako zrýchleného prístupu na zvládnutie činností údržby spojených s funkčnými zmenami produktu.

Na základe preskúmania a rozhodnutia CB sa činnosti údržby ukončia jedným z týchto rozhodnutí alebo ich kombináciou:

- pokračovanie certifikátu, čo zodpovedá zachovaniu existujúceho certifikátu bez zmeny,
- obnovenie certifikátu s novou dobou platnosti, čo zodpovedá opätovnému vydaniu toho istého certifikátu s novou dobou platnosti,
- vydanie certifikátu buď s rozšíreným rozsahom, zníženou úrovňou záruky, alebo so zníženým rozsahom certifikátu, aby stále spĺňal súčasnú úroveň záruky, prípadne s novým obdobím platnosti;
- pozastavenie platnosti certifikátu až do prijatia nápravných opatrení zo strany výrobcu alebo poskytovateľa produktu IKT,
- odňatie certifikátu.

K rozhodnutiam sa priloží Správa o udržiavaní, ktorú vydá CB v súlade s Prílohou 11, KONTINUITA ZÁRUKY, a ktorá je jednoznačne spojená s certifikátom; rozhodnutie sa v nej odôvodní a prípadne sa v nej uvedú všetky potrebné zmeny pôvodného certifikátu.

V prípade, že nebola podaná žiadosť o udržiavanie certifikátu, ktorého platnosť uplynula, certifikát podlieha archivácii. Archivácia spočíva v tom, že sa naďalej poskytuje prístup k certifikátu a súvisiacim informáciám s jasným označením, že dátum jeho platnosti už uplynul.

V prípade, že sa začne údržba a žiadna zo zodpovedných strán neprijme včas žiadne opatrenie, certifikát sa odníme.

Na podporu vhodného rozhodnutia o najčastejších možných prípadoch CB zohľadní nasledujúcu tabuľku.

Tabuľka 5: *Menovité rozhodnutia spojené s udržiavaním certifikátov*

Prípady	Menovité rozhodnutia
Ten istý produkt IKT stále spĺňa bezpečnostné požiadavky na certifikáciu.	Pokračujte v platnosti certifikátu až do dátumu jeho vypršania
Dátum platnosti certifikátu vypršal a nebola predložená žiadna žiadosť o údržbu.	Archivácia certifikátu
Nové úlohy hodnotenia (pozri opätovné posudzovanie definované v prílohe 11) vrátane testovania zraniteľnosti boli vykonané na tej istej verzii produktu IKT a sú úspešné.	Obnovenie certifikátu s potenciálne predĺženou platnosťou
Upravená/opravená verzia produktu IKT spĺňa bezpečnostné požiadavky na certifikáciu v súlade s procesmi vývojára a žiadne nové úlohy hodnotenia neboli považované za potrebné.	Vydanie nového certifikátu s rozsahom zodpovedajúcim novej verzii s rovnakým obdobím platnosti
Nové úlohy hodnotenia (pozri prehodnotenie definované v prílohe 11) vrátane testovania zraniteľnosti boli vykonané na upravenej/opravenej verzii produktu IKT a sú úspešné.	Vydanie nového certifikátu s rozšíreným rozsahom zodpovedajúcim upravenej verzii a s predĺženou dobou platnosti
Vykonali sa potrebné úlohy hodnotenia (pozri opätovné posudzovanie definované v prílohe 11) a zistilo sa, že tá istá verzia produktu IKT nespĺňa všetky uplatniteľné požiadavky a zníženie rozsahu certifikátu by umožnilo zachovať úroveň bezpečnosti.	Vydanie nového certifikátu s obmedzeným rozsahom a prípadne s predĺženou platnosťou

[19] V prípade potreby podpora znamená finančnú podporu opísaných činností.

[20] Ako je definované v kapitole 8, ŠPECIFICKÉ KRITÉRIÁ A METÓDY HODNOTENIA.

Prípady	Menovité rozhodnutia
Vykonali sa potrebné úlohy hodnotenia (pozri opätovné posudzovanie definované v prílohe 11) a zistilo sa, že tá istá verzia produktu IKT nespĺňa všetky platné požiadavky a zníženie úrovne záruky by umožnilo zachovať certifikát.	Vydanie nového certifikátu so zníženou úrovňou záruky s možným predĺžením doby platnosti.
Vykonali sa potrebné úlohy hodnotenia (pozri opätovné posudzovanie definované v prílohe 11) a zistilo sa, že tá istá verzia produktu IKT nespĺňa všetky uplatniteľné požiadavky a je možné zachovať certifikát na tej istej úrovni a s tým istým rozsahom, hoci nie okamžite, alebo nesprávne používanie certifikátu alebo značky nie je okamžite vyriešené vhodným stiahnutím a primeranými nápravnými opatreniami zo strany výrobcu alebo poskytovateľa.	Pozastaviť certifikát až do prijatia nápravných opatrení zo strany výrobcu alebo poskytovateľa produktu IKT.
Nevykonali sa potrebné úlohy hodnotenia.	Odobratie certifikátu
Vykonali sa potrebné úlohy hodnotenia (pozri opätovné posudzovanie definované v prílohe 11) a zistilo sa, že tá istá verzia produktu IKT nespĺňa všetky platné požiadavky.	Odobratie certifikátu
Nevykonávali sa včas potrebné činnosti údržby.	Odobratie certifikátu

Certifikát zostáva v stave "pozastavený" maximálne tri mesiace, pričom tento stav možno predĺžiť len vtedy, ak je omeškanie spôsobené nedostatočnou dostupnosťou CB, ITSEF alebo NCCA. V prípade, že predajca neprijme žiadne opatrenie v stanovenej lehote, CB zmení stav certifikátu na "zrušený".

Každá zmena štatútu certifikátu sa zverejní bez zbytočného odkladu v súlade s požiadavkami kapitoly 20, POLITIKA ZVEREJŇOVANIA CERTIFIKÁTOV.

ZÁKLADNÉ INFORMÁCIE

Požiadavky boli stanovené s ohľadom na požiadavky súvisiace s normami ISO/IEC 17065 a ISO/IEC 17067, Posudzovanie zhody - Základy certifikácie produktov a usmernenia pre schémy certifikácie produktov.

Zohľadnil sa celý životný cyklus certifikátu, počnúc jeho vydaním s vymedzenou dobou platnosti až po jeho riadne alebo potenciálne ukončenie platnosti (dobou platnosti alebo predbežne z dôvodu výberu podľa pravidiel výberu vzoriek pre všeobecné monitorovanie certifikátov, potenciálneho alebo skutočného nesúladu s bezpečnostnými požiadavkami alebo zisteného nesúladu s akreditačnými požiadavkami CAB, ustanoveniami CSA alebo požiadavkami schémy).

Jednou zo základných podmienok vydania certifikátu pre produkt IKT je úspešné hodnotenie na základe CEM. Ďalšie podmienky vyplývajú z príslušných ustanovení CSA, ako sú potrebné oprávnenia pre CAB na základe článku 60.3 CSA, ktoré sú mimo certifikácie v jej technickom význame, a ak nie sú po certifikácii splnené, môžu sa považovať za prípady nezhody.

Všetky ostatné certifikačné činnosti sa týkajú fázy po vydaní certifikátu, keď nastane "*zmena ovplyvňujúca certifikáciu*", ako sa uvádza v norme ISO/IEC 17065. Tieto činnosti sú opísané ako "údržba". V takom prípade je CB povinná konať v reakcii na daný spúšťací mechanizmus.

Platí znenie normy ISO/IEC 17065, ktoré opisuje všetky príslušné činnosti súvisiace s vydaným certifikátom (pozri bod 7.10):

Obrázok 3: *Zmeny ovplyvňujúce certifikáciu (výňatok z normy ISO/IEC 17065)*

7.10 Zmeny ovplyvňujúce certifikáciu

7.10.1 Keď sa certifikčnou schémou zavádzajú nové alebo revidované požiadavky, ktoré majú vplyv na klienta, musí certifikačný orgán zabezpečiť, aby sa tieto zmeny oznámili všetkým klientom. Certifikačný orgán musí overiť implementovanie zmien u svojich klientov a musí prijať schémou požadované opatrenia.

POZNÁMKA. – Na zabezpečenie implementovania týchto požiadaviek môžu byť nevyhnutné zmluvné dojednania s klientmi. Vzor licenčnej zmluvy na potreby certifikácie, vrátane aspektov týkajúcich sa oznámenia o zmenách, ak je to vhodné, sa uvádza v ISO / IEC Guide 28: 2004, príloha E.

7.10.2 Certifikačný orgán musí zvážiť aj iné zmeny, ktoré ovplyvňujú certifikáciu, vrátane zmien iniciovaných klientom, a musí rozhodnúť o vhodnej činnosti.

POZNÁMKA. – Zmeny ovplyvňujúce certifikáciu môžu obsahovať nové informácie týkajúce sa plnenia certifikačných požiadaviek získaných certifikačným orgánom po tom, ako bola certifikácia stanovená.

7.10.3 Činnosti na implementovanie zmien ovplyvňujúcich certifikáciu musia obsahovať, v prípade potreby, nasledujúce:

- vyhodnotenie (pozri 7.4);
- preskúmanie (pozri 7.5);
- rozhodnutie (pozri 7.6);
- vydanie revidovanej formálnej certifikačnej dokumentácie (pozri 7.7) s cieľom rozšíriť alebo zúžiť predmet certifikácie;
- vydanie certifikačnej dokumentácie revidovaných dozorných činností (v prípade dozoru je súčasťou certifikačnej schémy).

13. PRAVIDLÁ TÝKAJÚCE SA NEDODRŽIAVANIA PREDPISOV

ODKAZ(Y) NA ČLÁNOK(-KY) CSA

Článok 54.1. *Európska schéma certifikácie kybernetickej bezpečnosti obsahuje aspoň tieto prvky:*
l) pravidlá týkajúce sa dôsledkov pre produkty IKT, služby IKT a procesy IKT, ktoré boli certifikované alebo pre ktoré bolo vydané EÚ vyhlásenie o zhode , ale ktoré nespĺňajú požiadavky schémy.

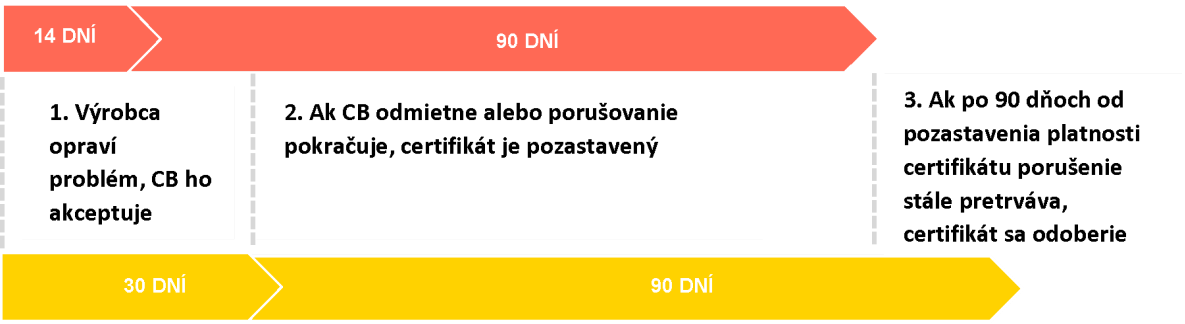
Článok 56.8. *Držiteľ európskeho certifikátu kybernetickej bezpečnosti informuje autoritu uvedenú v odseku 7 o všetkých následne zistených zraniteľnostiach alebo nezrovnalostiach týkajúcich sa bezpečnosti certifikovaného produktu IKT, služby IKT alebo procesu IKT, ktoré môžu mať vplyv na ich súlad s požiadavkami týkajúcimi sa certifikácie. Uvedená autorita alebo orgán bez zbytočného odkladu postúpi uvedené informácie dotknutej národnej autorite pre certifikáciu kybernetickej bezpečnosti.*

Bez toho, aby boli dotknuté činnosti NCCA vymedzené v článkoch 58.7 a 58.8 CSA a uvedené v kapitole 11, PRAVIDLÁ MONITOROVANIA SÚLADU, dôsledky pre produkty IKT, ktoré boli certifikované, ale nie sú v súlade s požiadavkami schémy, v rámci s prípadov vymedzených v kapitole 11, PRAVIDLÁ MONITOROVANIA SÚLADU, sú uvedené nižšie.

V prípade potvrdených odchýlok alebo nezrovnalostí súvisiacich s nesúladom s požiadavkami týkajúcich sa certifikátu vydaného na ich produkt IKT zo strany výrobcu alebo poskytovateľa má to vo všeobecnosti nasledovné dôsledky:

- CAB, ktorý vydáva certifikát, požiada výrobcu alebo poskytovateľa o poskytnutie tvrdení a zmien v lehote 14 dní/30 dní v prípade certifikátov na úrovni záruky "vysoká/"významná" CSA, aby sa obnovil súlad;
- CAB preskúma poskytnuté tvrdenia a zmeny a prijme alebo zamietne ich; rozhodnutie sa zašle výrobcovi alebo poskytovateľovi;
- pokračujúce porušovanie týchto povinností vedie k pozastaveniu platnosti certifikátu pre produkt IKT a k dočasnému pozastaveniu žiadostí o certifikát, ktoré výrobca alebo poskytovateľ predloží CAB, pričom CAB o tom informuje NCCA;
- ak sa riešenie odmietne alebo pozastavenie dosiahne 90 dní, certifikát sa odoberie.

***Obrázok 4**: Časový harmonogram riešenia nesúladu pri uplatňovaní požiadaviek súvisiacich s certifikátom*



V konkrétnom prípade potvrdenej odchýlky od požiadaviek vzhľadom k povinnostiam držiteľa certifikátu týkajúcich sa udržiavania platnosti certifikátu alebo informovania príslušných autorít alebo orgánov
o akýchkoľvek následne zistených zraniteľnostiach, ako sa vyžaduje v článku 56.8 CSA:

- okamžité pozastavenie platnosti certifikátu sa začne v okamihu, keď vydavateľ certifikátu oznámi vlastníkovi certifikátu, pričom maximálna doba pozastavenia platnosti certifikátu je 14 dní/30 dní pre certifikáty na úrovni záruky "vysoká"/"významná" podľa CSA;
- počas tohto obdobia:
  - nesúlad sa overí alebo vyvráti s potrebnou podporou[21] výrobcu alebo poskytovateľa;
  - ak sa overí, že nezhoda má vplyv na certifikát, považuje sa to za nezhodu certifikovaného

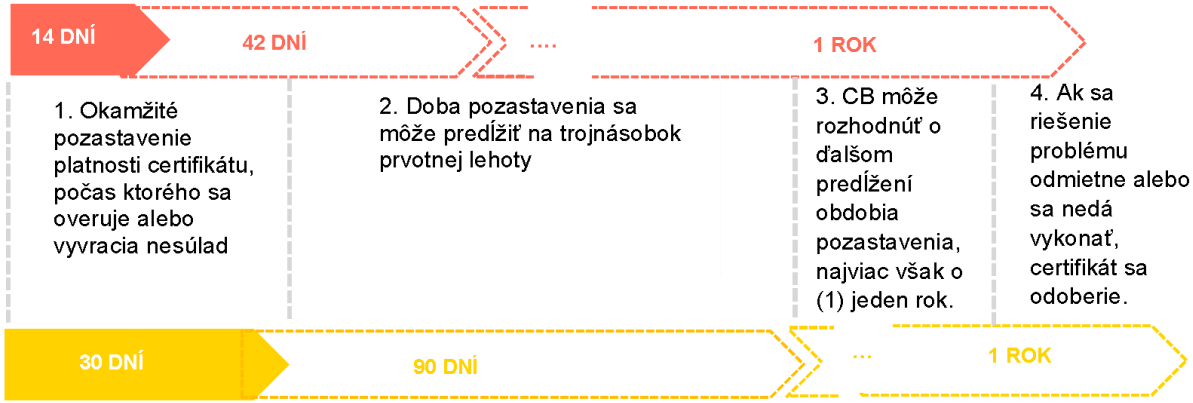
[21] V prípade potreby podpora znamená finančnú podporu opísaných činností.

produktu IKT;

- o výrobca alebo poskytovateľ produktu IKT akceptuje alebo odmietne riešenie overenej nezhody súvisiacej s produktom a potrebné činnosti údržby, ako je definované v kapitole 12, PODMIENKY VYDÁVANIA, UDRŽIAVANIA, POKRAČOVANIA A OBNOVOVANIA CERTIFIKÁTOV; ak vymedzené obdobie nepostačuje na vyššie opísanú úlohu, vydavateľ certifikátu môže na základe odôvodnenej žiadosti predĺžiť obdobie pozastavenia, najviac však na trojnásobok vyššie uvedenej lehoty;

- ak sa riešenie odmietne, certifikát sa odoberie;
- keď je riešenie prijaté, výrobca alebo poskytovateľ pristúpi k potrebným zmenám produktu IKT a CB k súvisiacim úpravám stavu certifikátu;
- v závislosti od technického charakteru a naliehavosti zmien CB rozhodne, či sa zmeny spracujú podľa požiadaviek stanovených v kapitole 12, PODMIENKY VYDÁVANIA, UDRŽIAVANIA, POKRAČOVANIA A OBNOVOVANIA CERTIFIKÁTOV, alebo podľa riešenia správy záplat definovaného v kapitole 14, PRAVIDLÁ TÝKAJÚCE SA RIEŠENIA ZRANITEĽNOSTÍ;
- v prípade potreby (napr. nedostatočná dostupnosť CB) môže CB rozhodnúť o ďalšom predĺžení obdobia pozastavenia najviac o jeden (1) rok.

***Obrázok 5**: Časový harmonogram riešenia nesúladu v prípade potvrdenej odchýlky od požiadaviek vzhľadom k povinnostiam držiteľa certifikátu týkajúcich sa zachovania platnosti certifikátu alebo informovania príslušných autorít alebo orgánov o akýchkoľvek následne zistených zraniteľnostiach*



Na začiatku obdobia pozastavenia je vlastník certifikátu informovaný o dĺžke tohto obdobia, dôvode pozastavenia a možných dôsledkoch. Stav pozastavenia certifikátu sa oznámi NCCA a sprístupní agentúre ENISA na uverejnenie na jej webovej stránke.

V prípade potvrdeného nesúladu s podmienkami, za ktorých sa certifikácia vykonáva a ktoré sa netýkajú jednotlivého produktu IKT, príslušná CB pod kontrolou svojho NCCA postupuje takto:

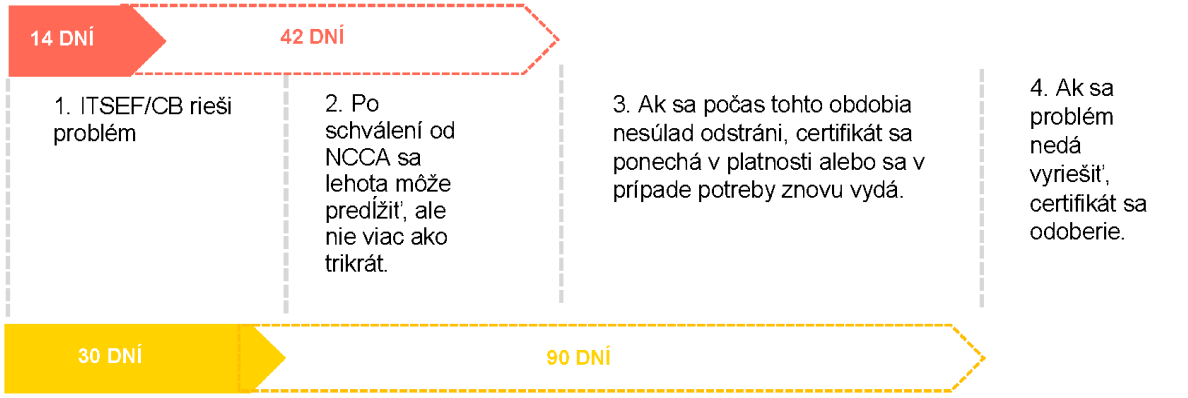
- identifikácia potenciálne ovplyvnených certifikovaných produktov IKT s podporou[22] príslušného ITSEF;
- ak to CB považuje za potrebné alebo podľa uváženia NCCA, žiadosť o sériu úloh hodnotenia, ktoré má vykonať na jednom alebo viacerých produktoch buď ITSEF, ktorý vykonal hodnotenie, alebo akýkoľvek iný ITSEF, ktorý by mal lepšie technické predpoklady na podporu tejto identifikácie;
- analýza príslušných hodnotiacich správ zo strany CB a v prípade potreby opätovné vydanie certifikátov v súlade s požiadavkami kapitoly 12, PODMIENKY VYDÁVANIA, UDRŽIAVANIA, POKRAČOVANIA A OBNOVOVANIA CERTIFIKÁTOV alebo notifikáciu výrobcom poskytovateľov produktov o vplyve nezhody na ich certifikáty.

Tieto činnosti sa vykonajú v lehote maximálne 14 dní/30 dní pre certifikáty na úrovni záruky "vysoká"/"významná" podľa CSA, ktorú možno predĺžiť len so súhlasom NCCA, najviac však na trojnásobok vyššie uvedenej lehoty. Ak sa počas tejto doby nesúlad odstráni, potom sa v certifikáte buď pokračuje, obnoví sa alebo sa znovu vydá v súlade s kapitolou 12, PODMIENKY VYDÁVANIA, UDRŽIAVANIA, POKRAČOVANIA A OBNOVOVANIA CERTIFIKÁTOV. Ak sa problémy nedajú vyriešiť, certifikát sa odoberie.

[22] V prípade potreby podpora znamená finančnú podporu opísaných činností.

Ak CB alebo NCCA nariadi vykonanie nových hodnotiacich činností, podporí ich[23] CB alebo ITSEF, ktorý preukázal, že nie je v súlade s predpismi.

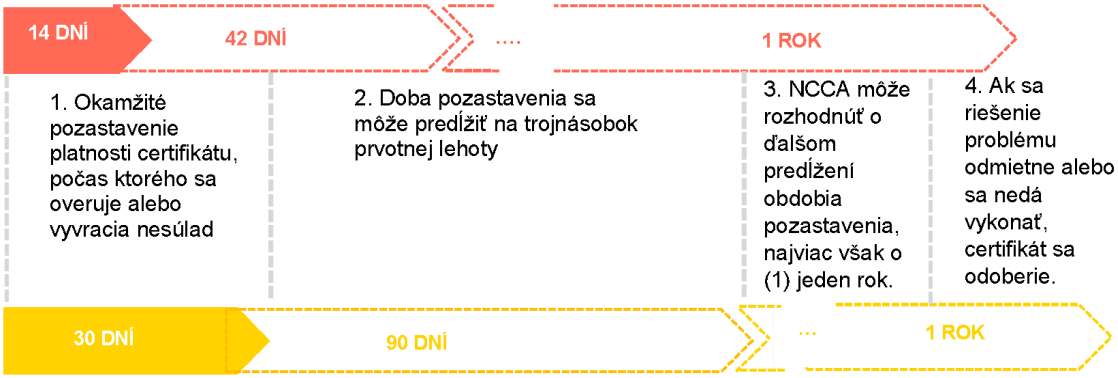
***Obrázok 6**: Časový harmonogram riešenia nezhôd v podmienkach, za ktorých sa vykonáva certifikácia*



Ak sa potvrdí, že vplyvy ovplyvňujú platnosť certifikátu, považujú sa za nezhodu certifikovaného produktu IKT:

- okamžité pozastavenie platnosti certifikátu sa začne v okamihu, keď vydavateľ certifikátu oznámi vlastníkovi certifikátu, pričom maximálna doba pozastavenia platnosti certifikátu je 14 dní/30 dní pre certifikáty na úrovni záruky "vysoká"/"významná" podľa CSA;
- počas tohto obdobia:
  - výrobca alebo poskytovateľ produktu IKT akceptuje alebo odmietne riešenie overených vplyvov súvisiacich s produktom; ak vymedzené obdobie nepostačuje na vyššie opísanú úlohu, NCCA môže na základe odôvodnenej žiadosti predĺžiť obdobie pozastavenia, najviac však na trojnásobok vyššie uvedenej lehoty;
- ak sa riešenie odmietne, certifikát sa odoberie;
- keď je riešenie prijaté, výrobca alebo poskytovateľ pristúpi k potrebným zmenám produktu IKT a CB k súvisiacim úpravám stavu certifikátu;
  - v závislosti od technického charakteru a naliehavosti zmien CB rozhodne, či sa zmeny spracujú podľa požiadaviek stanovených v kapitole 12, PODMIENKY VYDÁVANIA, UDRŽIAVANIA, POKRAČOVANIA A OBNOVENIA CERTIFIKÁTOV, alebo podľa riešenia správy záplat definovaného v kapitole 14, PRAVIDLÁ TÝKAJÚCE SA RIEŠENIA ZRANITEĽNOSTÍ;
- v prípade potreby (napr. nedostatočná dostupnosť CB) môže NCCA rozhodnúť o ďalšom predĺžení obdobia pozastavenia, najviac však o jeden rok.

***Obrázok 7:** Časový harmonogram riešenia nezhôd v podmienkach, v ktorých sa vykonáva certifikácia a v ktorých sa potvrdili vplyvy ovplyvňujúce platnosť certifikátu*



Dôsledky potvrdených nesúladov v podmienkach, za ktorých prebieha certifikácia a ktoré sa netýkajú jednotlivých produktov IKT, NCCA oznámi ECCG.

[23] V prípade potreby podpora znamená finančnú podporu opísaných činností.

Ak sú dôsledky spojené s predtým nezistenými zraniteľnosťami, postupuje sa v súlade s požiadavkami stanovenými v kapitole 14, PRAVIDLÁ TÝKAJÚCE SA RIEŠENIA ZRANITEĽNOSTÍ.

Ak vydavateľ certifikátu odoberie certifikát, urobí tak v súlade s podmienkami definovanými v článku 58.8 písm. e) CSA pre certifikáty stanovené na úrovni záruky "vysoká" CSA.

Propagácia certifikátov, ktoré boli pozastavené alebo odobraté pre ich produkty IKT, výrobcami alebo poskytovateľmi nie je povolená.

ZÁKLADNÉ INFORMÁCIE

Dôsledky pre produkty IKT, ktoré boli certifikované, ale nespĺňajú požiadavky schémy, sú definované podľa prípadov nesúladu stanovených v kapitole 11, PRAVIDLÁ MONITOROVANIA SÚLADU. Zohľadňujú aj povinnosti uvedené v článku 56 ods. 8: "*Držiteľ európskeho certifikátu kybernetickej bezpečnosti informuje orgán alebo subjekt uvedený v odseku 7 o všetkých následne zistených zraniteľnostiach*".

Status pozastavenia certifikátov sa zavádza s cieľom umožniť potrebnú analýzu vplyvov posudzovaných zlyhaní pred tým, ako sa rozhodne o akomkoľvek inom opatrení súvisiacom so zmenou statusu certifikátu v súlade s pravidlami kapitoly 12, PODMIENKY VYDÁVANIA, UDRŽIAVANIA, POKRAČOVANIA A OBNOVOVANIA CERTIFIKÁTOV.

V prípade potreby si takáto analýza môže vyžadovať potrebnú podporu vydavateľov certifikátov a ich skúšobných laboratórií a/alebo držiteľov certifikátov.

Dočasné pozastavenie alebo obmedzenie žiadosti o certifikát pre produkt alebo zo strany vývojára bolo zavedené pri opakovanom porušení povinností schémy zo strany vývojára: CAB môže pozastaviť alebo obmedziť prístup vývojára k certifikačným činnostiam schémy, kým CAB opätovne nepredloží dostatočné dôkazy o dodržiavaní povinností vývojára a kým ich nepotvrdí NCCA.

Dôsledky nedodržania podmienok, za ktorých sa certifikácia vykonáva a ktoré sa netýkajú jednotlivých produktov IKT, sú tu definované pre príslušné certifikáty. Dôsledky pre CAB a ich skúšobné laboratóriá tu nie sú definované a mali by sa posudzovať v rámci zodpovednosti NCCA za dohľad nad ich činnosťami, ako je definované v článku 58 CSA.

Pravidlá týkajúce sa zaobchádzania s predtým nezistenými zraniteľnosťami sú definované v kapitole 14, PRAVIDLÁ TÝKAJÚCE SA RIEŠENIA ZRANITEĽNOSTÍ, a preto sa tu neopakujú.

14. PRAVIDLÁ TÝKAJÚCE SA RIEŠENIA ZRANITEĽNOSTÍ

ODKAZ(-Y) NA ČLÁNOK(-KY) CSA

Článok 54 1. *Európska schéma certifikácie kybernetickej bezpečnosti obsahuje aspoň tieto prvky:*

m) pravidlá nahlasovania a riešenia predtým nezistených zraniteľností produktov IKT, služieb IKT a procesov IKT z hľadiska kybernetickej bezpečnosti.

Článok 55 .1. *Výrobca alebo poskytovateľ certifikovaných produktov IKT, služieb IKT alebo procesov IKT alebo produktov IKT, služieb IKT a procesov IKT, pre ktoré bolo vydané EÚ vyhlásenie o zhode, zverejní tieto doplňujúce informácie o kybernetickej bezpečnosti*:

(a) kontaktné informácie výrobcu alebo poskytovateľa a akceptované metódy na prijímanie informácií o zraniteľnosti od koncových užívateľov a výskumníkov v oblasti bezpečnosti;

(b) odkaz na registre online, ktoré uvádzajú zverejnené zraniteľnosti týkajúce sa daného produktu IKT, služby IKT alebo procesu IKT, a všetky príslušné kybernetickobezpečnostné rady.

Článok 56.8. *Držiteľ európskeho certifikátu kybernetickej bezpečnosti informuje autoritu uvedenú v odseku 7 o všetkých následne zistených zraniteľnostiach alebo nezrovnalostiach týkajúcich sa bezpečnosti certifikovaného produktu IKT, služby IKT alebo procesu IKT, ktoré môžu mať vplyv na ich súlad s požiadavkami týkajúcimi sa certifikácie. Uvedená autorita alebo orgán bez zbytočného odkladu postúpi uvedené informácie dotknutej národnej autorite pre certifikáciu kybernetickej bezpečnosti.*

Riešenie zraniteľnosti

Výrobcovia alebo poskytovatelia produktov IKT používajú všeobecné kroky podľa normy ISO/IEC 30111 pre riešenie zraniteľností: príprava, prijatie, overenie, vývoj nápravných opatrení, vydanie, po vydaní, pričom pre schému EUCC platia tieto osobitné pravidlá.

1 PRÍPRAVA

Výrobcovia alebo poskytovatelia produktov IKT vypracujú metódy prijímania informácií o zraniteľnosti a zverejnia ich v súlade s článkom 55 ods. 1 písm. c) CSA.

2 PRIJATIE

V nasledujúcich prípadoch, keď:

- výrobca alebo poskytovateľ certifikovaného produktu IKT dostane informácie o zraniteľnosti podľa článku 55.1 písm. c) CSA;
- sa na uvedených online registre objavila nová zverejnená zraniteľnosť podľa článku 55.1 písm. d) CSA;
- výrobca alebo poskytovateľ zistí súvisiacu zraniteľnosť svojho certifikovaného produktu IKT iným spôsobom,

výrobca alebo poskytovateľ do jedného pracovného dňa oznámi certifikačnému orgánu (CB), ktorý vydal certifikát, možnosť súvisiacej zraniteľnosti a do piatich pracovných dní oznámi dátum, kedy bude vykonaná analýza zraniteľnosti.

Ak je informácia o možnej zraniteľnosti týkajúcej sa certifikovaného produktu IKT k dispozícii najskôr v CB, CB o tom do jedného pracovného dňa informuje výrobcu alebo poskytovateľa a do piatich pracovných dní požiada o analýzu zraniteľnosti a o termín tejto analýzy.

CB sa dohodne na navrhovanom termíne, ktorý však nesmie presiahnuť 90 dní. Ak obe strany považujú za potrebné alebo sa nemôžu dohodnúť na takomto dátume, môžu o tom informovať NCCA a požiadať ju o radu

Platnosť certifikátu sa pozastaví v týchto prípadoch, ak výrobca alebo poskytovateľ:
- neinformuje CB v dohodnutom termíne;
- neposkytne analýzu zraniteľnosti v dohodnutom termíne;
- neodpovie na žiadosť CB v rámci vopred dohodnutej lehoty, napr. do piatich pracovných dní.

3 OVERENIE

Analýza zraniteľnosti sa zdokumentuje a dokumentácia sa uchováva najmenej päť rokov pre všetky strany.

Musí obsahovať výpočet potenciálu útoku podľa kapitoly 3 NORMY POUŽITÉ PRI HODNOTENÍ, ktorý môže preskúmať ITSEF. Tento výpočet potenciálu útoku musí pomôcť pri rozhodovaní, či je zraniteľnosť zostatková alebo zneužiteľná na zvolenej úrovni AVA_VAN pre certifikát.

Uvedie sa, či je zraniteľnosť pre certifikovaný produkt IKT vyvrátená alebo potvrdená.

V prípade potreby môže výrobca alebo poskytovateľ pred ukončením výpočtu požiadať zdroj(-e) informácií o ďalšie informácie.

V prípade, že sa zraniteľnosť vyvráti, proces sa zastaví a informácie sa uchovajú pre prípadné ďalšie vyšetrovanie.

V prípade, že sa zraniteľnosť potvrdí a vzťahuje sa na produkt, uplatňujú sa nasledujúce odseky.

Analýza zraniteľnosti musí obsahovať posúdenie vplyvu na produkt IKT a možné riešenie (riešenia) zraniteľnosti s týmito informáciami:
- možné riziká spojené s blízkosťou alebo dostupnosťou možného útoku;
- úroveň zmien, ktoré sa budú musieť uplatňovať v súlade s prílohou 11, KONTINUITA ZÁRUKY.

Informácie môžu obsahovať podrobnosti o možnom zneužití zraniteľnosti: v takom prípade musia byť označené príslušnou TLP klasifikáciou, aby sa zabezpečila príslušná ochrana v súlade so štandardnými pravidlami definovanými na stránke https://www.first.org/tlp/.

Alternatívne ku TLP klasifikácii sa môže použiť PRÍLOHA 2 MSSR 9.1.3 Klasifikácia informácií, údajov a materiálov. Norma ISO 29147 uvádza aj TLS, S/MIME a PGP ako typické bezpečnostné mechanizmy, ktoré možno tiež zvážiť

Analýza sa zašle CB, ktorý ju schváli, a môže viesť k záveru, že zraniteľnosť nemožno obísť. V takom prípade sa certifikát odoberie. Ak analýza dospeje k záveru, že zraniteľnosť možno obísť, certifikát sa pozastaví a uplatnia sa nasledujúce opatrenia.

CB informuje NCCA o overených informáciách o zraniteľnosti.

Pri monitorovaní platných certifikátov zo strany NCCA sa pri výbere vzoriek certifikátov, ktoré sa majú opätovne posúdiť, zohľadní počet nevybavených takýchto analýz zraniteľnosti.

4 VÝVOJ NÁPRAVNÝCH OPATRENÍ

Certifikovaný produkt IKT môže obsahovať mechanizmus správy záplat, ako je definovaný v prílohe 15, SPRÁVA ZÁPLAT, ktorý je určený na skúšobné použitie[24] a ktorý bol posúdený v rámci jeho certifikácie: potom sa uplatňujú súvisiace podmienky.

Ak certifikovaný produkt IKT neobsahuje takýto mechanizmus správy záplat, postup údržby opísaný v kapitole 12, PODMIENKY VYDÁVANIA, UDRŽIAVANIA, POKRAČOVANIA A OBNOVOVANIA CERTIFIKÁTOV a súvisiace činnosti definované v prílohe 11, KONTINUITA ZÁRUKY, sa uplatňujú na overenie správnosti zmien vykonaných na pokrytie zraniteľnosti a na opätovné vydanie všetkých potrebných aktualizovaných certifikátov.

V oboch prípadoch výrobca alebo poskytovateľ prijme rozhodnutie o náprave a vykoná potrebné zmeny v produkte IKT, ktoré sa testujú v súlade s prílohou 15 alebo prílohou 11. Vykoná sa aj testovanie bez regresie, aby sa zabezpečila ďalšia možnosť zavedenia novej opravy.

[24] Ako je definované v kapitole 8, ŠPECIFICKÉ KRITÉRIA HODNOTENIA A METÓDY HODNOTENIA.

5 VYDANIE A PO VYDANÍ

Ak boli nápravné opatrenia a súvisiace zmeny produktu IKT vyhlásené za vhodné na nasadenie, výrobca alebo poskytovateľ priamo pristúpi k ich nasadeniu alebo k ich vydaniu v súlade s požiadavkami článku 55.1 písm. d) CSA.

Okrem toho sa na základe analýzy príčin zraniteľnosti aktualizuje životný cyklus zabezpečenia produktu IKT.

Zverejnenie zraniteľnosti

Výrobcovia alebo poskytovatelia produktov IKT môžu pre všeobecné pravidlá týkajúce sa zverejňovania zraniteľností používať túto normu:

- ISO/IEC 29147 Informačné technológie - Bezpečnostné techniky - Zverejňovanie zraniteľností.

Počas analýzy zraniteľnosti môže výrobca uplatniť obdobie embarga, čo znamená, že prípadná zraniteľnosť nebude ďalej zverejnená. Toto obdobie nesmie trvať dlhšie ako jeden (1) mesiac. NCCA však môže zvážiť predĺženie tohto obdobia, ak dostane odôvodnenú žiadosť, najmä ak sa potvrdí, že je potrebné poskytnúť čas predajcom na nižších úrovniach, ktorí integrujú produkt alebo službu, na analýzu vplyvu zraniteľnosti (z technického aj certifikačného hľadiska).

Okrem vyššie uvedených všeobecných pravidiel zverejňovania informácií sa po definovaní stratégie na odstránenie problému výrobcom alebo poskytovateľom so súhlasom CB alebo hneď po prijatí rozhodnutia, že zraniteľnosť nemožno zmierniť, informácie týkajúce sa potvrdenej zraniteľnosti zverejnia NCCA v súlade s článkom 56.8) CSA.

Informácie nesmú obsahovať podrobnosti o možnom zneužití zraniteľnosti. Obsahuje prvky potrebné na to, aby NCCA pochopil vplyv zraniteľnosti, zmeny, ktoré sa majú vykonať v produkte, a prípadne informácie CB o širšej uplatniteľnosti zraniteľnosti na iné certifikované produkty.

NCCA v súlade s článkom 58 ods. 7 písm. h) zdieľa tieto informácie s ostatnými NCCA, ktoré sa môžu tiež rozhodnúť ďalej analyzovať problém alebo po informovaní výrobcu alebo poskytovateľa produktu IKT o výmene informácií požiadať súvisiace CAB, aby analyzovali, či sú dotknuté ďalšie certifikované produkty. Táto výmena informácií sa uskutočňuje dôverne (šifrovane).

Keď sa na certifikovanom produkte vykoná oprava, výrobca alebo poskytovateľ zriadi potrebnú CVE s podporou NCCA a príslušného národného CSIRT a pristúpi k jej uverejneniu v príslušnom zozname v súlade s požiadavkami článku 55 CSA. Agentúra ENISA musí byť informovaná o zmenách stavu príslušných certifikátov.

NCCA môžu rozvíjať svoje kapacity, aby mohli pôsobiť ako "koordinátori", ako je definované v norme ISO/IEC 29147, prípadne môžu na plnenie tejto úlohy určiť svoj národný CSIRT. V takom prípade má CSIRT prístup k potrebným podrobnostiam týkajúcim sa zraniteľností a certifikovaných produktov IKT.

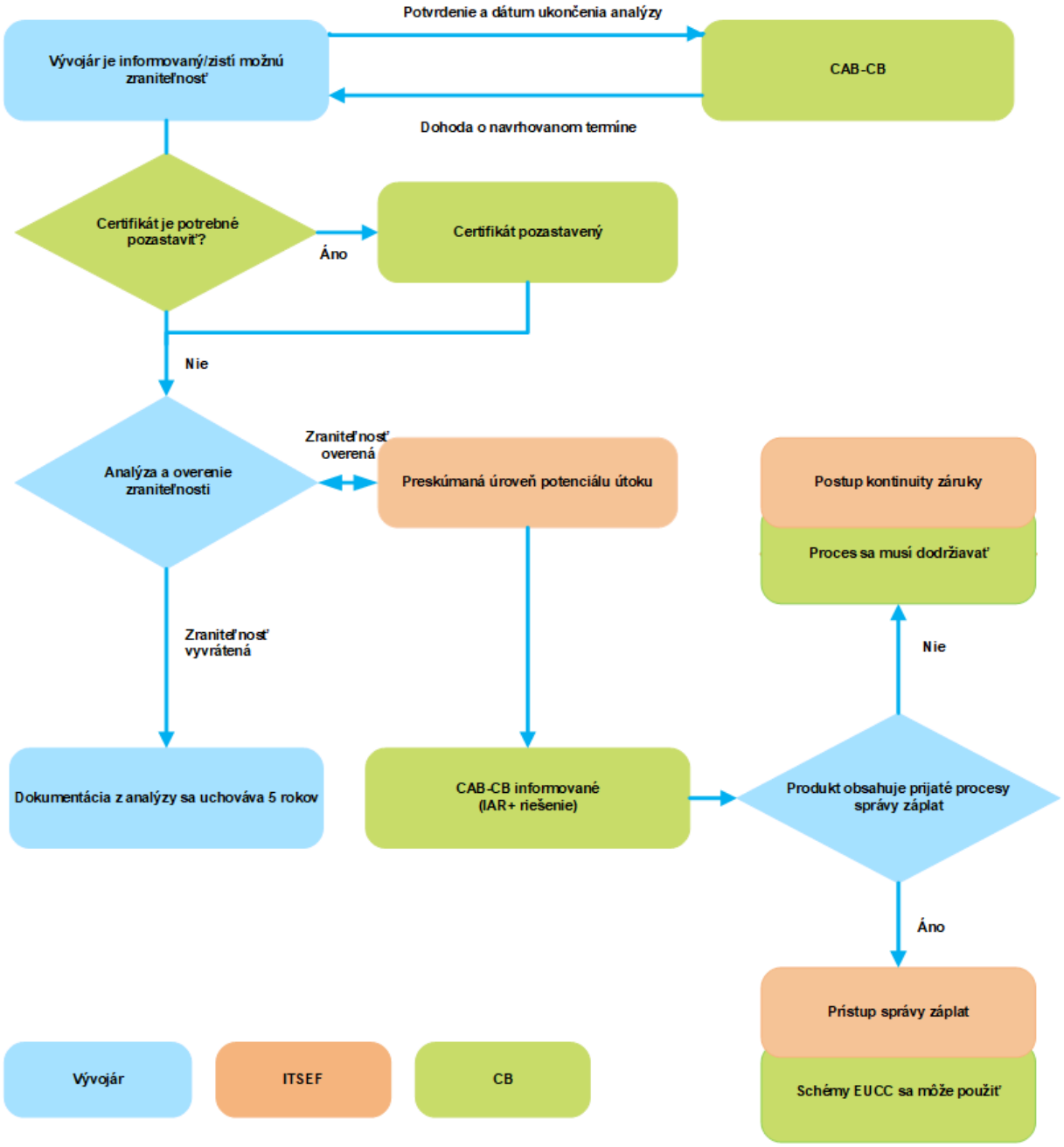
ZÁKLADNÉ INFORMÁCIE

Procesy spracovania a zverejňovania zraniteľností schémy EUCC sú založené na normách ISO ISO/IEC 30111 a ISO/IEC 29147. Keďže však tieto normy neobsahujú žiadnu bezpečnostnú záruku o tom, či vyvinuté a nasadené nápravné opatrenia nezavádzajú nové zraniteľnosti, a nedefinujú žiadne úlohy pre hodnotiaci orgán tretej strany a jeho metodiku, boli do tejto kapitoly, ako aj do kapitoly 15, SPRÁVA ZÁPLAT, uvedené dodatočné informácie na pokrytie týchto nedostatkov.

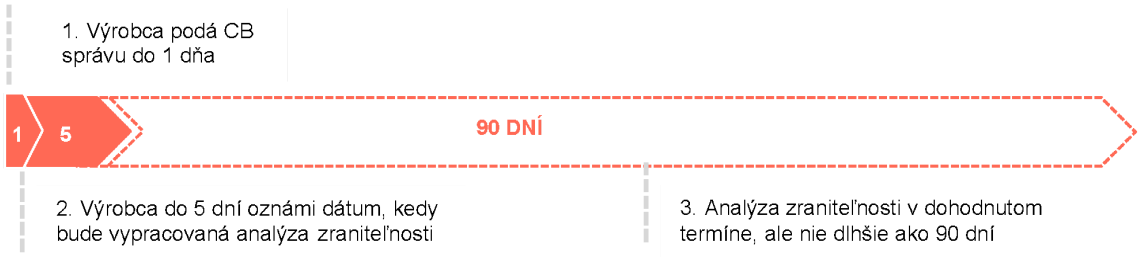
Okrem už prijatých metodík opísaných v prílohe 11 schémy EUCC pridáva aj nové metódy spracovania procesov zraniteľnosti a zverejnenia a správy záplat.

Nasledujúci obrázok poskytuje prehľad tohto procesu:

***Obrázok 8**: Procesy spracovania a zverejňovania zraniteľností*



***Obrázok 9:** Časová os všeobecného riešenia zraniteľnosti*



15. UCHOVÁVANIE ZÁZNAMOV CAB

ODKAZ(-Y) NA ČLÁNOK(-KY) CSA

Článok 54 1. *Európska schéma certifikácie kybernetickej bezpečnosti obsahuje aspoň tieto prvky:*

n) prípadne pravidlá týkajúce sa uchovávania záznamov orgánmi posudzovania zhody.

Každý CAB musí viesť systém záznamov v súlade s požiadavkami platnej akreditačnej normy ISO/IEC 17065 alebo ISO/IEC 17025 pre svoju činnosť.

Systém záznamov musí obsahovať všetky záznamy a iné dokumenty vyhotovené v súvislosti s každou certifikáciou; musí byť dostatočne úplný, aby umožňoval sledovanie priebehu každej certifikácie.

Všetky záznamy sa bezpečne a prístupne uchovávajú najmenej päť (5) rokov po uplynutí platnosti certifikátu.

V prípade, že bol pridelený iný dátum skončenia platnosti certifikátu v súlade s podmienkami kapitoly 12, PODMIENKY VYDÁVANIA, UDRŽIAVANIA, POKRAČOVANIA A OBNOVOVANIA CERTIFIKÁTOV, zohľadní sa pri novom výpočte doby uchovávania záznamov, pričom platí rovnaké pravidlo, ako bolo uvedené predtým. Nové alebo revidované informácie týkajúce sa činností opísaných v kapitole 12, PODMIENKY VYDÁVANIA, UDRŽIAVANIA, POKRAČOVANIA A OBNOVOVANIA CERTIFIKÁTOV sa pridajú k predchádzajúcim záznamom o certifikáte.

ZÁKLADNÉ INFORMÁCIE

Normy ISO/IEC 17065 a ISO/IEC 17025 už stanovujú požiadavky týkajúce sa uchovávania záznamov počas celého obdobia platnosti certifikátu. Aby bolo možné zvládnuť prípadné obchodné spory, odporúča sa predĺžiť obdobie uchovávania záznamov po uplynutí platnosti certifikátu. Dodatočné obdobie piatich (5) rokov je v súčasnosti bežnou praxou.

Proces údržby, recertifikácie a opätovného hodnotenia zo strany CAB môže zmeniť dátum skončenia platnosti certifikátu. Tento nový dátum skončenia platnosti sa musí uplatniť na uchovávanie záznamov vytvorených v rámci tohto procesu. Keďže platnosť certifikátu nemusí mať pevnú hodnotu, odporúčalo sa stanoviť požiadavku po uplynutí platnosti certifikátu, aby bolo možné riadiť prípadné obchodné spory.

16. NÁRODNÉ ALEBO MEDZINÁRODNÉ SCHÉMY

ODKAZ(-Y) NA ČLÁNOK(-KY) CSA

Článok 1.2. *Týmto nariadením nie sú dotknuté kompetencie členských štátov týkajúce sa činností spojených s verejnou bezpečnosťou, obranou, národnou bezpečnosťou a činností štátu v oblasti trestného práva.*

Článok 54 1. *Európska schéma certifikácie kybernetickej bezpečnosti obsahuje aspoň tieto prvky:*

o) určenie národných alebo medzinárodných schém certifikácie kybernetickej bezpečnosti, ktoré sa vzťahujú na rovnaký typ alebo kategórie produktov IKT, služieb IKT a procesov IKT, bezpečnostných požiadaviek, kritérií a metód hodnotenia a úrovne záruky.

Článok 57 1. *Bez toho, aby bol dotknutý odsek 3 tohto článku, národné schémy certifikácie kybernetickej bezpečnosti a súvisiace postupy týkajúce sa produktov IKT, služieb IKT a procesov IKT, na ktoré sa vzťahuje európska schéma certifikácie kybernetickej bezpečnosti, strácajú účinnosť k dátumu stanovenému vo vykonávacom akte prijatom podľa článku 49 ods. 7. Národné schémy certifikácie kybernetickej bezpečnosti a súvisiace postupy týkajúce sa produktov IKT, služieb IKT a procesov IKT, na ktoré sa európska schéma certifikácie kybernetickej bezpečnosti nevzťahuje, existujú naďalej.*

Článok 57 3. *Existujúce certifikáty, ktoré boli vydané v rámci národných schém certifikácie kybernetickej bezpečnosti a na ktoré sa vzťahuje európska schéma certifikácie kybernetickej bezpečnosti, platia naďalej až do konca doby ich platnosti.*

Nasledujúce certifikačné schémy založené na spoločných kritériách sa vzťahujú na rovnaký typ alebo kategóriu produktov IKT, bezpečnostné požiadavky, kritériá a metódy hodnotenia a úrovne záruky:

V rámci EÚ:

- Francúzska schéma, ktorú prevádzkuje ANSSI: https://www.ssi.gouv.fr/administration/produits-certifies/cc/
- Nemecká schéma, ktorú prevádzkuje BSI: https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachC C/zertifizierungnachcc_node.html
- Talianska schéma, ktorú prevádzkuje OCSI: www.ocsi.isticom.it/
- Holandská schéma, ktorú prevádzkujú TÜV Rheinland NL a NLNCSA: http://www.tuv-nederland.nl/nl/17/common_criteria.html
- Španielska schéma, ktorú prevádzkuje CCN: https://oc.ccn.cni.es/
- Švédska schéma, ktorú prevádzkuje FMV: http://fmv.se/en/Our-activities/CSEC---The-Swedish-Certification-Body- for-IT-Security/

Štáty Európskeho hospodárskeho priestoru (EHP) Európskeho združenia voľného obchodu (EZVO),:

- Nórska schéma, ktorú prevádzkuje SERTIT: http://www.sertit.no/

Niektoré z týchto schém nemusia v súčasnosti pokrývať všetky technické domény definované v kapitole 4, ÚROVNE ZÁRUKY. Tieto informácie možno získať na nasledujúcej stránke SOG-IS MRA: https://www.sogis.eu/uk/status_participant_en.html.

Vzhľadom na možnosť, že :

- certifikát vydaný v rámci týchto schém by sa v prípade potreby[25] mohol zmeniť na certifikát v rámci schémy EUCC, ak sa vykonajú potrebné činnosti;
- CB môže súhlasiť s opätovným použitím výsledkov hodnotiacich činností vykonaných v rámci týchto schém na certifikáciu v rámci schémy EUCC;
- Certifikát vydaný v rámci týchto schém sa môže opätovne použiť na zložené certifikácie v rámci schémy EUCC až do skončenia jeho platnosti, ak sa pri hodnotení potvrdí, že zložený produkt IKT

[25] Splnenie požiadaviek trhu alebo regulačných požiadaviek.

spĺňa všetky požiadavky schémy EUCC;
Agentúra ENISA môže vypracovať súvisiace usmernenia na podporu podmienok spojených s týmito možnosťami, ako je vymedzené v kapitole 25, ODPORÚČANIA AHWG. Toto usmernenie sa vypracuje v spolupráci s ECCG.

Na základe odporúčaní stanovených v tejto kapitole môžu Európska komisia a členské štáty EÚ zvážiť stanovenie dátumu dvoch (2) rokov po prijatí vykonávacieho aktu podľa článku 49 ods. 7, aby existujúce schémy prestali byť účinné.

Niektoré z týchto schém môžu vykonávať certifikačné činnosti, ktoré sa vzťahujú na rovnaký typ alebo kategóriu produktov IKT, bezpečnostné požiadavky, kritériá a metódy hodnotenia a presahujú rozsah pôsobnosti schémy EUCC, pokiaľ ide o úrovne záruky (napr. ak pre schému EUCC ešte nebola definovaná/pripojená žiadna technická doména/žiadny špecifický ochranný profil na tento účel pre certifikáty súvisiace s AVA_VAN.4 alebo 5).

Príslušné certifikáty sa v rámci schémy EUCC nevydávajú.

Nasledujúce medzinárodné schémy zapojené do CCRA sa vzťahujú na rovnaký typ alebo kategóriu produktov IKT, bezpečnostné požiadavky, kritériá a metódy hodnotenia a nemusia sa týkať všetkých úrovní záruky schémy EUCC: https://www.commoncriteriaportal.org/ccra/schemes/?CFID=50893710&CFTOKEN=ccb21e6bbf0ccebe-BBE1E229-155D-00D0-0A23555C0903C74A

ZÁKLADNÉ INFORMÁCIE

Použitie existujúcich schém zavedených na certifikáciu produktov IKT pomocou spoločných kritérií by malo byť naďalej možné pre certifikácie, ktoré by nepatrili do rozsahu pôsobnosti schémy EUCC, či už na iné účely (napr. národná bezpečnosť) alebo nad rámec podmienok schémy (napr. certifikát AVA_VAN.4 alebo 5 pre produkt IKT, na ktorý sa nevzťahuje technická doména ani osobitný ochranný profil pripojený k tejto schéme, ako napr. čisto softvérový produkt). Takéto certifikáty by nemali niesť uznávaciu značku alebo štítok schémy EUCC.

Okrem týchto špecifických prípadov a v záujme využitia kombinovaných výhod spoločných kritérií a EUCC certifikácie, sa vlastníkom rizika, ktorí potrebujú certifikáciu podľa Spoločných Kritérií pre produkty IKT, odporúča, aby sa pre tieto produkty IKT použili tieto alebo rovnocenné požiadavky: "Certifikácia podľa spoločných kritérií [produktu IKT] sa vykoná podľa schémy EUCC alebo podľa schémy SOG-IS CC prevádzkovanej jedným z členských štátov EÚ, ak je vydanie certifikátu naplánované pred okamihom, keď sa začnú vydávať certifikáty podľa schémy EUCC."

Ak je produkt IKT certifikovaný schémou SOG-IS členského štátu pred tým, ako začne platiť schéma EUCC, vlastník rizika môže zvážiť dodatočnú požiadavku, aby sa žiadosť o certifikát EUCC certifikovaného produktu SOG-IS podala, keď začne platiť schéma EUCC. V skutočnosti je to deklarovaným cieľom tejto schémy, aby sa zabezpečila účinná konverzia certifikátu SOG-IS MRA.

Konverzia certifikátu SOG-IS MRA na schému EUCC a opätovné použitie certifikátov pre zloženie umožní efektívne opätovné použitie existujúcich certifikátov, čo si bude vyžadovať usmernenie, ako harmonizovaným spôsobom riešiť rozdiely medzi starými a novými schémami.

Na certifikátoch používaných pri zložení: uprednostňovaným riešením by malo byť, aby sa certifikáty používané pri zložení konvertovali do novej schémy. Ak sa to však neurobí z nejakého daného dôvodu, ktorý možno riešiť na úrovni zloženého produktu (napr. dostupnosť doplňujúcich informácií o kybernetickej bezpečnosti podľa článku 55 CSA, obsah a formát certifikátu...), je vhodné mať záložné riešenie, pri ktorom zložený produkt IKT môže "niesť váhu" potrebných zlepšení na dosiahnutie požiadaviek schémy EUCC.

17. OBSAH A FORMÁT CERTIFIKÁTOV

ODKAZ(-Y) NA ČLÁNOK(-KY) CSA

Článok 54 1. *Európska schéma certifikácie kybernetickej bezpečnosti obsahuje aspoň tieto prvky:*

p) obsah a formát európskych certifikátov kybernetickej bezpečnosti a vyhlásení o zhode EÚ , ktoré majú byť vydané.

Certifikát musí obsahovať aspoň tieto informácie:

- jedinečný identifikátor stanovený vydavateľom certifikátu;
- informácie týkajúce sa certifikovaného produktu IKT a jeho výrobcu alebo poskytovateľa:
  - názov produktu IKT a prípadne TOE;
  - typ produktu IKT a prípadne TOE;
  - verzia pre produkt IKT;
  - názov a kontaktné údaje výrobcu alebo poskytovateľa;
  - odkaz na webové sídlo výrobcu alebo poskytovateľa na prístup k doplnkovým informáciám o kybernetickej bezpečnosti certifikovaného produktu IKT v súlade s článkom 55 CSA;
- informácie týkajúce sa hodnotenia a certifikácie produktu IKT:
  - názov a kontaktné údaje orgánu alebo autority, ktorá certifikát vydala;
  - názov ITSEF, ktorý vykonal hodnotenie, ak sa líši od certifikačného orgánu;
  - názov zodpovednej NCCA;
  - odkaz na túto schému;
  - odkaz na správu o certifikácii spojenú s certifikátom;
  - dosiahnutú úroveň záruky z CSA (buď "významná", alebo "vysoká");
  - Verzia/vydanie CC použitá na hodnotenie;
  - identifikácia úrovne alebo balíka záruky z CC vrátane použitých komponentov záruk a úrovne AVA_VAN, na ktorú sa vzťahuje;
  - ak sa uplatňuje, uvádza sa odkaz na ochranný(-é) profil(y), ktorému(-ým) produkt IKT vyhovuje;
  - dátum vydania a obdobie platnosti Certifikátu;
- ak je k dispozícii, značka alebo štítok priradený k schéme, ako je definované v kapitole 10, ZNAČKY A ŠTÍTKY.

Ak sa certifikovaná časť produktu IKT (TOE) výrazne líši od produktu IKT, na perimetri TOE sa uvedie jasný údaj o informáciách týkajúcich sa certifikovaného produktu IKT; prípadne sa preto TOE môže identifikovať špecifickým názvom súvisiacim s jeho vyhradenou funkcionalitou v rámci produktu IKT a špecifickým typom.

Agentúra ENISA môže v spolupráci s ECCG poskytnúť usmernenie, ako určiť jedinečné identifikátory s cieľom uľahčiť používateľom prístup k histórii certifikátov spojených s produktom a jeho rôznymi verziami.

Ak sa uplatňuje, v balíku záruky sa rozlišuje medzi hodnotením úrovne záruky CC časť 3, ktoré je v zhode a rozšíreným hodnotením úrovne záruky CC časť 3, a to v súlade s podmienkami definovanými v prílohe 1.

Agentúra ENISA môže v spolupráci s ECCG poskytnúť usmernenia k taxonómii produktov IKT s cieľom ponúknuť harmonizovaný zoznam typov produktov IKT v celej EÚ. Po vytvorení takejto taxonómie:

- CAB posúdi, na ktorý typ sa certifikáty vzťahujú;
- NCCA môže definovať, pre ktoré konkrétne typy sa môžu využívať potenciálne predĺženie doby platnosti súvisiacich certifikátov, ako je definované v kapitole 19, OBDOBIE PLATNOSTI CERTIFIKÁTOV.

Každý certifikát podpíše príslušná zodpovedná osoba autority alebo orgánu a sprístupní ho NCCA a agentúre ENISA spolu s príslušnou správou o certifikácii v elektronickej forme a v anglickom jazyku. V prípade, že sú tieto dokumenty vyhotovené v inom ako anglickom jazyku, poskytne sa overený preklad.

Keď sa pre schému vytvorí značka, agentúra ENISA môže do certifikátu priradiť QR kód súvisiaci so značkou. Tento QR kód môže výrobca alebo poskytovateľ použiť spolu so štítkom v dokumentácii alebo na obale súvisiacom s certifikovaným produktom IKT.

Vydavateľ certifikátu vypracuje pre každý certifikát správu o certifikácii. Musí obsahovať aspoň informácie uvedené v prílohe 13 a musí obsahovať toto vyhlásenie o odmietnutí zodpovednosti:

Certifikácia alebo certifikát sa v plnej miere vzťahuje na požiadavky certifikácie kybernetickej bezpečnosti produktu v čase vydania certifikátu. Nesúvisí so samotným produktom.

Certifikácia nie je schválením produktu, obalu ani ničoho iného, čo súvisí s produktom, vyjadruje len to, že materiál a informácie súvisiace s kybernetickou bezpečnosťou produktu spĺňajú požiadavky tejto certifikácie. Neexistujú žiadne záruky týkajúce sa vhodnosti na daný účel alebo predajnosti, neprítomnosti chýb, omylov, presnosti, neporušovania práv duševného vlastníctva, práv spotrebiteľov a akýchkoľvek iných súvisiacich práv. Vydavateľ certifikátu alebo vlastník certifikačnej schémy kybernetickej bezpečnosti za žiadnych okolností nezodpovedá za priame, nepriame, materiálne, technické a s funkčnosťou IT súvisiace alebo morálne škody akéhokoľvek druhu, ktoré vznikli v súvislosti s produktom z dôvodu jeho nepoužívania alebo používania.

Žiadna strata dobrého mena, prerušenie práce, zlyhanie alebo porucha počítača, strata alebo poškodenie, zmeny, nesprávne použitie, zneužitie, úprava, zničenie, krádež, výkupné alebo akákoľvek iná forma neoprávneného prístupu k údajom alebo akákoľvek komerčná škoda nezakladá zodpovednosť vydavateľa certifikátu alebo navrhovateľa certifikačnej schémy alebo akejkoľvek inej organizácie, ktorá uznáva alebo uvádza do platnosti tento certifikát, s výnimkou hrubej nedbanlivosti alebo úmyselného konania spôsobeného fyzickými osobami pracujúcimi v rámci týchto inštitúcií.

ZÁKLADNÉ INFORMÁCIE

Obsah certifikátov EUCC je odvodený od obsahu certifikátov SOG-IS MRA a zahŕňa aj potrebné informácie súvisiace s novou schémou, ako je odkaz na doplňujúce informácie o kybernetickej bezpečnosti v súlade s článkom 55 CSA, ako aj prípadnú značku alebo štítok spojenú/-ý so schémou.

Možnosť agentúry ENISA vydávať QR kódy súvisiace s certifikátmi by mala umožniť výrobcovi alebo poskytovateľovi prostredníctvom dokumentácie alebo balíka súvisiaceho s certifikovaným produktom uľahčiť prístup na webovú stránku agentúry ENISA, na ktorej sú zobrazené certifikáty.

Keďže certifikát nemôže obsiahnuť všetky relevantné informácie súvisiace s certifikovaným produktom, spolu s certifikátom sa vypracuje a uverejní správa o certifikácii, ktorá obsahuje podrobnejšie informácie.

18. DOSTUPNOSŤ INFORMÁCIÍ

ODKAZ(-Y) NA ČLÁNOK(-KY) CSA

Článok 54 1. *Európska schéma certifikácie kybernetickej bezpečnosti obsahuje aspoň tieto prvky:*

q) Obdobie, počas ktorého výrobca alebo poskytovateľ produktov IKT, služieb IKT alebo procesov IKT má uchovávať k dispozícii EÚ vyhlásenia o zhode, technickú dokumentáciu a všetky ďalšie relevantné informácie,

Každý výrobca alebo poskytovateľ produktov IKT musí udržiavať systém zverejňovania informácií, ktoré sa majú sprístupniť verejnosti, v súlade s postupmi opísanými v kapitole 23, DOPLŇUJÚCE INFORMÁCIE O KYBERNETICKEJ BEZPEČNOSTI – ČLÁNOK 55 pre Doplňujúce informácie o kybernetickej bezpečnosti.

Všetky informácie musia byť k dispozícii najmenej päť (5) rokov po expirácii certifikátu.

Ak bol v súlade s činnosťami opísanými v kapitole 12, PODMIENKY VYDÁVANIA, UDRŽIAVANIA, POKRAČOVANIA A OBNOVOVANIA CERTIFIKÁTOV, pridelený iný dátum expirácie certifikátu, zohľadní sa pri výpočte obdobia dostupnosti informácií podľa rovnakého pravidla, ako bolo uvedené predtým.

Dostupné informácie sa aktualizujú o nové alebo revidované informácie týkajúce sa činností vykonávaných podľa kapitoly 12, PODMIENKY VYDÁVANIA, UDRŽIAVANIA, POKRAČOVANIA A OBNOVENIA CERTIFIKÁTOV.

Záznamy o informáciách dodaných CAB na účely certifikačného procesu, ako aj vzorky verzie certifikovaného produktu IKT sa bezpečne uchovávajú a na požiadanie sa sprístupnia CAB alebo NCCA (podľa článku 58.8 písm. a) CSA) do piatich rokov po expirácii certifikácie v súlade s dobou platnosti stanovenou v kapitole 15, UCHOVÁVANIE ZÁZNAMOV CAB.

ZÁKLADNÉ INFORMÁCIE

Doba uchovávania záznamov výrobcov a poskytovateľov produktov IKT nesmie byť kratšia ako doba uchovávania záznamov CAB, t. j. päť (5) rokov po skončení platnosti certifikátu.

Treba poznamenať, že výrobcovia a poskytovatelia však môžu byť nútení predĺžiť toto obdobie, aby splnili požiadavky iných nariadení (napr. nariadenia EÚ č. 305/2011[26] , 2014/53/EÚ[27] , 2014/35/EÚ[28], 2006/42/ES[29]), ktoré stanovujú iné obdobie dostupnosti dokumentácie, a to až do desiatich (10) rokov.

Ak je potrebné certifikát upraviť, niektoré informácie súvisiace s produktom IKT môžu byť zrušené a nahradené novými informáciami a potreba zachovať dostupné informácie o produkte IKT sa týka len platných a aktuálnych informácií. Vyradené informácie sa stále archivujú počas desiatich (10) rokov alebo počas platnosti príslušného certifikátu plus päť (5) rokov, ak táto doba presahuje desať (10) rokov.

Dostupnosť informácií týkajúcich sa certifikácie: požaduje sa dostupnosť certifikovanej verzie produktu na úrovni výrobcu alebo vývojára pre prípadné ďalšie vyšetrovanie, ktoré by mohlo byť potrebné, keďže sa predpokladá, že si to CAB z praktických dôvodov nemôže dovoliť sám.

[26] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011R0305.
[27] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0053.
[28] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0035.
[29] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32006L0042.

19. OBDOBIE PLATNOSTI CERTIFIKÁTOV

ODKAZ(-Y) NA ČLÁNOK(-KY) CSA

Článok 54 1. *Európska schéma certifikácie kybernetickej bezpečnosti obsahuje aspoň tieto prvky:*

r) maximálne obdobie platnosti európskych certifikátov kybernetickej bezpečnosti vydaných v rámci schémy.

Maximálne obdobie platnosti certifikátov je päť (5) rokov.

Za určitých podmienok, vrátane schválenia jej NCCA, a po dodržaní postupov definovaných v kapitole 12, PODMIENKY VYDÁVANIA, UDRŽIAVANIA, POKRAĆOVANIA A OBNOVOVANIA CERTIFIKÁTOV, CAB môže pokračovať v certifikáte s predĺženou platnosťou po uplynutí pôvodných piatich (5) rokov. Certifikáty s predĺženou dobou platnosti sa môžu posudzovať pri odbere vzoriek podľa kapitoly 11 PRAVIDLÁ MONITOROVANIA SÚLADU.

V rámci konkrétnej technickej domény môže byť stanovené kratšie maximálne obdobie platnosti, ako je definované v kapitole 4, ÚROVNE ZÁRUKY.

ZÁKLADNÉ INFORMÁCIE

Vzhľadom na veľkú rozmanitosť produktov IKT, ktoré možno certifikovať v rámci tejto schémy, na ich rôzne možné implementácie (softvér, hardvér...) a vývoj (časté alebo zriedkavé aktualizácie), na rôzne úrovne záruky, ktoré možno dosiahnuť, a s tým spojené úsilie o posúdenie ich odolnosti, ako aj na podmienky ich nasadenia a ich životnosť, bola pre všeobecný prípad zvolená priemerná maximálna doba päť (5) rokov.

Toto obdobie je tiež v súlade s obdobím vymedzeným podľa CCRA30[30].

Bola však stanovená možnosť prekročiť toto obdobie piatich (5) rokov a s tým spojené podmienky definované v kapitole 12, PODMIENKY VYDÁVANIA, UDRŽIAVANIA, POKRAČOVANIA A OBNOVOVANIACERTIFIKÁTOV (vrátane prehodnotenia kybernetickej bezpečnosti súvisiacich produktov IKT), aby sa umožnilo certifikovať produkty IKT, ktoré sa nasadzujú na dlhšie obdobie (napríklad pasy), počas celého ich životného cyklu.

Na druhej strane sa zaviedla možnosť obmedziť maximálnu lehotu, pretože sa to môže stať nevyhnutnosťou pre niektoré špecifické produkty IKT: predpokladá sa, že sa to môže vyskytnúť v prípade špecifických technických domén.

[30] https://www.commoncriteriaportal.org/products/ CCDB schválila uznesenie o časovom obmedzení platnosti vzájomne uznávaných certifikátov CC. Certifikáty zostanú na CPL päť rokov. S účinnosťou od 1. júna 2019 budú certifikáty s uplynutou dobou platnosti (t. j. 5 a viac rokov od dátumu vydania certifikátu) presunuté do zoznamu archívu na portáli CCRA, pokiaľ nebola doba platnosti predĺžená pomocou príslušných postupov.

20. POLITIKA ZVEREJŇOVANIA CERTIFIKÁTOV

ODKAZ(-Y) NA ČLÁNOK(-KY) CSA

Článok 54 1. *Európska schéma certifikácie kybernetickej bezpečnosti obsahuje aspoň tieto prvky:*

s) politiku zverejňovania európskych certifikátov kybernetickej bezpečnosti, ktoré boli vydané, zmenené alebo zrušené v rámci schémy.

Agentúra ENISA zverejní certifikáty spolu s príslušnou správou o certifikácii a všetkými relevantnými informáciami, ktoré sa vyžadujú v iných kapitolách tohto dokumentu, na osobitnej webovej stránke o európskych schémach certifikácie kybernetickej bezpečnosti v súlade s článkom 50 ods. 1 CSA.

Certifikáty sa zverejňujú s ich platným stavom, ako sa rozhodlo na základe uplatnenia požiadaviek stanovených v kapitole 12, PODMIENKY VYDÁVANIA, UDRŽIAVANIA, POKRAČOVANIA A OBNOVENIA CERTIFIKÁTOV a v kapitole 13, PRAVIDLÁ TÝKAJÚCE SA NESÚLADU.

Certifikáty môžu NCCA a súvisiace CB zverejňovať aj na svojich webových stránkach. Každá zmena stavu certifikátu sa oznámi agentúre ENISA.

Zmeny a zrušenia certifikátov vyplývajúce z činností údržby sa takisto zverejňujú tak, aby používatelia certifikátov mohli zistiť, ktoré verzie certifikovaného produktu IKT sú certifikované, ktoré verzie už nie sú certifikované a ktoré príslušné informácie sa uplatňujú (napríklad usmernenia).

Agentúra ENISA v spolupráci s ECCG stanoví podmienky a/alebo usmernenia na vydávanie a včasné zverejňovanie certifikátov a ich aktualizácií a súvisiacich relevantných informácií a zverejní ich na svojom webovom sídle venovanom certifikácii kybernetickej bezpečnosti.

Takéto informácie o európskych schémach certifikácie kybernetickej bezpečnosti sú na webovom sídle dostupné v anglickom jazyku. Musia byť k dispozícii minimálne počas celého obdobia platnosti certifikátu.

Certifikáty môžu byť doplnené ďalšími informáciami, ako je napríklad QR kód, ktorý poskytuje priamy odkaz na príslušný bezpečnostný zámer (bezpečnostný zámer v zjednodušenej verzii, ak je k dispozícii) a certifikát produktu, a (so súhlasom výrobcov alebo poskytovateľov) obrázky certifikovaných produktov IKT, aby sa poskytla lepšia užívateľská dostupnosť a aby sa certifikáty propagovali. ENISA preto môže stanoviť postup na generovanie QR-kódu: takýto postup môže znamenať, že certifikačné orgány (CB) pred vydaním certifikátu požiadajú ENISA o vygenerovanie QR-kódu, ktorý sa použije na certifikáte
a poskytne ho výrobcom alebo poskytovateľom pre ich obchodné a technické dokumenty.

Iba produkty IKT s platným certifikátom môžu byť propagované ako certifikované produkty IKT ich príslušným výrobcom alebo poskytovateľom, alebo používateľmi týchto produktov.

Ak sú ochranné profily certifikované podľa podmienok tejto schémy, agentúra ENISA poskytne na svojej webovej stránke pre certifikáciu kybernetickej bezpečnosti zoznam týchto ochranných profilov.

ZÁKLADNÉ INFORMÁCIE

V súlade s kapitolou 17, OBSAH A FORMÁT CERTIFIKÁTOV, sa používateľom (a potenciálnym používateľom) certifikátov sprístupnia certifikáty a súvisiace správy o certifikácii, ako aj relevantné informácie o bezpečnej konfigurácii a používaní certifikovaného produktu IKT (usmernenie). Zmeny a doplnenia certifikátu budú musieť obsahovať rovnaký typ informácií ako vydávanie certifikátov vrátane usmernení a používatelia budú mať jednoduchý prístup k stavu certifikátov pri používaní špecializovanej webovej stránky agentúry ENISA.

Aby sa umožnil jednoduchý prístup k doplňujúcim informáciám o kybernetickej bezpečnosti definovaným v článku 55, v certifikáte bude k dispozícii overený odkaz na tieto informácie.

Agentúra ENISA je bez zbytočného odkladu informovaná o vývoji certifikátov, či už ide o zmenu alebo

zrušenie, v súlade s požiadavkami príslušných kapitol tejto schémy a Odôvodnenia 93 CSA.

Aby sa zabezpečila potrebná flexibilita a vynútiteľnosť podmienok predkladania informácií agentúre ENISA a ich zverejňovania, agentúra ENISA stanoví všeobecné podmienky a/alebo usmernenia.

Všeobecné podmienky a/alebo usmernenia by mali zabezpečiť, aby boli informácie presné a aktuálne, keďže informácie poskytnuté agentúrou ENISA by mohli slúžiť ako jednotný referenčný bod. Malo by sa v nich vymedziť, aké informácie sa majú agentúre ENISA zasielať a v akom primeranom časovom rámci. V súlade so zásadami transparentnosti a otvorenosti by sa osnovy týchto podmienok/pokynov mali zverejniť na webovej stránke agentúry ENISA.

Pokiaľ ide o propagáciu platných certifikátov, certifikáty, ktorých platnosť vypršala, budú archivované a sprístupnené na inej webovej stránke ako platné certifikáty.

21. VZÁJOMNÉ UZNÁVANIE S TRETÍMI KRAJINAMI

ODKAZY(-Y) NA ČLÁNOK(-KY) CSA

Článok 54 1. *Európska schéma certifikácie kybernetickej bezpečnosti obsahuje aspoň tieto prvky:*

t) podmienky vzájomného uznávania schém certifikácie s tretími krajinami.

Vzájomné uznávanie certifikačných schém s tretími krajinami sa podporuje uzavretím dohody o vzájomnom uznávaní (MRA) medzi účastníkmi.

Táto MRA môže obsahovať tieto informácie:

- účastníkov MRA;
- účel a duch tejto dohody;
- členstvo;
- rozsah;
- výnimky;
- definície;
- podmienky uznávania certifikátov
- vzájomné posudzovanie;
- publikácie;
- zdieľanie informácií;
- prijímanie nových účastníkov a príslušné autority alebo orgány;
- správu tejto dohody;
- rozdiely;
- náklady na túto dohodu;
- revízia;
- trvanie;
- dobrovoľné ukončenie účasti;
- začatie a pokračovanie;
- účinok tejto dohody.

Podmienky uznávania certifikátov účastníkmi takejto dohody zahŕňajú minimálne tieto podmienky:

- účastníci sa zaviažu, že budú uznávať platné certifikáty o zhode od každého prijatého účastníka;
- prijatie účastníkov potvrdzuje, že procesy hodnotenia a certifikácie boli vykonané riadne odborným spôsobom:
  - na základe všeobecne uznávaných kritérií hodnotenia bezpečnosti IKT;
  - pomocou všeobecne uznávaných metód hodnotenia bezpečnosti IKT;
  - v kontexte hodnotenia a certifikácie schémy, ktorý riadi certifikačný orgán v krajine akceptovaného účastníka;
  - vydané certifikáty a správy o certifikácii spĺňajú ciele tejto dohody;
- certifikáty, ktoré spĺňajú všetky tieto podmienky, sa na účely tejto dohody označujú ako vyhovujúce certifikáty;
- kritériá hodnotenia bezpečnosti IKT sú stanovené v kapitole 3, NORMY POUŽITÉ PRI HODNOTENÍ tohto dokumentu;
- minimálne požiadavky na správy o certifikácii sú stanovené v prílohe 13 k tomuto dokumentu;
- schéma účastníkov alebo schéma, ku ktorej účastníci pristupujú, sa pripraví s príslušnou národnou autoritou, certifikačnými orgánmi (CB) a skúšobnými laboratóriami (ITSEF) v súlade s týmito požiadavkami:
  - Národná autorita dohliada na certifikačné činnosti, v prípade potreby oznamuje a autorizuje CB a ITSEF a oznamuje NCCA členských štátov EÚ akúkoľvek zraniteľnosť certifikovaných produktov IKT;

- CB bola akreditovaná v príslušnej krajine uznaným akreditačným orgánom v súlade s normou ISO/IEC 17065 a v prípade potreby bola autorizovaná národnou autoritou;
- účastníci uznajú CB za vyhovujúcu prostredníctvom mechanizmu vzájomného posudzovania zavedeného pre MRA;
- ITSEF bol akreditovaný vo svojej príslušnej krajine uznaným akreditačným orgánom v súlade s normou ISO/IEC 17025 a v prípade potreby podlieha posúdeniu národnou autoritou s cieľom potvrdiť jeho kompetentnosť vykonávať hodnotenia v súlade s kapitolou 6, ŠPECIFICKÉ POŽIADAVKY PLATNÉ PRE CAB tohto dokumentu;

- s cieľom pomôcť konzistentnému uplatňovaniu kritérií a metód medzi hodnotením a certifikáciou schém, plánujú účastníci pracovať na jednotnom výklade v súčasnosti platných kritérií a metód a zaväzujú sa prijať podporné dokumenty, ktoré sú výsledkom tejto práce. V snahe dosiahnuť tento cieľ účastníci plánujú aj pravidelnú výmenu informácií o výkladoch a diskusie potrebné na vyriešenie rozdielov vo výklade;
- ako ďalšiu pomoc pri dosahovaní cieľa konzistentného, dôveryhodného a kompetentného uplatňovania kritérií a metód certifikačné orgány preberajú zodpovednosť za monitorovanie všetkých prebiehajúcich hodnotení v rámci MRA na primeranej úrovni a vykonávajú ďalšie postupy na zabezpečenie toho, aby všetky ITSEF pridružené k CB:
  - vykonávali hodnotenia nestranne;
  - správne a dôsledne uplatňovali kritériá a metódy;
  - mali a udržiavali si požadované odborné kompetentnosti;
  - primerane chránili dôvernosť citlivých alebo chránených informácií.

MRA môže zahŕňať obmedzenie úroveň záruky certifikátov, ktorá podlieha uznaniu.

CB účastníkov takejto dohody, ktorá vydáva certifikáty na rovnocennej úrovni záruky "vysoká" podľa CSA, podlieha vzájomnému posudzovaniu v súlade s postupom stanoveným v tomto schéme v prílohe 12.

Postup sa môže upraviť a zjednodušiť pre CB, ktoré vydávajú certifikáty na rovnocennej úrovni záruky "významná" CSA, aby mohli využívať výhody medzinárodného akreditačného systému, a pozostáva minimálne z týchto činností tímu vzájomného posudzovania, pokiaľ ide o preskúmanie:

- dokumentácie súvisiacej s 2 certifikačnými projektmi na úrovni záruky "významná";
- postupov súvisiacich s bezpečnosťou informácií.

ZÁKLADNÉ INFORMÁCIE

Pri vytváraní MRA sa môžu využiť skúsenosti existujúcich MRA (CCRA a SOG-IS MRA), ktoré definujú podmienky účasti a uznávania certifikátov a ktoré nezohľadňujú rovnaké úrovne záruky pre uznávanie certifikátov.

22. VZÁJOMNÉ POSUDZOVANIE

ODKAZ(-Y) NA ČLÁNOK(-KY) CSA

Článok 54 1. *Európska schéma certifikácie kybernetickej bezpečnosti obsahuje aspoň tieto prvky:*

u) prípadné pravidlá týkajúce mechanizmu vzájomného posudzovania, ktorý je stanovený schémou pre autority alebo orgány vydávajúce európske certifikáty kybernetickej bezpečnosti pre úroveň záruky "vysoká" podľa článku 56(6). Tento mechanizmus sa uplatňuje bez toho, aby bolo dotknuté vzájomné posudzovanie ustanovené v článku 59.

Hoci každá(-ý) autorita alebo orgán vydávajúci certifikáty (ďalej označované ako certifikačné orgány alebo CB) pre úroveň záruky "vysoká" podľa článku 56.6 CSA, vrátane pridružených skúšobných laboratórií (ITSEF), pôsobí na vlastnú zodpovednosť, musí sa zaviesť vzájomné posudzovanie, aby sa:

- posúdilo, či pracujú harmonizovaným spôsobom a vydávajú certifikáty rovnakej kvality;
- umožnilo opakované použitie certifikátov na certifikáciu zložených produktov, ako sa ponúka v kapitole 2, ÚČEL SCHÉMY;
- identifikovali všetky potenciálne silné stránky, ktoré vyplývajú z ich každodennej práce a ktoré môžu byť prínosom pre ostatných;
- identifikovali všetky potenciálne nedostatky, ktoré vyplývajú z ich každodennej práce a ktoré by mali byť predmetom vzájomného posudzovania CB;
- našiel harmonizovaný spôsob, ako postupovať pri zverejňovaní a spracúvaní zraniteľností, a vymieňať si osvedčené postupy týkajúce sa vybavovania sťažností.

Poznámka: Vzájomné posudzovanie nemá za cieľ zasahovať do činností vykonávaných NCCA ani ich posudzovať, pretože to je predmetom procesu vzájomného hodnotenia podľa požiadaviek článku 59 CSA. Nesmie tiež zasahovať do činností vykonávaných národným akreditačným orgánom (NAB) ani ich posudzovať.

S cieľom umožniť včasnú spätnú väzbu v súvislosti s otázkami týkajúcimi sa národných aspektov schémy, ktorými sa zaoberá NCCA, sa na vzájomnom posudzovaní zúčastňuje zástupca NCCA hodnotenej CB.

Vzájomné posudzovanie každej CB, ktorá vydáva certifikáty o úrovni záruky "vysoká", sa uskutočňuje pravidelne v intervale, ktorý nepresiahne päť (5) rokov.

ECCG[31] vypracuje a udržiava plán vzájomných posudzovaní, ktorým sa zabezpečí dodržiavanie tejto periodicity, a zohľadní úroveň priority, ktorá sa môže priradiť vzájomnému posudzovaniu CB vydávajúcej certifikáty na úrovni záruky "vysoká" v prípade údajného nedodržiavania požiadaviek zo strany tejto CB a v prípade CB s nedávnou činnosťou, ktoré sa prvýkrát alebo po dlhšej prestávke (viac ako dva roky) zaoberajú certifikáciou.

V prípade článku 56 ods. 6 písm. a) CSA podlieha vzájomnému posudzovaniu orgán posudzovania zhody, ktorý vydáva certifikáty, ako aj NCCA, ktorá postupuje pri predbežnom schvaľovaní každého jednotlivého certifikátu. To zahŕňa postup stanovený NCCA pre predchádzajúce schválenie každého jednotlivého certifikátu.

V prípade článku 56 ods. 6 písm. b) CSA podlieha vzájomnému posudzovaniu CAB vydávajúci certifikáty aj NCCA. To zahŕňa všeobecné požiadavky na delegovanie právomocí definované NCCA.

Vzájomné posudzovanie sa vykonáva podľa postupu stanoveného v prílohe 12. Ak to nie je riadne odôvodnené, vzájomné posudzovanie sa vykonáva na mieste pre vzájomné posudzovanie CB a prípadne pre vybraný súbor ITSEF.

Ak bola certifikácia nad úrovňou AVA_VAN.3 pre produkty IKT, na ktoré sa nevzťahuje technická doména, zavedená podľa osobitných ochranných profilov certifikovaných v rámci tejto schémy na tento účel, produkty IKT certifikované v súlade s týmito ochrannými profilmi sa pri výbere v rámci mechanizmu vzájomného posudzovania posudzujú s vysokou prioritou.

Tím pre vzájomné posudzovanie sa môže rozhodnúť opätovne použiť výsledky predchádzajúcich

[31] ECCG môže zriadiť špecializovanú podskupinu, ktorá sa bude zaoberať vzájomným posudzovaním na základe organizácie, ktorá má byť zriadená na udržiavanie schémy EUCC (pozri kapitolu 25, ODPORÚČANIA AHWG).

vzájomných posudzovaní posudzovanej autority alebo orgánu, ktoré sa týkajú časti rozsahu pôsobnosti, za týchto podmienok:

- tieto výsledky nesmú byť staršie ako päť (5) rokov;
- ak sa predchádzajúce vzájomné posudzovanie vzájomne posudzovaných CB vykonalo v rámci inej schémy, uvedie sa opis postupov vzájomného posudzovania platných pre túto inú schému;
- v správe o vzájomnom posudzovaní sa jasne uvedie, ktoré časti boli opätovne použité bez ďalšieho hodnotenia a ktoré časti boli opätovne použité s dodatočným hodnotením;
- ak sa vzájomné posudzovanie týka technickej domény, opätovné použitie neumožňuje vyhnúť sa kontrole vzájomne posudzovanej CB a súvisiacich ITSEF.

Tím vzájomného posudzovania oznámi svoje zistenia ECCG v správe o vzájomnom posudzovaní s uvedením závažnosti prípadných nedostatkov. Správa o vzájomnom posudzovaní obsahuje v prípade potreby usmernenia alebo odporúčania týkajúce sa činností alebo opatrení, ktoré má prijať vzájomne posudzovaný CB, ako aj opatrenia, ktoré navrhol vzájomne posudzovaný CB na riešenie zistení.

Pri stanovovaní opatrení na spracovanie zistení môže vzájomne posudzovaný CB požiadať o podporu tím vzájomného posudzovania. Tieto opatrenia sa v rámci správy o vzájomnom posudzovaní zašlú ECCG s uvedením spôsobu, akým plánuje nápravu zistení. V prípade potreby môže ECCG informovať príslušnú(-ý):

- NCCA vzájomne posudzovaného CB na posúdenie potenciálneho vplyvu zostávajúcich zistení na certifikáty vydané vzájomne posudzovaným CB alebo na akúkoľvek autorizáciu alebo notifikáciu týkajúcu sa vzájomne posudzovaného CB a súvisiacich ITSEF;
- Národný akreditačný orgán (NAB) vzájomne posudzovaného CB, aby zvážil potenciálny vplyv zostávajúcich zistení na akreditáciu vzájomne posudzovaného CB a súvisiacich ITSEF;

a môže požiadať o ich závery.

Vzájomne posudzovaný CB a príslušná NCCA majú možnosť riešiť s ECCG všetky nedostatky a odporúčania uvedené v správe pred tým, ako agentúra ENISA zverejní výsledky vzájomného posudzovania. Taktiež NAB má možnosť riešiť všetky nedostatky a odporúčania v prípade, že boli NAB predložené pred zverejnením výsledkov.

Agentúra ENISA sa môže zúčastňovať na vzájomnom posudzovaní.

CB informujú žiadateľov o certifikáciu na úrovni záruky „vysoká“ podľa CSA, že ich certifikačné projekty môžu podliehať vzájomnému posudzovaniu zavedeného touto schémou.

ZÁKLADNÉ INFORMÁCIE

Vzájomné posudzovanie NCCA sa zavádza článkom 59 CSA. Posudzuje najmä:

(d) postupy monitorovania, autorizácie a dozoru, pokiaľ ide o činnosti orgánov posudzovania zhody;

(e) ak je to relevantné, či personál autorít alebo orgánov, ktorí vydávajú certifikáty pre úroveň záruky "vysoká" podľa článku 56 ods. 6, má primerané odborné znalosti.

Okrem toho možno pre každú schému definovať vzájomné posudzovanie, pričom v prvej časti tejto kapitoly sú definované špecifické ciele schémy EUCC a požiadavky.

Podľa CCRA aj SOG-IS MRA sa od CB vyžaduje vzájomné posudzovanie v pravidelných cykloch. Takéto posudzovania môžu zahŕňať skúšobné laboratórium (ITSEF) spojené s CB: cieľom je posúdiť odborné kompetentnosti ITSEF súvisiace s technickou doménou.

Tento prístup zaručuje vysokú kvalitu hodnotiacich činností, ktorá sa vyžaduje pre úroveň bezpečnostnej záruky „vysoká“, a harmonizáciu metód hodnotenia medzi rôznymi CAB, čo umožňuje objektívnejšie výsledky a postup pri zložených certifikáciách produktov v rámci rôznych CAB.

Je dôležité, aby sa pre takéto činnosti vrátane opätovného posudzovania a potrebných priorít súvisiacich s nováčikmi v oblasti certifikácie alebo s tými, ktorí majú problémy s certifikáciou, vypracoval plán.
V rámci vzájomného posudzovania sa zaviedlo aj zameranie na certifikáty, ktoré by sa vydávali nad úrovňou AVA_VAN.3 bez technických domén a s novou možnosťou vytvoriť na tento účel osobitné PP, ako spôsob, ako ponúknuť *následnú* kontrolu, ktorá bude prospešná pre uznávanie týchto certifikátov.

Postup uvedený v prílohe využíva existujúce postupy SOG-IS a zohľadňuje možnosť opätovného použitia výsledkov z iných mechanizmov vzájomného posudzovania.

Považuje sa za dôležité, aby posudzovaný orgán alebo autorita v prípade potreby predložil ECCG účinné opatrenia na primerané prispôsobenie svojich postupov a odborných znalostí s cieľom opätovne ubezpečiť ostatných účastníkov schémy o kvalite certifikátu, ktorý vydáva.

V prípadoch, keď sa ECCG domnieva, že kvalita certifikátov nie je v súlade s požiadavkami tejto schémy, ECCG môže informovať a konzultovať to s NCCA a NAB posudzovaného orgánu alebo autority, aby vyvodili závery o vplyve na svoju autorizáciu a akreditáciu.

23. DOPLŇUJÚCE INFORMÁCIE O KYBERNETICKEJ BEZPEČNOSTI - ČLÁNOK 55

ODKAZ(-Y) NA ČLÁNOK(-KY) CSA

Článok 54 1. *Európska schéma certifikácie kybernetickej bezpečnosti obsahuje aspoň tieto prvky:*

v) formát a postupy, ktoré musia dodržiavať výrobcovia alebo poskytovatelia produktov IKT, služieb IKT alebo procesov IKT pri poskytovaní a aktualizácii doplňujúcich informácií o kybernetickej bezpečnosti v súlade s článkom 55.

Článok 55 .1. *Výrobca alebo poskytovateľ certifikovaných produktov IKT, služieb IKT alebo procesov IKT alebo produktov IKT, služieb IKT a procesov IKT, pre ktoré bolo vydané EÚ vyhlásenie o zhode, zverejňuje tieto doplňujúce informácie o kybernetickej bezpečnosti*:

(a) poradenstvo a odporúčania na pomoc koncovým používateľom s bezpečnou konfiguráciou, inštaláciou, zavedením, prevádzkou a údržbou produktov IKT alebo služieb IKT;

(b) obdobie, počas ktorého sa bude koncovým používateľom poskytovať bezpečnostná podpora, a to najmä pokiaľ ide o dostupnosť aktualizácií, ktoré sa týkajú kybernetickej bezpečnosti;

(c) kontaktné informácie výrobcu alebo poskytovateľa a akceptované metódy na prijímanie informácií o zraniteľnosti od koncových používateľov a výskumníkov v oblasti bezpečnosti;

(d) odkaz na registre online , ktoré uvádzajú zverejnené zraniteľnosti týkajúce sa produktu IKT, služby IKT alebo procesu IKT, a všetky príslušné kybernetickobezpečnostné rady.

Článok 55 .2. *Informácie uvedené v odseku 1 musia byť k dispozícii v elektronickej podobe a zostávajú k dispozícii a podľa potreby sa aktualizujú aspoň do skončenia platnosti príslušného európskeho certifikátu kybernetickej bezpečnosti alebo EÚ vyhlásenia o zhode.*

Všetky doplňujúce informácie o kybernetickej bezpečnosti, ktoré sú vyhlásené za potrebné na certifikáciu alebo iné činnosti podľa tejto schémy, poskytujú výrobcovia alebo poskytovatelia príslušnej strane za podmienok stanovených v príslušných kapitolách.

V súlade s požiadavkami kapitoly 17, OBSAH A FORMÁT CERTIFIKÁTOV, sa do certifikátu zapracuje najmä odkaz na webové sídlo a príslušné stránky, kde sú tieto informácie k dispozícii. Po splnení všetkých požiadaviek na certifikáciu vydávajúci orgán požiada výrobcu alebo poskytovateľa o poskytnutie adresy URL (odkazu), aby ju bolo možné spracovať pred tým, ako sa certifikát nahrá na webovú stránku agentúry ENISA na účely certifikácie.

Výrobcovia alebo poskytovatelia produktov IKT zverejnia na svojich webových stránkach doplňujúce informácie o kybernetickej bezpečnosti v súlade s článkom 55.

Informácie sú k dispozícii v elektronickej forme a v anglickom jazyku a zostávajú k dispozícii minimálne do skončenia platnosti príslušného európskeho certifikátu kybernetickej bezpečnosti. Aktualizuje sa v súlade s požiadavkami kapitoly 12, PODMIENKY VYDÁVANIA, UDRŽIAVANIA, POKRAČOVANIA A OBNOVOVANIA CERTIFIKÁTOV.

Najmä usmernenia a odporúčania na pomoc koncovým používateľom pri bezpečnej konfigurácii, inštalácii, zavedení, prevádzke a údržbe produktov IKT, ako sú vymedzené v článku 55 ods. 1 písm. a), musia byť kedykoľvek v súlade s usmerneniami a odporúčaniami, ktoré boli posúdené počas hodnotenia, alebo aktualizované. Ak sa líšia od týchto odporúčaní, môžu byť predložené na preskúmavanie hodnotiteľovi produktu IKT, aby bolo možné posúdiť očakávaný súlad.

ZÁKLADNÉ INFORMÁCIE

Okrem verejnej dostupnosti informácií, ako sa vyžaduje v článku 55, sa môže požadovať aj potreba

prístupu k všetkým informáciám alebo ich časti počas certifikácie, napríklad na overenie, či informácie spĺňajú požiadavky schémy. Týmto spôsobom sa v rámci postupu dbá aj na to, aby výrobca mal k dispozícii URL ešte pred vydaním certifikátu. Táto špecifická potreba preskúmať časť doplňujúcich informácií o kybernetickej bezpečnosti počas fázy certifikácie sa však vyskytne len vtedy, ak príslušná kapitola tejto schémy stanovuje takúto požiadavku.

Na účely jednoduchého a harmonizovaného prístupu používateľov certifikátov k webovým stránkam, na ktorých budú informácie dostupné na webových stránkach výrobcov alebo poskytovateľov, bude potrebné v certifikáte uviesť príslušný odkaz.

Podmienky poskytovania doplňujúcich informácií o kybernetickej bezpečnosti by mali byť súčasťou podrobnejšej politiky zverejňovania, ktorú agentúra ENISA stanoví v súlade s požiadavkami kapitoly 20, POLITIKA ZVEREJŇOVANIA CERTIFIKÁTOV.

24. ĎALŠIE PRVKY SCHÉMY

24.1 CERTIFIKÁCIA OCHRANNÝCH PROFILOV

ODKAZ(Y) NA ČLÁNOK(-KY) CSA

Článok 54 1. *Európska schéma certifikácie kybernetickej bezpečnosti obsahuje aspoň tieto prvky:*

a) predmet a rozsah certifikačnej schémy vrátane typu alebo kategórií produktov IKT, služieb IKT a procesov IKT, na ktoré sa vzťahuje.

Hodnotenie kybernetickej bezpečnosti a certifikácia ochranných profilov (PP), formálneho dokumentu definovaného podľa CC, ktorý vyjadruje súbor bezpečnostných požiadaviek nezávislých od implementácie pre kategóriu produktov IKT, ktoré spĺňajú špecifické potreby spotrebiteľov, je doplnkovým prvkom schémy EUCC.

Certifikácia ochranného profilu musí preukázať, že ochranný profil je úplný, konzistentný a technicky spoľahlivý a vhodný na použitie ako vzor, na ktorom sa dá postaviť ďalší ochranný profil alebo bezpečnostný zámer.

Vychádza z rovnakých podmienok tejto schémy, ktoré sa uplatňujú na certifikáciu produktu IKT, ktorý by bol nakoniec certifikovaný v súlade s ochranným profilom, s týmito výnimkami:

- jeho hodnotenie sa obmedzí na podmnožinu činností súvisiacich s kritériami APE, ako sú uvedené v časti 3 CC;
- ochranný profil môže ako produkt IKT podliehať údržbe na účely aktualizácií alebo opráv a nevyžaduje si uplatňovanie monitorovacích činností opísaných v kapitole 11, PRAVIDLÁ MONITOROVANIA SÚLADU, ani činností opísaných v kapitole 14, PRAVIDLÁ TÝKAJÚCE SA RIEŠENIA ZRANITEĽNOSTÍ;
- certifikát ochranného profilu je podmnožinou certifikátu produktu IKT;
- Doplňujúce informácie o kybernetickej bezpečnosti vymedzené v článku 55 nie sú potrebné.

V certifikáte ochranného profilu sa uvádza úroveň záruky, na ktorú sú zamerané produkty IKT, ktoré budú v súlade s týmto ochranným profilom , v súlade s mapovaním podrobne opísaným v kapitole 4, ÚROVNE ZÁRUKY, a obsahuje tieto prvky:

- jedinečný identifikátor stanovený vydavateľom certifikátu;
- informácie týkajúce sa certifikovaného ochranného profilu IKT a jeho vývojára:
  - názov ochranného profilu IKT;
  - typ ochranného profilu IKT;
  - verzia pre ochranného profilu IKT;
  - meno a kontaktné údaje vývojára;
- informácie týkajúce sa hodnotenia a certifikácie ochranného profilu IKT:
  - názov a kontaktné údaje CB, ktorý certifikát vydal;
  - názov ITSEF, ktorý vykonal hodnotenie, ak sa líši od certifikačného orgánu;
  - názov zodpovednej NCCA;
  - odkaz na túto schému;
  - odkaz na správu o certifikácii spojenú s certifikátom;
  - dosiahnutú úroveň záruky z CSA (buď "významná", alebo "vysoká");
  - identifikácia použitých komponentov záruk z CC vrátane úrovne AVA_VAN, na ktorú sa vzťahuje;
  - prípadne odkaz na ochranné profil(-y) , s ktorým(-i) je ochranný profil IKT v súlade;
  - dátum vydania.

Správa o certifikácii spojená s certifikátom musí obsahovať príslušné oddiely prílohy 13 podľa predchádzajúceho zoznamu.

ZÁKLADNÉ INFORMÁCIE

Metodika spoločných kritérií poskytuje možnosť definovať vo forme ochranných profilov (Protection profiles - PP) súbor bezpečnostných požiadaviek nezávislých od implementácie pre kategórie

produktov IKT, ktoré spĺňajú špecifické potreby spotrebiteľov. PP sú široko používané skupinami spotrebiteľov
a záujmovými komunitami a ako také sa môžu stať normami a zároveň sa na ne odkazuje v predpisoch EÚ.

Takéto PP možno hodnotiť a certifikovať aj pomocou rovnakej metodiky.

Podľa CC časť 1: Hodnotenie PP je nepovinné. Hodnotenie sa vykonáva tak, že sa na ne uplatňujú kritériá APE uvedené v CC časť 3. Cieľom takéhoto hodnotenia je preukázať, že PP je úplný, konzistentný a technicky správny a vhodný na použitie ako vzor, na ktorom možno postaviť ďalší PP alebo ST. Založenie PP/ST na hodnotených PP má dve (2) výhody:

- je oveľa menšie riziko, že sa v PP vyskytnú chyby, nejasnosti alebo medzery;
- hodnotenie nového PP/ST môže často opätovne použiť výsledky hodnotenia hodnoteného PP, čo vedie k menšiemu úsiliu pri hodnotení nového PP/ST.

PP nie sú produkty IKT a nepodliehajú rovnakým pravidlám údržby. V certifikátoch ako takých nie je uvedená žiadna doba platnosti, pretože je skôr vecou komunít zainteresovaných strán, ktoré tieto PP vytvorili, aby rozhodli o tom, kedy by sa PP mali ukončiť, aby sa zvážili alebo uplatnili na produkty IKT

24.2 BEZPEČNOSŤ INFORMÁCIÍ

ODKAZ(Y) NA ČLÁNOK(KY)CSA

Bod 16 prílohy: *Orgán posudzovania zhody a jeho personál, jeho výbory, jeho dcérske spoločnosti, jeho subdodávatelia a akýkoľvek pridružený orgán alebo personál externých subjektov orgánu posudzovania zhody zachovávajú povinnosť mlčanlivosti a služobné tajomstvo, pokiaľ ide o všetky informácie získané pri výkone svojich úloh posudzovania zhody podľa tohto nariadenia alebo akéhokoľvek ustanovenia vnútroštátneho práva, ktorým sa toto nariadenie vykonáva, okrem prípadov, keď sa ich poskytnutie vyžaduje na základe práva Únie alebo členského štátu, ktoré sa na tieto osoby vzťahuje, okrem styku*
s príslušnými orgánmi členských štátov, v ktorých sa vykonávajú svoju činnosť. Práva duševného vlastníctva sú chránené. Orgán posudzovania zhody musí mať zavedené zadokumentované postupy, pokiaľ ide o požiadavky tohto bodu.

Pokiaľ nie je v tejto schéme stanovené inak a bez toho, aby boli dotknuté existujúce národné ustanovenia a postupy v členských štátoch týkajúce sa dôvernosti, všetky strany zapojené do uplatňovania tejto schémy zachovávajú dôvernosť informácií a údajov získaných pri vykonávaní svojich úloh s cieľom chrániť:

a) osobné údaje v súlade s GDPR[32];
b) dôverné obchodné informácie a obchodné tajomstvá fyzickej alebo právnickej osoby vrátane práv duševného vlastníctva počas certifikačného životného cyklu produktu a do konca uvedeného času uchovávania všetkých certifikačných informácií, pokiaľ ich zverejnenie nie je nevyhnutné vo verejnom záujme alebo nepodlieha súdnemu príkazu;
c) informácie potrebné na účinné vykonávanie tejto schémy, najmä na účely vzájomných preskúmaní, vzájomných posudzovaní alebo auditov, účinnej spolupráce medzi zúčastnenými autoritami a orgánmi, riešenia verejne neznámych a následne zistených zraniteľností v procese certifikácie alebo po nej a riešenia sťažností.

Bez toho, aby bol dotknutý predchádzajúci odsek, informácie vymieňajúce sa na dôvernom základe medzi príslušnými autoritami navzájom a príslušnými autoritami a Komisiou, sa nezverejňujú bez predchádzajúceho súhlasu autority, ktorá ich poskytla.

Všetky informácie získané od CAB (CB a pridružených ITSEF) alebo výrobcov alebo poskytovateľov sa používajú len na účely certifikácie a NCCA ich považujú za dôverné - pokiaľ sa medzi stranami nedosiahne iná dohoda alebo pokiaľ tok informácií nevyžaduje osobitný predpis schémy.

Agentúra ENISA môže v spolupráci s ECCG poskytnúť usmernenia o tom, ako zabezpečiť

[32] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

bezpečnosť informácií na základe pracovných postupov súvisiacich s činnosťami opísanými v schéme EUCC.

ZÁKLADNÉ INFORMÁCIE

Bezpečnosť informácií je pri činnostiach súvisiacich s kybernetickou bezpečnosťou kľúčová. Všetky činnosti súvisiace s certifikáciou kybernetickej bezpečnosti patria do tejto druhej skupiny.

Informácie, ktoré žiadateľ poskytne CAB na účely certifikácie, môžu byť citlivé, najmä preto, že čím vyššia je úroveň hodnotenia, tým hlbšie hodnotiteľ preniká do analýzy produktu IKT a súvisiaceho životného cyklu na základe podrobných informácií, ktoré môžu obsahovať dôverné obchodné informácie a obchodné tajomstvá vrátane práv duševného vlastníctva.

Informácie vytvorené v rámci činností certifikácie kybernetickej bezpečnosti, ako sú technické správy hodnotení a súvisiace s posudzovaním, spracovaním a zverejňovaním zraniteľností, budú obsahovať aj citlivé časti informácií, ktoré pri nedostatočnej ochrane môžu zjavne ohroziť používateľov súvisiacich produktov, a to aj vtedy, keď sú tieto produkty certifikované.

Preto sa stanovia povinnosti jednotlivých účastníkov schémy na zaistenie bezpečnosti informácií a zohľadnia sa požiadavky na výrobcov a vývojárov, aby boli v súlade s článkom 55 CSA, a aby sa zo strany všetkých jednotlivcov alebo subjektov nevyhnutne dodržiavali politiky a právne rámce v oblasti slobodného prístupu k informáciám, zákony o prístupe k informáciám a/alebo akékoľvek iné podobné vnútroštátne, európske a medzinárodné politiky a predpisy.

25. ODPORÚČANIA AHWG

25.1 ODPORÚČANIA NA PRIJATIE SCHÉMY EUCC

ODKAZ(Y) NA ČLÁNOK(-KY) CSA

Článok 57 1. *Bez toho, aby bol dotknutý odsek 3 tohto článku, národné schémy certifikácie kybernetickej bezpečnosti a súvisiace postupy týkajúce sa produktov IKT, služieb IKT a procesov IKT, na ktoré sa vzťahuje európska schéma certifikácie kybernetickej bezpečnosti, strácajú účinnosť k dátumu stanovenému vo vykonávacom akte prijatom podľa článku 49 ods. 7. Národné schémy certifikácie kybernetickej bezpečnosti a súvisiace postupy týkajúce sa produktov IKT, služieb IKT a procesov IKT, na ktoré sa európska schéma certifikácie kybernetickej bezpečnosti nevzťahuje, existujú naďalej.*

Pracovná skupina AHWG odporúča, aby sa pri prijatí schémy EUCC zohľadnil nevyhnutný prechod z SOG-IS MRA.

ZÁKLADNÉ INFORMÁCIE

Za prechodné obdobie sa tu považuje obdobie medzi dátumom prijatia vykonávacieho aktu prijatého podľa článku 49 ods. 7 a dátumom stanoveným v tomto vykonávacom akte, keď národné systémy prestávajú byť účinné.

Na základe diskusií s EK sa za najpravdepodobnejší považuje scenár "veľkého tresku", ktorý pozostáva z nasledujúcich bodov:

- všetky existujúce schémy sa ukončia k rovnakému dátumu;
- počas prechodného obdobia je nulová paralelná emisia certifikátov EUCC a SOG-IS MRA pre rovnaké produkty IKT.

ODPORÚČANIA

Po prvé, prechodné obdobie by malo technicky umožniť ekosystému certifikácie kybernetickej bezpečnosti produktov IKT, ktorý používa SOG-IS MRA, prijať nové pravidlá zavedené pre schému EUCC, najmä:

- existujúce a nové CB majú byť akreditované podľa normy ISO/IEC 17065;
- existujúce a nové ITSEF majú byť akreditované podľa ISO/IEC 17025;
- nové súkromné CAB majú byť zavedené na úrovni "významná" ;
- CB majú byť autorizované svojimi ITSEF pre úroveň "vysoká";
- výrobcovia alebo poskytovatelia produktov IKT sa majú oboznámiť s povinnými požiadavkami na údržbu a prijať ich, ako aj s pravidlami riešenia zraniteľností a vydávania;
- NCCA a CB majú zaviesť monitorovacie činnosti;
- NCCA majú zaviesť dohľad nad trhom;
- vytvorenie organizácie na udržiavanie schémy, ktorá bude ďalej rozvíjať schému a podporovať všetky otázky týkajúce sa výkladu a harmonizácie v súvislosti s prijatím novej schémy.

Potom by sa malo zabrániť akémukoľvek narušeniu trhu v súvislosti s certifikačnými činnosťami. Prechodné obdobie by malo umožniť najmä:

- ukončenie súčasných certifikačných projektov v rámci existujúcich schém alebo ich jednoduchá premena na projekty EUCC;
- plynulý prenos certifikátov, ktoré si z dlhodobého hľadiska vyžadujú údržbu, teda v rámci schémy EUCC, alebo opätovné použitie pre zložené hodnotenia a certifikácie v rámci schémy EUCC.

Nakoniec by sa malo umožniť vytvorenie podmienok na vytvorenie MRA typu CCRA s tretími krajinami, ako aj označenie na podporu certifikátov EÚ.

Kandidátska schéma zaviedla niektoré možné podmienky opakovaného použitia, aby sa uľahčil

prechod (napr. opakované použitie certifikačných činností alebo opakované použitie výsledkov vzájomného posudzovania).

To však nemohlo plniť všetky požiadavky spojené so schémou EUCC, najmä akreditáciu všetkých CB a ITSEF, ktoré chcú pokračovať v činnostiach v rámci EUCC. Považuje sa to za dôležitú požiadavku a na základe skúseností členov AHWG aj za časovo náročnú činnosť (ktorá môže trvať viac ako rok - najmä preto, že doteraz neboli harmonizované všetky existujúce národné výklady súvisiacich noriem). Činnosti dohľadu nad trhom sú tiež novými činnosťami, ktoré zaviedol CSA.

Pracovná skupina AHWG preto odporúča ako technicky prijateľné prechodné obdobie dva (2) roky.

V prípade skrátenia by to malo byť sprevádzané prípadnými dočasnými výnimkami od pravidiel prijatých v rámci schémy EUCC, najmä s cieľom znížiť oneskorenie technicky náročných prechodných krokov, ako už bolo uvedené. Agentúra ENISA by mohla byť poverená podporou ECCG pri vypracovaní
a navrhovaní analýzy takýchto možných výnimiek.

Agentúra ENISA by mala v každom prípade podporiť aj vypracovanie odporúčaní pre plynulý prechod certifikátov a certifikačných činností.

25.2 ODPORÚČANIA NA UDRŽIAVANIE SCHÉMY EUCC

ODKAZ(Y) NA ČLÁNOK (KY) CSA

Článok 62.4 *ECCG má tieto úlohy:*

e) prijímať stanoviská určené Komisii, ktoré sa týkajú udržiavania a preskúmania existujúcich európskych schém certifikácie kybernetickej bezpečnosti.

Pracovná skupina AHWG odporúča na udržiavanie schémy EUCC vzhľadom na existujúce skupiny podporujúce MRA SOG-IS nasledovne.

ECCG by mala poveriť skupiny expertov, ktoré by zahŕňali NCCA, CAB a súvisiace skúšobné zariadenia a výrobcov alebo poskytovateľov produktov IKT, aby:

- zlepšili metódy hodnotenia a skúšania;
- podporovali vývoj nových technických domén;
- podporovali vývoj špecifických ochranných profilov, ktoré by v súlade s podmienkami definovanými v kapitole 4, ÚROVNE ZÁRUKY, umožnili certifikáciu nad AVA_VAN.3 pre produkty IKT, ktoré nie sú pokryté technickou doménou;
- poskytnúť písomné usmernenie k harmonizácii ochranných profilov.

Skupina expertov by sa mali zamerať na harmonizáciu metodiky skúšania, analýzu nových útokov a ich použiteľnosť na produkty IKT (hodnotenie, aktualizácia metodiky testovania) a navrhnúť nové alebo revidované podporné dokumenty.

To sa týka najmä úroveň záruky „vysoká“ CSA.

Mali by byť organizované tak, aby pokrývali všetky všeobecné a špecifické oblasti, a ECCG by mala zvážiť existujúce kompetencie existujúcej štruktúry podporujúcej súčasnú SOG-IS MRA[33].

Skupina expertov by sa mohla využiť aj ako konzultanti, ktorí by v prospech ECCG zisťovali, či pri určitých útokoch dochádza ku krížovej kontaminácii medzi certifikátmi v rámci konkrétnej domény alebo dokonca medzi doménami.

Agentúra ENISA by mala zverejniť zoznam poverených skupín expertov a ich príslušné mandáty.

[33] https://www.sogis.eu/uk/detail_operation_en.html

26. ODKAZY

CSA *(zákon o kybernetickej bezpečnosti)*

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2019/881 zo 17. apríla 2019 o ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013.

SOG-IS MRA

Dohoda o vzájomnom uznávaní certifikátov hodnotenia bezpečnosti informačných technológií VERZIA 3.0, VÝBOR PRE RIADENIE, január 2010.

CCRA

DOHODA o uznávaní certifikátov Spoločných kritérií v oblasti bezpečnosti informačných technológií, 2. júla 2014.

ODKAZOVANÉ NORMY

Tabuľka 6: *Odkazy na normy*

Odkaz	Názov
ISO/IEC 15408	Informačné technológie - Bezpečnostné techniky - Kritériá hodnotenia bezpečnosti IT
ISO/IEC 18045	Informačné technológie - Bezpečnostné techniky - Metodika hodnotenia bezpečnosti IT
ISO/IEC 17000	Posudzovanie zhody - slovník a všeobecné zásady
ISO/IEC 17065	Posudzovanie zhody - požiadavky na orgány vykonávajúce certifikáciu produktov, procesov a služieb
ISO/IEC 17025	Skúšobné a kalibračné laboratóriá
ISO/IEC 19896-3	Požiadavky na kompetentnosť testerov a hodnotiteľov informačnej bezpečnosti. Časť 3: Požiadavky na znalosti, zručnosti a efektívnosť hodnotiteľov ISO/IEC 15408
ISO/IEC WD TS 23532-1	Požiadavky na kompetentnosť laboratórií na testovanie a hodnotenie bezpečnosti IT - Časť 1: Testovanie a hodnotenie podľa ISO/IEC 15408
ISO/IEC 27001	Informačné technológie - Bezpečnostné metódy - Systémy manažérstva informačnej bezpečnosti – Požiadavky
ISO/IEC 27002	Informačné technológie - Bezpečnostné metódy - Pravidlá dobrej praxe riadenia informačnej bezpečnosti
ISO/IEC 27005	Informačné technológie - Bezpečnostné metódy - Riadenie rizík informačnej bezpečnosti
ISO/IEC 29147	Informačné technológie - Bezpečnostné techniky - Odhaľovanie zraniteľnosti
ISO/IEC 30111	Informačné technológie - Bezpečnostné techniky - Postupy riešenia zraniteľností
ISO/IEC 7816-4	Identifikačné karty - Karty s integrovanými obvodmi - Časť 4: Organizácia, bezpečnosť a príkazy na výmenu

27. PRÍLOHA 1: VYHLÁSENIE O BALÍKU ZÁRUKY V CERTIFIKÁTE

ÚČEL

V kapitole 17, OBSAH A FORMÁT CERTIFIKÁTOV, sa vymedzujú minimálne informácie, ktoré majú byť uvedené vo všetkých certifikátoch pre produkty IKT vydaných v rámci schémy EUCC, a uvádza sa možnosť deklarovať rozšírené balíky záruky, ako to povoľuje CC.

Účelom tejto prílohy je objasniť požadované informácie o úrovni záruky alebo balíku záruky v certifikáte, aby sa predišlo jeho nesprávnemu použitiu a nedorozumeniam zo strany používateľov.

KONKRÉTNY STAV

Žiadne.

KRÍŽOVÝ ODKAZ NA KAPITOLU(-Y), V KTOREJ(-ÝCH) SÚ TIETO PRVKY VYHLÁSENÉ ZA UPLATNITEĽNÉ

Kapitola 8, ŠPECIFICKÉ KRITÉRIA A METÓDY HODNOTENIA. Kapitola 17, OBSAH A FORMÁT CERTIFIKÁTOV

V balíku záruky potvrdenom v certifikáte sa rozlišuje medzi hodnotením úrovne záruky (EAL), ktoré je v zhode CC časť 3 a rozšíreným EAL CC časť 3.

Rozšírenie sa označí uvedením skratiek rozšírených komponentov.

Rozšírenie sa podrobne uvedie v správe o certifikácii. Samotný certifikát môže obsahovať ďalšie informácie o rozšírenom komponente, napr. úplný názov komponentu ako "AVA_VAN.5 Pokročilá metodická analýza zraniteľnosti".

Príklady:

- CC časť 3 v súlade s EAL4 rozšírený o ALC_FLR.2 a AVA_VAN.5;
- alebo EAL4 v súlade s CC Part 3 rozšírený o ALC_FLR.2 - Postupy hlásenia chýb a AVA_VAN.5 - Pokročilá metodická analýza zraniteľností.

Znak "+" ako skratka pre rozšírenie EAL sa nepoužíva.

V prípade, že certifikát nepotvrdzuje žiadnu EAL, v certifikáte sa aspoň uvedie: "Špecifický balík záruky" alebo v prípade nároku na ochranný profil bez EAL: "Balík záruky v zhode s PP".

28. PRÍLOHA 2: MINIMÁLNE BEZPEČNOSTNÉ POŽIADAVKY NA LOKALITU

ÚČEL

V tejto prílohe sa definuje súbor minimálnych požiadaviek, ktoré musí vývojár splniť a ktoré môže hodnotiteľ overiť počas akéhokoľvek typu hodnotenia podľa schémy EUCC s cieľom zabezpečiť súlad s ALC_DVS.1 a ALC_DVS.2 spôsobom, ktorý je v súlade s dnešnými štandardnými postupmi pre hodnotenia vyžadujúce potenciál útoku spojený s AVA_VAN.5.

KONKRÉTNY STAV

Tieto minimálne požiadavky možno považovať za usmernenie pre ďalšie hodnotenie úrovní.

KRÍŽOVÝ ODKAZ NA KAPITOLU(-Y), V KTOREJ(-ÝCH) SÚ TIETO PRVKY VYHLÁSENÉ ZA UPLATNITEĽNÉ

Kapitola 8, ŠPECIFICKÉ KRITÉRIA A METÓDY HODNOTENIA.

1 ÚVOD

1.1 Cieľ

CEM opisuje v skupine ALC_DVS, čo má hodnotiteľ preskúmať, pokiaľ ide o bezpečnosť vývojára, ale nedefinuje minimálne bezpečnostné požiadavky na lokalitu.

Účelom tejto prílohy je definovať súbor minimálnych požiadaviek, ktoré musí vývojár splniť a ktoré je hodnotiteľ schopný overiť počas akéhokoľvek typu hodnotenia podľa schémy EUCC, aby sa zabezpečil súlad s ALC_DVS.1 a ALC_DVS.2 spôsobom, ktorý je v súlade s dnešnými štandardnými postupmi pre hodnotenia vyžadujúce potenciál útoku spojený s AVA_VAN.5.

Požiadavky stanovené v tejto prílohe sú "minimálne" v tom zmysle, že:

- všetci vývojári musia implementovať kontroly a súvisiace bezpečnostné opatrenia definované v tejto prílohe;
- môžu sa uplatňovať dodatočné požiadavky na uľahčenie ST alebo na splnenie potrieb ochrany TOE.

1.2 Objasnenie ďalších výstupov súvisiacich s rozsahom auditov na mieste

Od EAL3 sa vyžaduje ALC_DVS.1 a pre EAL6 sa očakáva ALC_DVS.2. Vzhľadom na odkaz na vysoký potenciál útoku, ktorý sa používa pre AVA_VAN.5, je bežnou praxou považovať ALC_DVS.2 za štandardné rozšírenie pre EAL4.

ALC_CMS.3 a ALC_CMS.4 sú závislé od ALC_DVS.1 a ALC_CMS.5 je závislý od ALC_DVS.2. Ostatné skupiny ALC ako ALC_CMS, ALC_DEL a ALC_TAT si vyžadujú návštevu na mieste, aby sa potvrdilo, že postupy vývojárov sú konzistentné s dôkazmi v dokumentácii

Preto sa v niektorých pracovných jednotkách ALC_CMC, ALC_CMS, ALC_DEL a ALC_TAT opísaných v CEM vyžaduje, aby sa listinné dôkazy doplnili návštevou rozvojového prostredia s cieľom skontrolovať, či sa postupy uplatňujú.

Táto príloha zahŕňa kontroly, ktoré sa musia zohľadniť, aby rozvojové prostredie malo primeranú úroveň ochrany na zachovanie dôvernosti a integrity TOE zodpovedajúcu celkovému potenciálu útoku, ako sa používa pre AVA_VAN.5 a ako sa uvádza pre TOE. Uvedené ciele sú konzistentné a vzájomne sa podporujú.

1.3 Štruktúra prílohy

Oddiel 9 pozostáva z jednej alebo viacerých bezpečnostných kontrol. Vývojár musí zohľadniť všetky kontroly, ale ak nie sú uplatniteľné, môže ich vynechať s potrebným odôvodnením. V oddiele Správa aktív sa definujú aktíva, ktoré sa majú chrániť, potrebné politiky a ich obsah, aby boli v súlade s CEM, a nasledujúce oddiely podrobne uvádzajú bezpečnostné kontroly s cieľmi a opisuje bezpečnostné opatrenia, ktoré sú potrebné na ochranu aktív súvisiacich s TOE.

Každá kontrola sa delí na 4 časti:

- Cieľ - definuje povinný cieľ kontroly, t. j. čo sa má dosiahnuť príslušnými bezpečnostnými opatreniami. Pokiaľ je kontrola uplatniteľná, ciele nemožno vynechať;
- Politiky - definuje politiky, ktoré sú povinné na uľahčenie dosiahnutia cieľa;
- Bezpečnostné opatrenia - opisuje očakávané bezpečnostné opatrenia, ktoré sú potrebné na ochranu aktív súvisiacich s TOE. Bezpečnostné opatrenia sa upravujú, nahrádzajú alebo vynechávajú len
  s odôvodnením, ktoré poskytuje jasný dôkaz, že sa dosiahla požadovaná úroveň bezpečnosti;
- Príklady - v prípade potreby ilustrujte požiadavky typickým nastavením alebo implementáciou. Tieto príklady slúžia na vysvetlenie a nemusia byť systematicky implementované tak, ako sú.

Kontroly a ciele opatrenia opísané v tomto dokumente nie sú vyčerpávajúce; v prípade potreby možno zvoliť aj ďalšie ciele opatrenia a kontroly.

1.4 Uplatnenie

Táto príloha sa uplatňuje na hodnotenie produktov IKT súvisiacich s technickou doménou smart kariet a podobných zariadení vrátane súvisiaceho vývoja softvéru. Súvisiaci softvér zahŕňa softvér potrebný na prevádzku smart kariet a podobných zariadení (firmvér, operačný systém), softvér, ktorý prispieva k bezpečnosti smart kariet a podobných zariadení, a softvér, ktorý beží na smart kartách a podobných zariadeniach.

Požiadavky sú osobitne zamerané na hodnotenie, pri ktorom má útočník vysoký potenciál útoku (AVA_VAN.5).

Túto prílohu možno považovať aj za usmernenie pre bezpečnostné hodnotenia lokalít spojených s inými produktmi IKT vždy, keď sa ALC_DVS objaví v kritériách bezpečnostných záruk, ktoré sa majú splniť. Vo všetkých prípadoch sa pri určovaní, či sú zavedené opatrenia dostatočné, zohľadňuje potenciál útoku pôvodcu hrozby v súlade so zvolenou úrovňou AVA_VAN.

V prípade technickej domény týkajúcej sa hardvérových skriniek s bezpečnostnými opatreniami nebude potrebné kontrolovať všetky výrobné miesta, ktoré vyrábajú elektronické komponenty (napr. integrované obvody, tranzistory, rezistory, pamäťové čipy) tvoriace TOE. Musia sa však navštíviť miesta relevantné z hľadiska bezpečnosti: patria sem miesta súvisiace s a) vývojom TOE, b) konečnou montážou, kde sa overuje integrita a autentickosť (ak je to vhodné) všetkých vstupujúcich, bezpečnostne relevantných častí TOE, c) počiatočným načítaním kľúčov a d) iné miesta, ak to výslovne vyžaduje ochranný profil (PP), na ktorý sa ST odvoláva.

Táto príloha vychádza z bodov 1102 a nasl. CEM a prílohy A.4.3.2 CEM. Požiadavky sú štruktúrované podľa normy ISO/IEC 27001.

Poznámka: hoci vychádza z normy ISO/IEC 27001, ďalšia podrobná špecifikácia cieľov
a bezpečnostných opatrení sa považuje za rozšírenie kontrol definovaných v tejto norme. Preto sa uplatňovanie len tejto normy nepovažuje za dostatočné a systém manažérstva informačnej bezpečnosti certifikovaný podľa normy ISO/IEC 27001 nie je nevyhnutný ani dostatočný na splnenie požiadaviek schémy EUCC definovaného v tejto prílohe.

Požiadavky uvedené v tejto prílohe sa vzťahujú na prostredia používané na vývoj (všetky kroky životného cyklu až po dodanie) TOE a interpretujú sa z pohľadu TOE v zmysle dôvernosti, integrity alebo autentickosti.

Požiadavky uvedené v tejto prílohe sú všeobecné a majú sa vzťahovať na všetky organizácie bez ohľadu na ich typ, veľkosť a charakter. Neboli zahrnuté žiadne konkrétne požiadavky zo strany PP.

1.5 Vývojár

Na splnenie požiadaviek CC pre ALC_DVS musí vývojár dosiahnuť všetky príslušné ciele stanovené v tomto dokumente. Preto sa musia zmysluplne a koordinovane implementovať príslušné opatrenia, zvyčajne opísané v pododdieloch týkajúcich sa bezpečnostných opatrení.

Vývojár musí zohľadniť všetky kontroly uvedené v tomto dokumente, aby mohol prejsť hodnotením bezpečnosti lokality. Každé vylúčenie kontrolných mechanizmov musí byť odôvodnené a musí sa preukázať, že neovplyvní schopnosť a/alebo zodpovednosť vývojára zabezpečiť úroveň bezpečnosti, ktorá spĺňa bezpečnostné potreby vyplývajúce z ST a cieľov definovaných v tomto dokumente.

Ak vývojár implementuje iné bezpečnostné nastavenie, napr. upraví, nahradí alebo vynechá bezpečnostné opatrenia, musí zabezpečiť a preukázať, že ciele sú splnené a požadovaná úroveň bezpečnosti je dosiahnutá.

Vývojár poskytne hodnotiteľovi odôvodnenie.

Vývojár sa môže odvolať na tento dokument, aby podporil odôvodnenie, že opatrenia zachovávajú dôvernosť a integritu.

1.6 ITSEF

V súlade s § 13.5 CEM je cieľom určiť, či sú bezpečnostné kontroly vývojára vo rozvojovom prostredí primerané na zabezpečenie dôvernosti a integrity návrhu a implementácie TOE, ktoré sú potrebné na zabezpečenie toho, aby nebola ohrozená bezpečná prevádzka TOE.

ALC_DVS sa zameriava na všetky miesta, na ktorých prebieha vývoj TOE a ktoré sú uvedené v bezpečnostnej dokumentácii vývoja. Táto príloha sa musí použiť na posúdenie každého z týchto miest.

V bodoch ALC_DVS.1.1 a ALC_DVS.2.1 sa uvádza, že hodnotiteľ preskúma bezpečnostnú dokumentáciu vývoja, aby zistil, či obsahuje podrobné informácie o všetkých bezpečnostných opatreniach použitých vo rozvojovom prostredí, ktoré sú potrebné na ochranu dôvernosti a integrity návrhu a implementácie TOE.

S cieľom určiť dostatočnosť použitých bezpečnostných opatrení ITSEF preskúma:

- politiky dôvernosti a integrity vývoja a predpoklady ST;
- zdôvodnenie (napr. posudzovanie rizika) vylúčenia alebo neúplného vykonania kontrol a;
- správne a zosúladené vykonávanie opatrení požadovaných v rámci kontrol.

Ak ST identifikuje bezpečnostný(-é) cieľ(-e) pre rozvojové prostredie, ktorý(-é) si vyžaduje(-ú) špecifické požiadavky na politiky, hodnotiteľ ho(ich) pri hodnotení zohľadní.

ALC_DVS.2.2 uvádza, že hodnotiteľ preskúma bezpečnostnú dokumentáciu vývoja, aby zistil, či je uvedené primerané odôvodnenie, prečo bezpečnostné opatrenia poskytujú potrebnú úroveň ochrany na zachovanie dôvernosti a integrity TOE.

Hodnotiteľ preskúma správne a zosúladené vykonávanie opatrení požadovaných v rámci kontrol. Ak vývojár implementuje kontroly neúplne alebo s inými bezpečnostnými opatreniami, ako sa očakáva, odôvodnenie poskytnuté vývojárom by malo obsahovať preukázanie, že sa dosiahla požadovaná úroveň bezpečnosti.

Hodnotiteľ preskúma túto ukážku a určí, či sa dosiahli ciele definované v kapitole 9 tohto dokumentu.

Hodnotiteľ určí, či odôvodnenie zohľadňuje ST pre všetky informácie, ktoré si môžu vyžadovať dodatočné bezpečnostné požiadavky rozvojového prostredia.

Hodnotiteľ určí, či odôvodnenie zahŕňa všetky aspekty vývoja a výroby na všetkých rôznych miestach so všetkými zúčastnenými úlohami až po dodanie TOE a či sa tento dokument uplatňuje na tieto rôzne etapy a miesta správne a konzistentne.

Požiadavky definované v tomto dokumente by mal hodnotiteľ použiť na vytvorenie kontrolného zoznamu na prípravu návštevy na mieste a preskúmanie dôkazov, ktoré sa vyžadujú podľa ALC_DVS.1.3

a ALC_DVS.2.4.

2 NORMATÍVNE ODKAZY

Na uplatňovanie tejto prílohy sú nevyhnutné tieto dokumenty. Pre datované odkazy platí len citované vydanie. Pre nedatované odkazy platí posledné vydanie odkazovaného dokumentu (vrátane všetkých zmien a doplnení).

- Spoločné kritériá hodnotenia bezpečnosti informačných technológií, časť 1-3, apríl 2017, verzia 3.1, vydanie 5;
- Spoločná metodika hodnotenia bezpečnosti informačných technológií, Metodika hodnotenia, apríl 2017, verzia 3.1 release 5;
- ISO/IEC 27002, Informačné technológie - Bezpečnostné techniky - Kódex postupov pre kontroly riadenia informačnej bezpečnosti.

Pri implementácii príslušných procesov môžu byť užitočné tieto normy.

- ISO/IEC 27001, Informačné technológie - Bezpečnostné metódy - Systémy manažérstva informačnej bezpečnosti - Požiadavky;
- ISO/IEC 27005, Informačné technológie - Bezpečnostné metódy - Riadenie rizík informačnej bezpečnosti.

3 TERMÍNY A DEFINÍCIE

Na účely tejto prílohy sa uplatňujú tieto pojmy a definície.

Aktíva: Objekty, ktorým vlastník TOE pravdepodobne pripisuje hodnotu.

V kontexte vývojového bezpečnostného systému sú aktíva informácie v elektronickej alebo inej forme, zariadenia na spracovanie informácií a procesy odkazovania (vrátane systémov kontroly prístupu a poplachových systémov), vývojové nástroje a prostredia, akýkoľvek prejav TOE a zákaznícky kód a údaje poskytnuté na vytvorenie TOE.

Dostupnosť: Vlastnosť byť prístupný a použiteľný na požiadanie oprávneného subjektu.

Obchodné operácie: Všeobecný termín pre súhrn operácií vykonávaných vývojárom v súvislosti s TOE, napr. "personalizácia" je súčasťou obchodných operácií.

COBIT: Ciele opatrenia pre informačné a súvisiace technológie.

Dôvernosť: Vlastnosť, že informácie nie sú sprístupnené alebo odhalené neoprávneným osobám, subjektom alebo procesom.

Kontrola: Súbor opatrení spojených s jedným alebo viacerými cieľmi, ktoré majú reagovať na hrozby.

Zariadenia na spracovanie údajov: Priestory, zariadenia, inštalácie alebo nástroje používané na spracovanie údajov.

Vývojár: Subjekt (miesto), ktorý ponúka služby a je súčasťou procesu vývoja a výroby; zahŕňa všetky kroky životného cyklu až po dodanie zákazníkovi, napr. vývoj softvéru, návrh čipu, výroba masky, výroba wafera, testovanie, montáž atď. Vývojár je zodpovedný aj za podporné funkcie.

Rozvojové prostredie: Prostredie, v ktorom sa TOE vyvíja; vývoj zahŕňa výrobu TOE.

DMZ: V oblasti počítačovej bezpečnosti je DMZ fyzická alebo logická podsieť, ktorá obsahuje externé služby organizácie a vystavuje ich väčšej nedôveryhodnej sieti, zvyčajne internetu.

DSD: Bezpečnostná vývojová dokumentácia.

DSS: Systém bezpečnosti vývoja.

Zamestnanie: Slovo "zamestnanie" sa tu vzťahuje na všetky tieto rôzne situácie: zamestnávanie ľudí (dočasné alebo dlhodobé), menovanie na pracovné pozície, zmena pracovných pozícií, pridelenie zmlúv a ukončenie ktoréhokoľvek z týchto dojednaní.

Zariadenie: Akékoľvek zariadenie, inštalácia alebo nástroj, bez ohľadu na to, či ide o softvér alebo hardvér, ktorý je súčasťou systému riadenia bezpečnosti.

FW: Firmware.

Oblasť s vysokým stupňom zabezpečenia: Oblasť, v ktorej sú prístupné údaje alebo materiály súvisiace s TOE klasifikované ako "kritické" alebo "veľmi kritické", a prípadne oblasti kontroly bezpečnosti (kontrola prístupu a detekcia vniknutia).

Informačná bezpečnosť (IS): Okrem toho môžu byť zahrnuté aj ďalšie vlastnosti, ako je autentickosť, zodpovednosť, neodmietnuteľnosť a spoľahlivosť.

Integrita: Integrita: vlastnosť ochrany presnosti a úplnosti aktív.

Podujatie IS: Identifikovaný výskyt stavu systému, služby alebo siete, ktorý naznačuje možné porušenie politiky informačnej bezpečnosti alebo zlyhanie bezpečnostných opatrení, alebo predtým neznámu situáciu, ktorá môže byť bezpečnostne relevantná.

Incident IS: Jedna alebo séria nežiaducich alebo neočakávaných udalostí v oblasti informačnej bezpečnosti, ktoré s veľkou pravdepodobnosťou ohrozujú obchodné operácie a informačnú bezpečnosť.

ISMS: Systém riadenia informačnej bezpečnosti.

ITIL: Knižnica infraštruktúry informačných technológií.

Škodlivý kód: Na základe predpokladaného zámeru autora sa vytvorí vírus, červ, trójsky kôň, spyware a adware.

Kód mobilného telefónu: Softvér získaný zo vzdialených systémov prenášaný cez sieť, napr. kód Java, ovládacie prvky ActiveX, flashové animácie, kancelárske makrá atď.

Mobilná výpočtová technika: Mobilná výpočtová technika využíva komunikačné technológie na prácu v nekontrolovanom prostredí mimo priestorov vývojára.

MSSR: Minimálne bezpečnostné požiadavky na pracovisko, skratka pre tento dokument.

Sieťová architektúra: Rámec pre špecifikáciu fyzických komponentov siete a ich funkčnej organizácie a konfigurácie, jej prevádzkových princípov a postupov, ako aj dátových formátov používaných pri jej prevádzke.

Organizácia: Skupina ľudí a zariadení s usporiadaním zodpovedností, právomocí a vzťahov.

Bezpečnostná politika organizácie: Súbor bezpečnostných pravidiel, postupov alebo usmernení pre organizáciu.

OS: Operačný systém.

Vlastník: Pojem vlastník označuje jednotlivca alebo subjekt, ktorý má schválenú riadiacu zodpovednosť za kontrolu výroby, vývoja, údržby, používania a bezpečnosti aktív. Pojem vlastník neznamená, že táto osoba má k aktívam akékoľvek vlastnícke práva.

Partner: Vývojová spoločnosť, maskovňa, výrobný závod, testovacia hala, montážna linka, bez ohľadu na ich vlastníctvo.

Politika: Politika sa môže vzťahovať na konkrétne prevádzkové prostredie.

Postup: Určený spôsob vykonania činnosti.

Proces: Postupnosť činností alebo postupov.

Spoľahlivosť: Schopnosť zariadenia alebo postupu vykonávať požadovanú funkciu v priebehu času.

Vzdialený prístup: Pripojenie k systému spracovania údajov z miesta mimo priestorov pomocou sieťového pripojenia, kde:
- spojenie je mimo logického bezpečnostného prostredia;
- pracovné miesto je mimo fyzického bezpečnostného prostredia.

Zvyškové riziko: Riziko, ktoré zostáva po ošetrení rizika.

Prijatie rizika: Rozhodnutie prijať riziko.

Analýza rizík: Systematické využívanie informácií na identifikáciu zdrojov a odhad rizika.

Posudzovanie rizika: Celkový proces analýzy a hodnotenia rizík.

Hodnotenie rizika: proces porovnania odhadovaného rizika s danými kritériami rizika s cieľom určiť významnosť rizika.

Riadenie rizík: Koordinované činnosti na riadenie a kontrolu organizácie s ohľadom na riziko.

Liečba rizík: Proces výberu a implementácie opatrení na úpravu rizika.

SAM: Modul zabezpečeného prístupu (alebo modul zabezpečenej aplikácie).

Citlivé údaje: Údaje, ktoré je potrebné chrániť, aby sa podporili požiadavky na dôvernosť a/alebo integritu.

Silná autentizácia: Autentizácia s najmenej dvoma nezávislými faktormi, napr. vlastníctvo a znalosť (odznak a PIN) alebo vlastníctvo a individuálny atribút (odznak a biometria).

Člen tímu: Pojem "člen tímu" zahŕňa zamestnancov, dodávateľov, konzultantov, študentov a používateľov tretích strán, ktorí sa podieľajú na zabezpečených procesoch alebo majú prístup k chráneným informáciám.

Práca na diaľku: Práca na diaľku využíva komunikačné technológie na prácu na diaľku z pevného miesta mimo sídla vývojára.

Používateľ tretej strany; akýkoľvek používateľ, ktorý nie je zamestnancom, dodávateľom, konzultantom alebo študentom, napr. zákazník, ITSEF, CB.

Hrozba: Akákoľvek okolnosť alebo udalosť, ktorá môže mať nepriaznivý vplyv na prevádzku organizácie, aktíva (vrátane TOE alebo jej častí) alebo jednotlivcov prostredníctvom neoprávneného prístupu, zničenia, zverejnenia, modifikácie a/alebo odmietnutia služby.

Taktiež potenciál zdroja hrozby úspešne zneužiť konkrétnu zraniteľnosť systému. Spoločné kritériá charakterizujú hrozbu z hľadiska (a) pôvodcu hrozby, (b) predpokladaného spôsobu útoku, (c) akejkoľvek zraniteľnosti, ktorá je základom útoku, a (d) systémového zdroja, ktorý je napadnutý.

Vrcholový manažment: Najvyššie postavený manažment (s titulmi ako predseda/predsedníčka, výkonný riaditeľ, generálny riaditeľ, prezident, výkonní riaditelia, výkonní viceprezidenti atď.) zodpovedný za celý podnik. V organizáciách, kde vývojár nie je jedinou činnosťou, sa "vrcholový manažment vývojárskej organizácie" môže vzťahovať na manažment divízie, obchodnej skupiny, produktovej línie atď.

VPN: virtuálna privátna sieť; termín bezpečná VPN sa používa pre siete VPN bez potenciálneho rizika odpočúvania, napr. pomocou šifrovaných tunelov IPSec alebo SSL alebo špeciálnych fyzicky zabezpečených vnútorných spojení v prípade prekročenia inej bezpečnostnej zóny.

Terminológia ISO, ako napríklad "môže", "smie", "normatívny", "musí" a "mal by", ktorá sa používa v prílohe, je definovaná v smerniciach ISO/IEC, časť 2:

(Všimnite si, že termíny "má byť" a "normatívny" majú pri používaní tejto normy ďalší význam. Pozri poznámku nižšie.)

- slovo "musí" označuje opatrenia, ktoré sa musia striktne dodržiavať, aby boli v súlade s prílohou, a od ktorých nie je povolená žiadna odchýlka.
- slovo "má byť" naznačuje, že spomedzi viacerých možností sa odporúča jedna ako obzvlášť vhodná bez toho, aby sa uvádzali alebo vylučovali iné, alebo že sa uprednostňuje určitý postup, ktorý však nie je nevyhnutne potrebný. Séria ISO/IEC 15408 interpretuje slovo "nie je nevyhnutne potrebné"
  v tom zmysle, že výber inej možnosti si vyžaduje zdôvodnenie, prečo nebola zvolená uprednostňovaná možnosť.
- slovo "smie" označuje spôsob konania, ktorý je v rámci prílohy prípustný.
- slovo "môže" sa používa na vyjadrenie možnosti a schopnosti, či už materiálnej, fyzikálnej alebo kauzálnej.
- výraz "dôvernosť a/alebo integrita" znamená buď "dôvernosť", alebo "integritu", alebo kombináciu oboch.
- výraz "normatívny" označuje opatrenia, ktoré nie je povinné dodržiavať, aby boli v súlade s dokumentom.

4 SYSTÉM BEZPEČNOSTI VÝVOJA A DOKUMENTÁCIA

4.1 Cieľ

V súlade s požiadavkami ALC_DVS.1.1C, resp. ALC_DVS.2.1C sa v bezpečnostnej dokumentácii

vývoja (DSD) opíšu fyzické, logické, procedurálne, personálne a iné bezpečnostné opatrenia, ktoré sú potrebné na ochranu dôvernosti a integrity návrhu a implementácie TOE v jeho rozvojovom prostredí.

DSD identifikuje všetky lokality, kde dochádza k rozvoju, rozvojové činnosti a bezpečnostné opatrenia uplatňované na každej lokalite v súvislosti s týmito činnosťami a pri preprave medzi rôznymi lokalitami.

Ak sa požaduje ALC_DVS.2, bezpečnostná dokumentácia vývoja musí zdôvodniť, že bezpečnostné opatrenia poskytujú potrebnú úroveň ochrany na zachovanie dôvernosti a integrity TOE podľa potenciálu útoku uvedeného v ST (AVA_VAN.5).

4.2 Zásady

Dôkazom hodnotenia bezpečnosti vývoja je ST a bezpečnostná dokumentácia vývoja (DSD). Vývojár preto musí vytvoriť, zaviesť, prevádzkovať, monitorovať, udržiavať, revidovať a zlepšovať zdokumentovaný systém bezpečnosti vývoja (DSS) v kontexte celkových obchodných činností organizácie a rizík, ktorým čelí.

DSD zdokumentuje a hodnotiteľ preskúma politiky dôvernosti a integrity vývoja, ktoré podrobne popisujú:

- ktoré informácie týkajúce sa vývoja TOE musia byť dôverné a ktorí členovia vývojového tímu majú k takýmto materiálom prístup;
- aký materiál musí byť chránený pred neoprávnenými úpravami, aby sa zachovala integrita TOE, a ktorí členovia vývojového personálu môžu takýto materiál upravovať.
- Politiky obsahujú opis organizácie vývojárov, príslušných úloh a zavedených bezpečnostných opatrení. Podľa ALC_DVS sa pri dokumentácii zohľadňujú tieto typy bezpečnostných opatrení:
- Fyzické, napr. kontrola prístupu a detekcia narušenia;
- Procedurálne, napr. udeľovanie a zrušenie prístupových práv, prenos chráneného materiálu, úlohy a zodpovednosti bezpečnostného personálu;
- Personál, napr. kontrola dôveryhodnosti;
- Ďalšie bezpečnostné opatrenia, napr. logická ochrana všetkých vývojových strojov.

4.3 Bezpečnostné opatrenia

Medzi hrozby, ktoré je potrebné pokryť vhodnými bezpečnostnými opatreniami, patria:

- "Náhodná hrozba": možnosť ľudskej chyby alebo opomenutia, neúmyselnej poruchy zariadenia alebo prírodnej katastrofy;
- "Úmyselná hrozba": možnosť útoku inteligentného subjektu (napr. individuálneho hackera alebo zločineckej organizácie). Príkladmi takýchto útokov sú krádež a lúpež, úmyselná výmena TOE alebo jeho častí a klonovanie.

Ak sa vyžaduje odôvodnenie, táto príloha sa môže použiť ako základ po prispôsobení konkrétnej situácii a prostrediu vývojára.

Schopnosť preukázať prepojenie vybraných kontrol s výsledkami procesu posudzovania a ošetrovania rizík a následne s politikou a cieľmi DSD môže podporiť pracovné balíky ITSEF aj odôvodnenie podľa ALC_DVS.2.2C.

Kontrola dokumentov

Dokumenty požadované DSS by mali byť kontrolované a chránené. Mal by sa stanoviť zdokumentovaný postup na vymedzenie riadiacich činností potrebných na:

- pred vydaním schváliť dokumenty z hľadiska ich primeranosti;
- preskúmavať a aktualizovať dokumenty podľa potreby a opätovne ich schvaľovať;
- zabezpečiť identifikáciu zmien a aktuálneho stavu revízie dokumentov;
- zabezpečiť, aby dokumenty zostali čitateľné a ľahko identifikovateľné;
- zabezpečiť, aby dokumenty boli k dispozícii tým, ktorí ich potrebujú, a aby sa prenášali, uchovávali a nakoniec likvidovali v súlade s postupmi platnými pre ich utajenie;
- zabrániť neúmyselnému používaniu zastaraných dokumentov;
- použiť na ne vhodnú identifikáciu, ak sa uchovávajú na akýkoľvek účel.

Zriadenie a riadenie DSS a DSD

Podľa CEM sa v ALC_DVS.1-2 vyžaduje, aby hodnotiteľ preskúmal politiky dôvernosti a integrity vývoja s cieľom určiť dostatočnosť použitých bezpečnostných opatrení.

Vývojár môže štruktúrovať DSD podľa potreby. Môže pozostávať zo systému manažérstva informačnej bezpečnosti podľa normy ISO 27001, môže byť štruktúrovaná podľa tejto prílohy alebo môže byť štruktúrovaná akýmkoľvek spôsobom, ktorý je pre vývojára vhodný.

Na podporu tohto pracovného balíka ITSEF by mal vývojár:

- definovať bezpečnostnú politiku, ktorá obsahuje rámec na stanovenie cieľov a stanovuje celkové smerovanie a zásady činnosti vzhľadom na potreby integrity a dôvernosti TOE;
- definovať prístup organizácie k posudzovaniu rizík vrátane metodiky posudzovania rizík, ktorá je vhodná pre DSS, identifikovanú bezpečnosť a právne a regulačné potreby na ochranu TOE;

Poznámka: Posudzovanie rizík je určené na identifikáciu, analýzu a hodnotenie rizík, identifikáciu, hodnotenie a výber cieľov opatrení a kontrolných mechanizmov na ošetrenie rizík a na získanie porovnateľných a reprodukovateľných výsledkov.

- formulovať plán zaobchádzania s rizikami, ktorý identifikuje vhodné riadiace opatrenia, zdroje, zodpovednosti a priority pre riadenie bezpečnostných rizík;
- implementovať plán zaobchádzania s rizikami s cieľom dosiahnuť stanovené ciele kontroly, ktorý zahŕňa zváženie financovania a rozdelenie úloh a zodpovedností;
- opísať všetky vybrané ciele opatrenia a kontroly a ich implementáciu vrátane potrebných procesov a operačných postupov.

DSD by mal obsahovať:

- zdokumentované vyhlásenia o politike a cieľoch DSS;
- rozsah pôsobnosti DSS, pokiaľ ide o TOE;
- postupy a kontroly na podporu DSS;
- zdokumentované postupy, ktoré organizácia potrebuje na zabezpečenie efektívneho plánovania, prevádzky a kontroly svojich procesov bezpečnosti vývojárov.

Monitorovanie a preskúmanie DSS

Vývojár by mal:

- vykonávať monitorovacie a revízne postupy a iné kontrolné mechanizmy s cieľom:
  - okamžite zistiť chyby vo výsledkoch spracovania;
  - okamžite identifikovať pokusy o narušenie bezpečnosti a úspešné incidenty;
  - umožniť manažmentu určiť, či bezpečnostné činnosti delegované na ľudí alebo realizované technológiou fungujú podľa očakávaní;
  - pomôcť odhaliť bezpečnostné udalosti, a tým predchádzať bezpečnostným incidentom pomocou indikátorov;
  - určiť, či opatrenia prijaté na vyriešenie porušenia bezpečnosti boli účinné;
- vykonávať pravidelné preskúmania efektívnosti DSS s prihliadnutím na výsledky bezpečnostných auditov, incidenty, výsledky meraní efektívnosti a návrhy a spätnú väzbu od všetkých zainteresovaných strán;
- v plánovaných intervaloch preskúmavať posudzovanie rizík a prehodnocovať zostatkové riziká a identifikované prijateľné úrovne rizík;
- vykonávať interné audity DSS v plánovaných intervaloch definovaných v DSD;
- aktualizovať bezpečnostné plány tak, aby zohľadňovali zistenia monitorovacích a kontrolných činností.

Údržba a aktualizácia DSD

Aby sa zabezpečila pravidelná aktualizácia DSD, vývojár:

- by mal implementovať identifikované zlepšenia DSS v DSD;
- by mal prijať príslušné nápravné a preventívne opatrenia v súlade s oddielom venovaným zlepšovaniu DSS;
- môže uplatniť poznatky získané z bezpečnostných skúseností iných organizácií a skúseností

samotnej organizácie;
- by mal oznámiť opatrenia a zlepšenia všetkým zainteresovaným stranám s úrovňou podrobnosti primeranou okolnostiam a podľa potreby sa dohodnúť na ďalšom postupe.

Kontrola záznamov

Mali by sa vytvoriť a uchovávať záznamy, ktoré poskytnú dôkaz o súlade s požiadavkami vrátane účinného fungovania DSS. Mali by byť vhodne chránené a kontrolované. Záznamy by mali zostať čitateľné, ľahko identifikovateľné a vyhľadateľné. Kontroly potrebné na identifikáciu, uchovávanie, ochranu, vyhľadávanie, čas uchovávania a likvidáciu záznamov by mali byť zdokumentované a zavedené.

Mali by sa viesť záznamy o fungovaní procesov a o všetkých prípadoch významných bezpečnostných incidentov súvisiacich s DSS.

4.4 Príklady

Bežnou praxou je vymedzenie rozsahu a hraníc DSS s ohľadom na charakteristiky organizácie, jej umiestnenie, aktíva a technológie, vrátane podrobností a zdôvodnenia každého vylúčenia z rozsahu pôsobnosti.

Pravidlá a predpisy týkajúce sa hierarchie dokumentov, štruktúry dokumentov, postupov vydávania atď. sú často definované v systéme manažérstva kvality podľa noriem radu ISO 9000. Zvyčajne sa v systéme QMS definuje aj prístup k preventívnym a nápravným opatreniam, schémam auditov a preskúmaniu manažmentom.

Systém riadenia informačnej bezpečnosti podľa noriem radu ISO 27000 definuje všetky potrebné opatrenia na zachovanie dôvernosti, integrity a dostupnosti informácií prostredníctvom procesu riadenia rizík a poskytuje zainteresovaným stranám istotu, že riziká sú primerane riadené. Dokumentácia ISMS odkazuje na rámec ITIL a/alebo COBIT vývojára.

Ak sú príslušné činnosti EUCC súčasťou väčšej organizácie, osobitné bezpečnostné opatrenia sú opísané v dodatočnej dokumentácii. Môžu to byť ďalšie kapitoly vo vyššie uvedených dokumentoch, osobitný dokument obsahujúci osobitné predpisy a odkazujúci na vyššie uvedené dokumenty pre všetky spoločné predpisy alebo osobitný DSD.

5 ZODPOVEDNOSŤ MANAŽMENTU

5.1 Cieľ

Vývojár musí mať presne definované, zdokumentované a pridelené úlohy a zodpovednosti za všetky činnosti, ktoré môžu mať vplyv na dôvernosť a integritu TOE.

Všetky zdroje potrebné na zachovanie dôvernosti a integrity TOE musia byť určené a dostupné.

Všetky fyzické, procedurálne, personálne a iné bezpečnostné opatrenia, ktoré sú potrebné na ochranu dôvernosti a integrity TOE, musia byť účinné.

5.2 Zásady

Celková bezpečnostná politika definuje prístup vývojára k bezpečnosti a oblasť použiteľnosti. Stanoví celkový zmysel smerovania a zásady činnosti s ohľadom na potreby dôvernosti a integrity TOE.

5.3 Bezpečnostné opatrenia

Vrcholový manažment by mal definovať právnu a organizačnú štruktúru vývojára a je zodpovedný za dôvernosť a integritu TOE.

Záväzok manažmentu

Vrcholový manažment by mal podporovať zavedenie, implementáciu, prevádzku, monitorovanie, preskúmanie, údržbu a zlepšovanie DSS, prinajmenšom tým, že pridelí jednu alebo viac osôb do funkcie bezpečnostného manažéra a poskytne potrebné zdroje.

Bezpečnostný manažér

Bezpečnostný manažér (manažéri) by mal byť zodpovedný za celkovú bezpečnosť v oblasti zodpovednosti vývojárov počas celého životného cyklu vývoja TOE vrátane všetkých subdodávateľov, ktorí môžu byť využití. V tejto funkcii by mal bezpečnostný manažér podliehať vrcholovému manažmentu organizácie vývojárov. Ciele a úlohy bezpečnostného manažéra zahŕňajú okrem iného požiadavky opísané v tomto oddiele.

Riadenie zdrojov

Organizácia by mala určiť a poskytnúť zdroje potrebné na splnenie požiadaviek stanovených v tejto prílohe. Určenie by sa malo pravidelne aktualizovať alebo po významnej zmene hrozieb alebo prostredia.

Vývojár je zodpovedný za všetky použité zdroje bez ohľadu na ich vlastníctvo.

Všetky úlohy a zodpovednosti spojené s činnosťami vývojárov by mali byť dobre definované a zdokumentované, napr. pracovné postupy, opisy úloh, organizačné schémy.

Všetci zamestnanci vrátane členov externých strán musia byť kompetentní vykonávať pridelené úlohy.

V prípade potreby by mali organizačné opatrenia zabezpečiť oddelenie povinností medzi vývojom, výrobou, testovaním, zárukou kvality a bezpečnosťou.

Dohody o mlčanlivosti

Mali by sa určiť a pravidelne prehodnocovať požiadavky na dohody o dôvernosti alebo o mlčanlivosti, ktoré odrážajú potreby vývojára na ochranu informácií, údajov a materiálov.

Mali by sa uzavrieť potrebné dohody.

6 INTERNÉ AUDITY DSS

6.1 Cieľ

Interné audity zabezpečia, aby sa bezpečnostné opatrenia vykonávali zmysluplne a zosúladene a aby bezpečnostné opatrenia účinne podporovali zamýšľaný účel.

6.2 Zásady

Zodpovednosti a požiadavky na plánovanie a vykonávanie auditov, podávanie správ o výsledkoch a uchovávanie záznamov sa vymedzia v zdokumentovanom postupe.

6.3 Bezpečnostné opatrenia

Organizácia by mala v plánovaných intervaloch vykonávať interné audity DSS s cieľom určiť, či sú ciele opatrenia, kontroly, procesy a postupy jej DSS:

- spĺňajú požiadavky tohto dokumentu s požiadavkami;
- spĺňajú identifikované bezpečnostné potreby TOE;
- sú účinne implementované a udržiavané;
- fungujú podľa očakávaní.

Program auditu by sa mal naplánovať s prihliadnutím na stav a dôležitosť procesov a oblastí, ktoré sa majú auditovať, ako aj na výsledky predchádzajúcich auditov. Mali by sa definovať kritériá, rozsah, frekvencia a metódy auditu. Výber audítorov a vykonávanie auditov by mali zabezpečiť objektívnosť a nestrannosť procesu auditu. Audítori nesmú vykonávať audit svojej vlastnej práce.

Vedenie zodpovedné za auditovanú oblasť zabezpečí, aby sa bez zbytočného odkladu prijali opatrenia na odstránenie zistených nezhôd a ich príčin. Následné činnosti by mali zahŕňať overovanie prijatých opatrení a podávanie správ o výsledkoch overovania.

7 DSS A PRESKÚMANIE MANAŽMENTON (INFORMATÍVNE)

7.1 Cieľ

Vedenie by malo zabezpečiť, aby mal vývojár dobre definované, zdokumentované a pridelené úlohy a zodpovednosti za všetky činnosti, ktoré môžu mať vplyv na dôvernosť a integritu TOE.

Všetky fyzické, procedurálne, personálne a iné bezpečnostné opatrenia, ktoré sú potrebné na ochranu dôvernosti a integrity TOE, by mali byť účinné.

7.2 Zásady

Proces preskúmania manažmentom by mal byť zdokumentovaný.

7.3 Bezpečnostné opatrenia

Vedenie by malo v plánovaných intervaloch alebo pri významných zmenách v implementácii bezpečnosti preskúmať DSS organizácie, aby sa zabezpečila jeho trvalá vhodnosť, primeranosť a efektívnosť. Toto preskúmanie môže zahŕňať posúdenie príležitostí na zlepšenie a potrebu zmien DSS. Výsledky preskúmaní by mali byť jasne zdokumentované a mali by sa uchovávať záznamy.

Vstupné údaje z preskúmania

Vstupy do preskúmania riadenia by mali zahŕňať:

- výsledky auditov a preskúmaní DSS;
- spätnú väzbu od zainteresovaných strán, najmä od hodnotiacich a certifikačných orgánov;
- stav preventívnych a nápravných opatrení;
- zraniteľnosti alebo hrozby, ktoré neboli dostatočne zohľadnené v predchádzajúcom posudzovaní rizík;
- následné opatrenia z predchádzajúcich preskúmaní riadenia;
- všetky zmeny, ktoré by mohli ovplyvniť DSS;
- odporúčania na zlepšenie.

Výstup z preskúmania

Výstup z preskúmania riadenia by mal zahŕňať všetky rozhodnutia a opatrenia týkajúce sa:

- zlepšenie efektívnosti DSS;
- aktualizácia posudzovania rizík a plánu zaobchádzania s rizikami;
- úprava postupov a kontrolných mechanizmov, ktoré majú vplyv na bezpečnosť, podľa potreby v reakcii na vnútorné alebo vonkajšie udalosti, ktoré môžu mať vplyv na DSS;
- potrebné zdroje.

8 ZLEPŠENIE DSS

8.1 Cieľ

Efektívnosť fyzických, procedurálnych, personálnych a iných bezpečnostných opatrení, ktoré sú potrebné na ochranu dôvernosti a integrity TOE, sa preskúma a v prípade potreby zlepší.

8.2 Zásady

V politikách sa vymedzí, ako sa udržiava efektívnosť bezpečnostných opatrení napriek vyvíjajúcim sa hrozbám a s ohľadom na možné nedostatky.

8.3 Bezpečnostné opatrenia

Neustále zlepšovanie

Vývojár môže neustále zlepšovať efektívnosť DSS pomocou bezpečnostnej politiky, bezpečnostných cieľov, výsledkov auditu, analýzy monitorovaných udalostí, nápravných a preventívnych opatrení

a preskúmania manažmentom.

Nápravné opatrenie

Vývojár by mal prijať opatrenia na odstránenie príčin nesúladu s požiadavkami DSS, aby sa zabránilo jeho opakovaniu.

Preventívne opatrenia

Vývojár by mal určiť opatrenia na odstránenie príčin potenciálnych nezhôd s požiadavkami DSS, aby sa zabránilo ich výskytu.

Vývojár by mal identifikovať zmenené hrozby a definovať preventívne opatrenia zamerané na výrazne zmenené riziká.

9 CIELE KONTROLY A KONTROLNÉ MECHANIZMY

9.1 Správa aktív

Bezpečnosť sa týka všetkých druhov aktív, ale nie všetky aspekty aktív patria do rozsahu pôsobnosti tohto DSS, napr. QM (manažérstvo kvality), ESH (životné prostredie, bezpečnosť, zdravie).

9.1.1 Celkový cieľ

Aktíva musia byť jasne identifikované s prideleným typom ochrany (dôvernosť, integrita, autentickosť) a spravované.

Každé aktívum má vlastníka.

9.1.2 Zodpovednosť za aktíva

Cieľ

Vymedzí sa vlastníctvo a prijateľné používanie aktíva a jeho rozmiestnenie.

Zásady

DSD by mala definovať vlastníctvo a správu všetkých aktív.

Pravidlá prijateľného používania informácií a aktív by sa mali určiť a zdokumentovať v súlade s politikami klasifikácie.

Bezpečnostné opatrenia

Najdôležitejšími aktívami v rozsahu pôsobnosti tejto prílohy sú TOE alebo jeho časti. Ich podoba sa však v jednotlivých segmentoch líši vo fáze vývoja ich životného cyklu.

Vývojár by mal pri definovaní aktív zohľadniť zoznam dôležitých aktív uvedený v príklade. Mali by byť k dispozícii a udržiavané súpisy aktív.

Pre všetky aktíva v rôznych fázach vývoja by sa mali určiť a vymenovať vlastníci. Vykonávanie vlastníctva musí byť zrejmé pre všetkých vlastníkov. Vykonávanie konkrétnych kontrol môže vlastník podľa potreby delegovať, ale vlastník zostáva zodpovedný za riadnu ochranu aktív.

Pravidlá prijateľného používania informácií a aktív by sa mali prísne presadzovať a overovať v rámci interných auditov.

Aktíva, najmä počítače, a všetko ostatné vybavenie a materiál, ktoré poskytol vývojár, by sa mali používať len na oficiálne účely a len v súlade s pravidlami stanovenými v DSS a súvisiacich dokumentoch.

Príklady

Pre typický produkt smart karty (výrobca IC) platia tieto segmenty životného cyklu a formy TOE;

- Návrh - koncept zabezpečenia, rozloženie, plán siete, softvér, údaje, väzba, návrh dokumentov (ADV-class)
- Výroba masky - údaje o vzore, údaje o maske, mriežka
- Výroba waferu - mriežka, wafer
- Test waferu - wafer, testovací program, aplikácia (flash), dáta aplikácie (EEPROM)
- Montáž - wafer, moduly/čipy/balenie, testovací program, inicializačné údaje, vstavaný softvér
- Výroba kariet a vložiek - moduly, karty
- Personalizácia - karty/vložky, vstavaný softvér, údaje
- Zásielky - mriežka, wafer, moduly/čipy, karty/vrstvy
- Odpady a šrot sa môžu objaviť vo všetkých segmentoch a mali by sa považovať za aktíva.

Pre typické produkty súvisiace s hardvérovými zariadeniami technickej domény s bezpečnostnými skrinkami platia tieto segmenty životného cyklu a formy TOE. Keďže táto TD zahŕňa rôzne typy produktov, segmenty životného cyklu by sa mierne líšili:

- Fáza návrhu a vývoja
- Fáza výroby
- Prípravná fáza
- Doručovanie komponentov*
- Montáž*
- Inicializácia
- Generovanie a vkladanie bezpečnostných údajov*
- Rozdelenie úložiska*
- Oprava*
- Fáza inštalácie a kalibrácie*
- Kontrola a kalibrácia*
- Aktivácia, párovanie alebo spájanie*
- Prevádzková fáza
- Príprava procesu dodania (zásielky)
- Manipulácia na konci životnosti

*vzťahuje sa len na špecifické fázy životného cyklu tachografu (pozri dodatok 10 prílohy 1B k ES č. 1360/2002 - všeobecné bezpečnostné zámery).

Odpady a šrot sa môžu objaviť vo všetkých segmentoch a mali by sa považovať za aktíva. Je potrebné zohľadniť prípravu procesu dodávky (Shipment).

Dôležité aktíva okrem TOE alebo jeho častí sú zvyčajne:

- Zabezpečenie: kontrola prístupu a poplašný systém, kľúče, prístupové kódy.
- Relevantné informácie pre znalosť TOE: špecifikácie, konštrukčná dokumentácia, usmernenia, zdrojový kód, zobrazenie integrovaného a vstavaného softvéru, výsledky penetračných testov.
- Citlivé údaje používané vo fáze vývoja TOE: kľúče, heslá, profil pamäte, dôkazy o integrite.
- Informácie: databázy, dátové súbory, zmluvy, systémová dokumentácia, informácie o výskume a vývoji, archivované informácie, údaje týkajúce sa výroby.
- Softvér: Softvér: nástroje pre výskum a vývoj, aplikácie, systémový softvér, vývojové nástroje, systémy CM.
- Fyzické aktíva: počítačové vybavenie, komunikačné vybavenie, vymeniteľné médiá.
- Služby: počítačové a komunikačné služby, všeobecné služby (energia, klimatizácia, osvetlenie), skladovanie a preprava

Inventarizácia aktív zahŕňa:

- Typ aktív
- Typ ochrany (dôvernosť, integrita, autentickosť, ...)
- Formát
- Umiestnenie
- Záložné informácie
- Informácie o licencii
- Úroveň ochrany, kritickosť

Vlastník aktív je zodpovedný za:

- Zabezpečenie, aby informácie a aktíva súvisiace so spracovateľskými zariadeniami boli vhodne utajené;
- Definovanie a pravidelné prehodnocovanie obmedzení prístupu a klasifikácií s prihliadnutím na platné zásady kontroly.

Vlastníctvo sa prideľuje na:

- Všetky obchodné procesy
- Definované súbory činností
- Aplikácie
- Všetky definované súbory údajov
- Fyzické aktíva (priestory, HW, siete atď.)

Všetky informácie o aktívach sa uchovávajú v príslušných databázach.

9.1.3 Klasifikácia informácií, údajov a materiálov

Cieľ

Aktíva majú primeranú úroveň ochrany v súlade s jeho klasifikáciou.

Zásady

Vývojár musí mať klasifikačnú politiku.

Vývojár musí mať vopred definované postupy označovania a manipulácie pre všetky používané kombinácie definovaných úrovní a informácií, údajov a materiálov zavedené v súlade s klasifikačnou schémou prijatou organizáciou.

Bezpečnostné opatrenia

Aktíva by mali byť klasifikované podľa vhodnej úrovne bezpečnosti z hľadiska ich kritickosti pre organizáciu vývojára a najmä pre plánovanú oblasť použitia každého príslušného TOE.

Klasifikácia sa týka informácií, údajov a materiálov v akejkoľvek forme:

- tlačené dokumenty, napr. dokumenty, poznámky, prezentácie, návrhy
- Elektronické údaje, napr. súbory, e-maily, softvér, vývojové nástroje, systémy CM, siete
- TOE a komponenty (masky/mriežka, wafer, matrice, čipy/moduly, vložky, karty, demonštrátory, vzorky, softvér atď.)
- Klasifikačná schéma musí zodpovedať klasifikácii uvedenej v CEM AVA, odsek 1975:
- Verejné informácie týkajúce sa TOE (napr. získané z internetu);
- Obmedzené informácie týkajúce sa TOE (napr. poznatky, ktoré sú kontrolované v rámci vývojárskej organizácie a zdieľané s inými organizáciami na základe dohody o mlčanlivosti);
- citlivé informácie o TOE (napr. znalosti, ktoré sú zdieľané medzi jednotlivými tímami v rámci vývojárskej organizácie a prístup k nim majú len členovia týchto tímov);
- Kritické informácie o TOE (napr. poznatky, ktoré sú známe len niekoľkým jednotlivcom, prístup k nim je veľmi prísne kontrolovaný na základe prísnej potreby vedieť a individuálneho záväzku);
- Veľmi kritický návrh hardvéru: Návrh moderných integrovaných obvodov zahŕňa nielen obrovské databázy údajov, ale aj sofistikované nástroje na mieru. Prístup k užitočným údajom si preto vyžaduje obrovské a časovo náročné úsilie, ktoré by spôsobilo, že odhalenie by bolo pravdepodobné aj
  s podporou insidera. Ak je útok založený na takýchto znalostiach, je potrebné zohľadniť novú úroveň "veľmi kritického návrhu". O tom, či sa poznatky nedajú získať iným spôsobom, sa musí rozhodnúť v každom jednotlivom prípade.

Klasifikácia by mala byť v súlade s faktorom "znalosť TOE", ktorý sa používa na výpočet potenciálu útoku v prílohe 7, Uplatnenie potenciálu útoku na smart karty.

Ku každému aktívu by mala byť priradená úroveň ochrany v súlade s politikou klasifikácie investora.

Postupy označovania a manipulácie s informáciami, údajmi a materiálom by mali zahŕňať okrem iného predpisy týkajúce sa:

- Vytváranie, označovanie, vydávanie
- Distribúcia
- Odosielanie / prenos
- Uchovávanie / skladovanie
- Likvidácia / zničenie / vymazanie

Pravidlá označovania a manipulácie by sa mali prísne dodržiavať.

Ak sa vyžaduje zachovanie dôvernosti, hotové produkty, polotovary, vyradený materiál alebo jeho časti, ktoré obsahujú TOE alebo jeho časti a ktoré už nie sú potrebné, sa zničia tak, aby ich zvyšky nebolo možné použiť žiadnym významným spôsobom, ktorý by mohol ovplyvniť dôvernosť TOE

Prístup k utajovaným skutočnostiam, t. j. utajovaným skutočnostiam označeným ako "citlivé" alebo "kritické", by sa mal udeľovať len na základe zásady "potrebujem vedieť".

Ak sa vyžaduje vysoká úroveň bezpečnosti obzvlášť kritického materiálu alebo operácie, napr. v prípade klasifikácie "kritický" alebo "alebo veľmi kritický", malo by sa ako kontrolný mechanizmus uplatňovať pravidlo dvoch ľudí ("zásada štyroch očí"). Podľa tohto pravidla si všetky prístupy a činnosti vyžadujú neustálu prítomnosť dvoch oprávnených osôb.

Informácie, údaje a materiál, ktoré sa považujú za citlivé, kritické alebo veľmi kritické, musia byť chránené v každom čase.

Procesy ničenia by mali byť navrhnuté tak, aby zabezpečili úplnú vysledovateľnosť každého kusu akejkoľvek hmotnej formy TOE alebo jeho častí.

Príklady

Typická klasifikačná schéma používa najmenej štyri úrovne utajenia, napr:

- otvorené, verejné
- na interné použitie, chránené spoločnosťou
- dôverné, na základe NDA
- prísne dôverné, firemné tajomstvo, prísne tajné

Dôverné elektronické informácie sú:

- distribuované len určitej skupine ľudí;
- prenášané elektronicky s vhodným koncovým šifrovaním (napr. v roku 2012 sa v nemeckých štatistických údajoch vyžaduje aspoň 80 bitov entropie, t. j. 256-bitový symetrický alebo 2048-bitový asymetrický kľúč RSA);
- uložené ako zašifrovaný súbor, v zabezpečenom kontajneri alebo v oddelenej sieti;
- vymazané pomocou nástroja na vymazávanie s použitím aspoň 1 prechodu s náhodným vzorom údajov.

Proces zničenia:

- Wafer, jednotlivé matrice a balené triesky sa drvia vo valcovni tak, že každá hrana každej matrice sa reže trikrát.
- Masky/mriežka sa opätovne leptajú, aby sa odstránil vzor, alebo sa drvia vo valcovni.
- Proces ničenia prejavov TOE sa zaznamenáva na kamerový záznam.
- Dôverná a prísne dôverná dokumentácia TOE na papieri alebo optických diskoch sa skartuje minimálne podľa normy DIN 66399, bezpečnostná trieda 3:
  - Trieda papiera P6 (max. pásy 0,78 mm x 11 mm)
  - Optické disky triedy O6 (max. zvyšková plocha 0,5 mm²)
  - Magnetické disky triedy T6 (max. 10 mm²)
  - Pevné disky triedy H6 (max. 10 mm²)
  - Elektronické disky (pamäťové karty, SSD) triedy E6 (max. 1 mm²)
- Súbory na prepisovateľných nosičoch údajov (HDD, SSD, USB kľúče) sa vymažú podľa US DoD 5220.22-M alebo sa zničia, ako je opísané vyššie.

9.1.4 Pravidlá na zachovanie integrity a autentickosti aktív

Cieľ

Aktíva musia byť chránené pred zmenou alebo neoprávnenou modifikáciou.

Zásady

Investor musí mať vopred definované postupy nakladania so všetkými dôležitými aktívami v súlade s potrebami ochrany. Prístup k riadeniu konfigurácie a jeho zavedenie musí byť definované v politike.

Vždy, keď sa časti TOE importujú z externých zdrojov, mali by sa v postupoch importu definovať spôsoby, akými vývojár zabezpečuje integritu a autentickosť importovaných častí.

Bezpečnostné opatrenia

Podľa ALC_CMC vhodný systém riadenia konfigurácie identifikuje a dokumentuje funkčné a fyzické charakteristiky TOE a jeho častí, kontroluje zmeny týchto charakteristík, zaznamenáva a oznamuje spracovanie zmien a stav implementácie a overuje súlad so špecifikovanými požiadavkami spôsobom relevantným pre rôzne časti životného cyklu. Systém riadenia konfigurácie zabezpečuje integritu TOE od počiatočných fáz návrhu až po všetky následné údržbové činnosti, aby bol TOE správny a úplný pred jeho odoslaním spotrebiteľovi a aby sa zabránilo neoprávnenej modifikácii, pridaniu alebo vymazaniu konfiguračných položiek TOE. (Podrobné požiadavky na systémy CM sú definované v CC časť 3, ALC.)

Vo fáze návrhu TOE sa v konfiguračnom zozname jasne definujú všetky konfiguračné položky pre konkrétny produkt spolu s presnou verziou každej položky relevantnej pre konkrétnu verziu TOE a jeho častí, čo umožní rozlíšiť položky patriace k rôznym verziám produktu.

Počas výroby systém CM zabezpečuje, aby sa používali len plánované postupy a receptúry, aby sa používali v správnom poradí a aby sa všetky výrobné kroky zdokumentovali s cieľom uľahčiť úplnú vysledovateľnosť.

Ak nie je možné uplatniť technické opatrenia, mali by sa zaviesť organizačné opatrenia, napr. zásada štyroch očí.

V prípade prenášaných údajov by sa mali zaviesť detekčné opatrenia, napr. kontrolný súčet, hash hodnota, podpis.

Ak importované časti pochádzajú z iných bezpečných rozvojových prostredí, počas prenosu sa chráni integrita, autentickosť a v prípade potreby aj dôvernosť. Import z nedôveryhodných zdrojov by mal zahŕňať kontrolu importovaných častí, ak modifikácia týchto častí môže potenciálne ohroziť integritu TOE. To sa týka najmä prenosu kódu ROM, obsahu EEPROM alebo softvéru súvisiaceho s TOE.

Príklady

Pre technickú doménu týkajúcu sa smart kariet a podobných zariadení: bezpečnostné opatrenia na prenos sa vzťahujú najmä na prenos kódu ROM alebo softvéru súvisiaceho s obsahom EEPROM alebo softvéru súvisiaceho s TOE.

Pre technickú doménu týkajúcu sa hardvérových zariadení s bezpečnostnými skrinkami: sú definované fyzické a logické bezpečnostné opatrenia. Prenos logických bezpečnostných opatrení sa vzťahuje najmä na prenos počiatočného firmvéru a softvéru, načítanie kryptografických kľúčov, personalizáciu a doplnkový softvér súvisiaci s TOE. Prenos fyzických bezpečnostných opatrení sa vzťahuje najmä na inicializáciu alebo Inštaláciu bezpečnostných prvkov HW a udržiavanie vonkajšieho krytu mimo viditeľného poškodenia až do dodania (príklad: manipulačné stopy).

9.2 Bezpečnosť ľudských zdrojov

9.2.1 Celkový cieľ

Celkovým cieľom je znížiť riziko krádeže, podvodu alebo zneužitia zariadení tým, že sa zabezpečí, aby zamestnanci, dodávatelia, konzultanti, študenti a používatelia z radov tretích strán rozumeli svojim povinnostiam a aby boli vhodní pre úlohy, ktoré sa im prisudzujú.

9.2.2 Pred nástupom do zamestnania

Cieľ

Vývojár udelí prístup k aktívam len dôveryhodným osobám.

Proces prijímania zamestnancov a uzatvárania zmlúv musí zabezpečiť správny výber členov tímu.

Zásady

DSD musí obsahovať zásady prijímania a zapracovávania zamestnancov, ktoré zabezpečia starostlivý výber dôveryhodných zamestnancov.

Bezpečnostné opatrenia

Overovanie minulosti všetkých uchádzačov o zamestnanie, dodávateľov a používateľov z radov tretích strán by sa malo vykonávať v súlade s príslušnými miestnymi zákonmi, predpismi a etikou a malo by byť primerané obchodným požiadavkám, klasifikácii informácií a materiálov, ku ktorým sa má pristupovať, a vnímaným rizikám.

Členovia tímu v rámci svojich zmluvných povinností odsúhlasia a podpíšu podmienky svojej pracovnej zmluvy, v ktorej sa uvedú ich povinnosti a povinnosti organizácie v oblasti bezpečnosti.

Zmluvy so všetkými zamestnancami (stálymi, dočasnými, subdodávateľmi, študentmi atď.) musia obsahovať doložku o zachovaní dôvernosti, ktorá zostáva v platnosti aj po skončení platnosti zmluvy; používatelia z radov tretích strán musia podpísať dohodu o mlčanlivosti.

Rovnaké bezpečnostné požiadavky sa vzťahujú aj na zamestnancov, ktorí sa presúvajú z iných oblastí v rámci organizácie vývojárov.

Príklady

Rešpektujúc predpisy o ochrane osobných údajov, vývojár vynakladá primerané úsilie na získanie dôvery v bezúhonnosť zamestnancov prostredníctvom:

- dôkladná kontrola úplnosti, presvedčivosti a autentickosť žiadostí,
- kontrola uvedených referencií,
- kontrola registra trestov ("Clearance Certificate", "Criminal Records Bureau check", "Výpis z registra trestov", "Potvrdenie o policajnej previerke" atď.).

9.2.3 Počas zamestnania

Cieľ

Všetci členovia tímu si musia byť vedomí hrozieb a problémov v oblasti informačnej bezpečnosti a poznať svoje povinnosti a

záväzky. Musia dodržiavať pravidlá a musia byť vybavení tak, aby pri svojej bežnej práci podporovali bezpečnostné politiky organizácie a znižovali riziko ľudskej chyby.

Zásady

Vývojár musí mať k dispozícii dokumenty definujúce bezpečnostné úlohy a zodpovednosti zamestnancov, dodávateľov a používateľov tretích strán v súlade s bezpečnostnou politikou organizácie (napr. v opisoch pracovných miest, projektových plánoch, zmluvách atď.).

Prístup k pravidelnej odbornej príprave by mal byť definovaný v politike.

V politike by sa mali vymedziť monitorovacie opatrenia vykonávané s cieľom odhaliť neregulárne správanie v súlade s miestnymi právnymi predpismi.

Bezpečnostné opatrenia

Vedenie vyžaduje, aby členovia tímu uplatňovali bezpečnosť v súlade so zavedenými zásadami a postupmi organizácie.

Všetci zamestnanci organizácie a v prípade potreby aj dodávatelia a používatelia z radov tretích strán by mali absolvovať príslušné školenie o informovanosti a pravidelné aktualizácie organizačných politík

a postupov, ktoré sú relevantné pre ich pracovnú funkciu. Môže to byť osobné alebo online školenie. O školeniach by sa mali viesť záznamy vrátane dátumu, účasti a obsahu.

S cieľom identifikovať porušenia bezpečnosti by sa mali analyzovať monitorovacie záznamy o bezpečnostných oblastiach a zabezpečených sieťach, napr. logovacie súbory, v súlade s miestnymi právnymi predpismi. Pre zamestnancov, ktorí sa dopustili porušenia bezpečnosti, by mal existovať formálny disciplinárny postup. Porušenie bezpečnostných pravidiel môže byť potrestané disciplinárnymi opatreniami v závislosti od povahy a závažnosti porušenia a jeho vplyvu na dôvernosť a integritu TOE, od toho, či ide o prvé alebo opakované porušenie, od toho, či porušiteľ bol alebo nebol riadne vyškolený, od príslušných právnych predpisov, obchodných zmlúv a ďalších faktorov podľa potreby.

Úvodný a pravidelný (ročný) program bezpečnostného školenia by mal členov vývojového tímu oboznámiť s ich povinnosťami, napr. zaobchádzanie s dokumentmi a informáciami, správanie na verejnosti, a povzbudiť ich k aktívnemu konaniu v prípade výskytu problémov. V rámci školení o informovanosti by sa mali riešiť zmeny v procesoch, poznatky z bezpečnostných incidentov a auditov a odpovede na často kladené otázky.

Príklady

Vedenie vývojára zabezpečuje, aby členovia tímu:

- boli riadne poučení o svojich bezpečnostných úlohách a povinnostiach pred udelením prístupu do citlivých oblastí, k informáciám alebo informačným systémom;
- majú k dispozícii usmernenia, v ktorých sú uvedené bezpečnostné očakávania týkajúce sa ich úlohy v organizácii;
- dosiahnuť úroveň povedomia o bezpečnosti, ktorá zodpovedá ich úlohám a povinnostiam v organizácii;
- dodržiavať pracovné podmienky, ktoré zahŕňajú politiku organizácie v oblasti informačnej bezpečnosti a vhodné pracovné metódy;
- naďalej mať primerané zručnosti a kvalifikáciu;
- dodržiavať pravidlá;
- ísť príkladom.

Disciplinárny proces sa používa ako odstrašujúci prostriedok, ktorý má zabrániť členom tímu porušovať organizačné bezpečnostné zásady a postupy a akékoľvek iné porušenia bezpečnosti.

9.2.4 Ukončenie alebo zmena zamestnania

Cieľ

Členovia tímu opúšťajú vývojára (ukončenie zmluvy alebo zmena zamestnania) riadne a kontrolovane spôsobom s cieľom zachovať integritu a/alebo dôvernosť aktív a/alebo informácií.

Zásady

Vývojár musí mať vhodné postupy pre ukončenie pracovného pomeru a zmenu pracovného miesta vrátane zrušenia prístupových práv.

Bezpečnostné opatrenia

Zodpovednosť za vykonanie ukončenia pracovného pomeru alebo zmeny pracovného pomeru musí byť jasne vymedzená a pridelená. To sa vzťahuje aj na zmluvy s používateľmi - tretími stranami.

Všetci členovia tímu sú povinní po ukončení pracovnej zmluvy alebo dohody vrátiť všetky aktíva vývojára, ktoré majú v držbe. To isté platí, keď opustia organizáciu vývojára z dôvodu zmeny pracovného zaradenia.

Prístupové práva (fyzické a logické) všetkých členov tímu k zariadeniam vývojára sa bezodkladne zrušia, ak už nie sú potrebné, najmä po skončení ich pracovného pomeru, zmluvy alebo dohody, alebo sa upravia pri zmene.

Proces zmeny/ukončenia pracovného pomeru by mal byť podporený kontrolným zoznamom pre zamestnancov, ktorí končia pracovný pomer, aby sa zabezpečilo splnenie všetkých príslušných úloh,

napr. vrátenie majetku spoločnosti, zrušenie prístupových práv.

V prípade pozastavenia alebo prepustenia z disciplinárnych dôvodov sa prístupové práva okamžite zrušia. Informuje sa bezpečnostný manažér.

V prípade potreby by mali byť členovia tímu informovaní o zmenených prístupových právach.

9.3 Fyzická a environmentálna bezpečnosť

9.3.1 Celkový cieľ

Fyzická bezpečnosť musí zabrániť neoprávnenému fyzickému prístupu do priestorov organizácie, zabezpečených oblastí, priestorov na dodávanie a nakladanie, aktív a informácií, ktoré môžu narušiť integritu alebo - ak sa to vyžaduje - dôvernosť TOE.

Integrita a - v prípade bezpečnostných systémov - dostupnosť (pozri aj bod 9.8) bezpečnostného vybavenia sa zabezpečuje tak, aby sa zabránilo strate, poškodeniu, krádeži, ohrozeniu alebo strate integrity aktív a bezpečnostných kontrol.

9.3.2 Fyzický bezpečnostný perimeter

Cieľ

Oblasti vývoja, v ktorých by mohlo dôjsť k narušeniu integrity a/alebo dôvernosti TOE alebo jeho častí, musia byť riadne zaistené.

Ochrana priestorov musí mať aspoň dve obranné línie, detekčnú vrstvu a zastavovaciu vrstvu. Tieto vrstvy musia oddeľovať oprávnené osoby od neoprávnených vrátane zamestnancov.

Zásady

Bezpečnostné politiky definujú koncepciu dvojvrstvovej bezpečnosti a podrobne opisujú zosúladenú funkciu týchto dvoch vrstiev.

Bezpečnostné opatrenia

Vrstva zastavenia a detekčná vrstva sa implementujú zosúladeným a zmysluplným spôsobom. Mali by sa poskytnúť dôkazy, že hodnota času odolnosti brzdnej vrstvy presahuje čas reakcie podporných síl.

Všetky otvory smerom k zabezpečenej rozvojovej oblasti (napr. klimatizačné a káblové kanály) musia byť chránené, aby sa účinne zabránilo vniknutiu.

Ak sa budovy nevyužívajú výlučne na činnosti vývojárov, napr. sú zdieľané s inými používateľmi z tej istej organizácie (podporné funkcie, výroba, výskum a vývoj), vrstvy musia oddeľovať rôzne činnosti.

V prípade, že sa nepracuje s fyzickým prejavom TOE alebo jeho častí a existuje výlučne logický prístup k elektronickým údajom, môže byť stop vrstva aj logická.

V prípade, že fyzický prejav TOE alebo jeho častí má mechanizmus "vlastnej ochrany", môže prispieť k zastaveniu alebo sa môže považovať za zastavovaciu vrstvu. Podrobnosti sú uvedené v príslušnej prílohe.

Príklady

V typickom prípade sa priestory nachádzajú na oplotenom pozemku. Plot je chránený snímačmi (vibračnými, napr. Perifone; pohybovými, napr. digitálny CCTV). Ak areál nemusí byť oplotený, môže sa nasadiť infračervená clona alebo sa vonkajší plášť budovy monitoruje digitálnou CCTV s detekciou pohybu ("Telemat").

Detekčná vrstva pozostáva aspoň z jedného z nasledujúcich prvkov:

- Plot so senzorom (vibračným, ultrazvukovým, pohybovým atď.)
- IR clona
- Digitálny CCTV s detekciou pohybu

- Stena s poplašnou tapisériou alebo vibračným senzorom
- Strážne stanovište 24/7

Stop vrstva je konštruktívne opatrenie, ktoré potrebuje čas na prekonanie:

- Betónové alebo tehlové kamenné steny, strop a podlaha;
- konštrukcia suchého muriva vynútená s vnútornou kovovou mriežkou (priemer > 8 mm, vzdialenosť mriežky < 100 mm), s oceľovým plechom (hrúbka > 3 mm) alebo s poplašnou tapisériou;
- okná v zádržnej vrstve sú buď chránené kovovými tyčami (priemer > 8 mm), alebo sú vyrobené so sklom proti vlámaniu;
- dverné kovanie musí byť správne nainštalované, uzamknuté dverné lamely upevnené na podlahe a strope.

Vývojové siete zabezpečené silnými prístupovými údajmi a bez údajov súvisiacich s TOE na miestnych dátových nosičoch sa považujú za logickú stop vrstvu.

Riadené dvere sú pevné (vrátane zárubní), zatvárajú sa automaticky a sú monitorované magnetickými kontaktmi a kamerovým systémom.

Okná sú zabezpečené neodnímateľnou kovovou mriežkou alebo magnetickými kontaktmi a snímačmi rozbitia skla.

Vzduchotechnika, káblové kanály atď. sú chránené zváranou kovovou mriežkou.

9.3.3 Fyzické kontroly vstupu

Cieľ

Zabezpečené priestory musia byť chránené vhodnými vstupnými kontrolami, aby sa zabezpečilo, že prístup bude umožnený len oprávneným pracovníkom.

Zásady

Musí byť zavedená politika riadenia prístupu vrátane predpisov pre návštevníkov a dodávateľov. Prístup sa udeľuje len na základe potreby vedieť.

V politike sa vymedzia pravidlá prístupu pre obslužné funkcie, napr. upratovanie, správu zariadení, upratovací personál.

V prípade potreby sa v zásadách podrobne uvedú prístupové práva pre úradníkov a podporné sily, napr. hasičov.

Bezpečnostné opatrenia

Žiadosti o prístup sa predkladajú písomne alebo prostredníctvom elektronického systému pracovného toku.

Musí byť zavedený proces, ktorý zabezpečí, že prístupové práva sa môžu udeliť len po schválení zodpovednými osobami, napr. manažérom žiadateľa, vlastníkom oblasti a bezpečnostným manažérom.

Oddelenie povinností by malo zabezpečiť, aby bolo nastavenie prístupových práv v systéme riadenia prístupu oddelené od výroby a vydávania preukazov.

Systém kontroly prístupu by mal byť odolný voči neoprávnenej manipulácii.

V závislosti od veľkosti a charakteru pracoviska a súvisiacich rizík by sa malo zabrániť "Tailgatingu" technickými alebo organizačnými opatreniami.

V oblastiach s vysokým stupňom zabezpečenia by sa mala zaviesť silná autentizácia.

Systém riadenia prístupu zabezpečuje sledovateľnosť. Všetky pokusy o prístup sa zaznamenávajú a neoprávnené pokusy o prístup by sa mali analyzovať a v prípade incidentu by sa mali uplatniť príslušné opatrenia.

Ak sa vyžaduje úplná vysledovateľnosť (v závislosti od povahy činností), zavedie sa automatizovaný

manžetový systém so silnou autentizácia.

V prípade, že sa na prístup do rozvojovej oblasti používajú fyzické kľúče (t. j. ak je kľúč jediným opatrením na kontrolu prístupu), táto oblasť musí mať uzamykací systém nezávislý od ostatných oblastí. Takéto kľúče sa musia uchovávať na bezpečnom mieste (napr. skrinky na kľúče, trezor), pričom prístup k nim majú len oprávnené osoby. Každé odobratie kľúča sa musí zaznamenať.

Príklady

V typickom nastavení je prístup do budovy kontrolovaný pomocou elektronického preukazu.

Celý systém riadenia prístupu s preukazom (napr. smart kartou), čítačkou a základným systémom je odolný voči neoprávnenej manipulácii. Beží na oddelenej, zabezpečenej sieti. Vzájomná autentizácia odznaku a čítačky zabraňuje neoprávnenému čítaniu prístupových údajov. Komunikácia medzi jednotlivými zložkami systému riadenia prístupu je zabezpečená vhodným protokolom (napr. OSDP V2). Šifrovanie a správa kľúčov sú zabezpečené bezpečným prístupovým modulom (SAM).

Oblasti s vysokým stupňom zabezpečenia (napr. laboratórium, dátové centrum, miestnosti bezpečnostnej kontroly) majú silnú autentizáciu, napr. odznak s kódom PIN alebo biometriu.

Tailgatingu sa zabraňuje turniketmi, a to buď turniketmi s plnou výškou, alebo štandardnými turniketmi monitorovanými strážou.

Prístup do oblastí s vysokou úrovňou zabezpečenia (napr. projektovanie, bezpečnostné laboratórium) je kontrolovaný automatickými mantinelmi so silnou autentizáciou.

9.3.4 Zabezpečenie kancelárií, miestností a zariadení

Cieľ

Fyzická bezpečnosť kancelárií, miestností a zariadení musí byť chránená pred neoprávneným prístupom.

Každé narušenie sa musí zistiť okamžite.

Zásady

V politike sa podrobne uvedú opatrenia zavedené na zabezpečenie odhaľovania a prevencie neoprávneného prístupu do kancelárií, miestností a zariadení. Zahŕňa jasné bezpečnostné postupy a bezpečnostné predpisy, ako aj - v prípade potreby - outsourcing.

Bezpečnostné opatrenia

Navrhnú a použijú sa systémy detekcie narušenia a poplachové systémy. Rozvojový priestor by mal byť zabezpečený alarmom a uzamknutý, keď je bez dozoru.

Dvere s kontrolovaným prístupom a núdzové východy by mali byť monitorované magnetickými kontaktmi a kamerovým systémom a miestnosti s obmedzeným prístupom by mali byť monitorované pomocou detekcie pohybu.

Ľahko prístupné okná by mali byť chránené proti vniknutiu.

Detekčné a monitorovacie systémy by mali byť napojené na bezpečnostné centrum s nepretržitou prevádzkou. Bezpečnostné centrum musí mať primeranú úroveň záruky. Pripojenie všetkých bezpečnostných zariadení (napr. detekcia vlámania, kamerový systém) k bezpečnostnému centru musí byť chránené proti neoprávnenej manipulácii. Všetky procesy súvisiace s bezpečnosťou sa musia kontrolovať.

V bezpečnostnom centre sa nachádzajú primárne systémy monitorovania CCTV, narušenia, požiaru, kontroly alarmu a riadenia prístupu:

- Nasledujúce procesy patria medzi príslušné bezpečnostné procesy:
  - Správa riadenia prístupu (práva na zmenu prístupu k odznakom alebo vytváranie odznakov)
  - Aktivácia a deaktivácia bezpečnostného systému

- Za relevantné bezpečnostné procesy sa nepovažujú tieto procesy
  - Prístup k CCTV len na zobrazenie
  - Reagovať len na bezpečnostné alarmy s eskaláciou do spoločnosti

Príklady

Okná na prízemí alebo inde, kam sa dá dosiahnuť z tribúny (strecha, balkón atď.) do vzdialenosti 2,5 m, sa považujú za ľahko prístupné.

9.3.5 Ochrana pred vonkajšími a environmentálnymi hrozbami

Cieľ

Bezpečnostné oblasti musia zostať v bezpečnom stave a chrániť TOE aj v prípade prírodnej katastrofy alebo katastrofy spôsobenej človekom.

Zásady

Vyžaduje sa politika prevencie a obnovy po havárii s podrobným opisom opatrení zavedených na ochranu TOE.

Bezpečnostné opatrenia

Vhodná fyzická ochrana proti škodám spôsobeným požiarom, povodňami a inými formami prírodných alebo človekom spôsobených katastrof by sa mala navrhnúť a uplatňovať na základe posudzovania rizika. Bezpečnostné systémy, ako je kontrola prístupu, kamerový systém atď., musia fungovať aj v prípade prírodnej alebo človekom spôsobenej katastrofy. Táto požiadavka sa vzťahuje aj na protokolovacie
a záložné systémy.

9.3.6 Práca v zabezpečených oblastiach

Cieľ

Navrhne sa a uplatní fyzická ochrana a usmernenia pre prácu v zabezpečených oblastiach. Personál musí si uvedomovať, že informácie sa môžu zdieľať len na základe zásady "need-to-know".

Zásady

Vypracuje sa, implementuje a udržiava politika kontroly prístupu založená na princípe "potreba vedieť".

Bezpečnostné opatrenia

Pravidlá kontroly prístupu a práva každého zamestnanca alebo návštevníka musia byť jasne uvedené v politike kontroly prístupu. Kontroly prístupu sú logické aj fyzické. Používatelia a poskytovatelia služieb musia dostať jasné vyhlásenie o obchodných požiadavkách, ktoré sa majú splniť prostredníctvom kontroly prístupu.

Osoby z externých strán (napr. zákazníci, vývojoví partneri, výrobní partneri, upratovačky, predajcovia, dodávatelia, dopravcovia) nesmú pracovať v bezpečnostných oblastiach bez dohľadu schválených interných pracovníkov (napr. hostiteľa, majiteľa oblasti, strážnika). Toto pravidlo sa nevzťahuje na externistov, ktorí pracujú ako členovia tímu a podliehajú rovnakým bezpečnostným predpisom ako internisti.

Voľné bezpečnostné priestory musia byť fyzicky chránené, napr. pomocou systémov detekcie vlámania a požiarneho poplachu, a pravidelne kontrolované.

Neoprávnené používanie fotografických a videokamier alebo zvukových nahrávacích zariadení je zakázané.

9.3.7 Verejný prístup, dodávky a nakladacie plochy

Cieľ

Prístupové miesta, ako sú miesta dodávok a nakladania a iné miesta, kde môžu neoprávnené osoby vstúpiť do priestorov, musia byť kontrolované a izolované od spracovateľských zariadení vývojára, aby sa zabránilo neoprávnenému prístupu.

Návštevníci nesmú neúmyselne získať prístup do zakázaných oblastí alebo informácií alebo do nich nahliadnuť.

Komponenty TOE musia byť chránené proti neoprávnenej manipulácii alebo krádeži počas prepravy medzi fyzicky oddelenými zabezpečenými oblasťami.

Zásady

V bezpečnostnej politike sa zohľadňuje, že pri navrhovaní a rozmiestňovaní lokalít a priestorov by sa malo zabrániť vzniku oblastí s vysokou mierou bezpečnosti v blízkosti verejných priestorov.

Bezpečnostná politika zahŕňa návštevný poriadok, ktorý sa musí vypracovať, zdokumentovať a preskúmať na základe bezpečnostných požiadaviek na prístup.

V bezpečnostnej politike sa (ak je to vhodné) definujú opatrenia na zabezpečenie ochrany komponentov TOE pred neoprávnenou manipuláciou alebo krádežou počas prepravy medzi fyzicky oddelenými zabezpečenými oblasťami. Opatrenia počas tranzitu musia zodpovedať klasifikácii dôvernosti a integrity.

Bezpečnostné opatrenia

Návštevníci

Návštevníci majú do rozvojového prostredia len vopred definovaný a kontrolovaný prístup. Trasy a chodníky určené pre návštevníkov by mali byť navrhnuté tak, aby sa zabezpečilo, že návštevníci neuvidia zakázané oblasti alebo informácie neúmyselne. Postupy vzťahujúce sa na návštevníkov by mali zahŕňať:

- Zdokumentovaný proces podávania žiadostí o návštevy, ktorý definuje, kto je oprávnený prijímať návštevy a kto je oprávnený ich schvaľovať.
- Registračný postup, ktorý zabezpečuje overenie totožnosti návštevníka na základe oficiálneho dokladu vydaného vládou (preukaz totožnosti s fotografiou). Zaznamenávajú sa informácie o návštevníkovi, kontaktná osoba v rozvojovom prostredí, čas príchodu a odchodu a dôvod návštevy.
- Návštevníci majú počas celej návštevy preukaz návštevníka.
- Návštevníci sú vo rozvojovom prostredí vždy sprevádzaní buď osobou z rozvojového prostredia, alebo bezpečnostným personálom.

Dodanie a preprava

Priestory pre prichádzajúce a odchádzajúce zásielky by mali byť oddelené; oddelenie môže byť fyzické alebo dočasné.

Dodávacie a expedičné priestory musia byť navrhnuté tak, aby žiadny personál dopravcu nemohol získať prístup do iných častí priestorov. Vonkajšie dvere týchto priestorov by mali byť pri otvorení vnútorných dverí zabezpečené (blokovanie).

Vodiči a nákladné vozidlá dopravcov by mali byť uvedení s menom, fotografiou, podpisom, značkou a evidenčným číslom. Prístup do priestorov môžu mať len nákladné vozidlá a vodiči uvedení na zozname.

Dodávky do priestorov vývojára by mali byť oznámené. Dopravca by nemal mať prístup do bezpečnostných priestorov vývojára vrátane expedičného priestoru a skladu, ale mal by sa zdržiavať v priestore dodávok a nakladania.

Dodávkový a nakladací priestor musí byť monitorovaný kamerovým systémom. Záznamy musia poskytovať jasné zábery, ktoré umožnia investorovi identifikovať akékoľvek neúmyselné vykladanie a nakladanie.

Prichádzajúci materiál sa pri vstupe zaeviduje a pred dodaním na miesto použitia sa skontroluje z hľadiska možných hrozieb.

Doprava

Neexistujú žiadne osobitné požiadavky na fyzický prenos materiálov v rámci fyzicky zabezpečenej oblasti okrem toho, že prenos sa musí zaznamenať, aby sa zabezpečila úplná vysledovateľnosť.

Kontroluje sa celý prepravný reťazec od oblasti počiatočného vývoja až po odoslanie TOE zákazníkovi. Preprava sa monitoruje z hľadiska porušenia bezpečnosti a na všetky incidenty sa musí okamžite reagovať a konať.

V určitých fázach životného cyklu môže byť TOE samoochranný podľa riadku 136 časti 1 CC. V takom prípade sa ochrana pri preprave nevyžaduje, ak sú zavedené bezpečnostné opatrenia umožňujúce príjemcovi nepochybne identifikovať pôvod zásielky.

Komponenty TOE musia byť chránené proti neoprávnenej manipulácii alebo krádeži počas prepravy medzi fyzicky oddelenými zabezpečenými oblasťami. Ochranný mechanizmus musí príjemcovi umožniť zistiť, či došlo k neoprávnenej manipulácii alebo krádeži.

Príjemcovi by sa mali poskytnúť všetky informácie potrebné na overenie neporušenosti a autentickosti zásielky. Mali by sa uviesť tieto informácie:

- Počet políčok
- Číslo(-á) plomby prepravného(-ých) boxu(-ov)
- Počet zabalených kusov
- Trasa a harmonogram
- Meno vodiča, evidenčné číslo nákladného vozidla

Aby sa zabránilo útokom, informácie o preprave by mali byť zašifrované.

Po prijatí príjemca bezodkladne skontroluje zásielku a potvrdí stav neporušenosti a autentickosti. V prípade porušenia celistvosti alebo autentickosti zásielky sa toto potvrdenie uchováva spolu s pôvodným oznámením o preprave.

Príklady

Počas prepravy je TOE prítomný kedykoľvek, okrem času, keď je uzamknutý v lietadle. Pri pozemnej preprave sa uplatňujú tieto pravidlá:

- TOE alebo jeho časti sú zabalené v zapečatených prepravných škatuliach s nepredvídateľným číslom plomby (plomba, olovnica alebo bezpečnostná páska)
- preprava vo vozidle (úžitková dodávka, nákladné vozidlo) s uzamknutým nákladným priestorom.
- prenos z bodu do bodu bez dodatočného užitočného zaťaženia alebo rozbočovača/relácie
- Počas celej prepravy sa uplatňuje pravidlo dvoch osôb a vozidlo nie je nikdy bez dozoru
- doprava je vybavená mobilným telefónom a GPS dohľadom.

9.3.8 Bezpečnosť zariadenia

Cieľ

Zabezpečí sa integrita a - v prípade bezpečnostných systémov - dostupnosť príslušných bezpečnostných zariadení, aby sa zabránilo ich strate,

poškodenie, krádež, ohrozenie alebo strata integrity aktív a bezpečnostných kontrol.

Zásady

Politika definuje manipuláciu a umiestnenie bezpečnostne relevantných zariadení s cieľom chrániť ich pred poruchami, ktoré by mohli ovplyvniť dostupnosť týchto zariadení, a pred ich zachytením alebo

poškodením.

Bezpečnostné opatrenia

Bezpečnostne relevantné zariadenia by mali byť umiestnené alebo chránené tak, aby sa znížili riziká vyplývajúce z environmentálnych hrozieb a nebezpečenstiev a možnosti neoprávneného prístupu.

Bezpečnostné zariadenia musia byť chránené pred výpadkami elektrickej energie a inými poruchami spôsobenými poruchami podporných médií.

Napájacie a telekomunikačné káble prenášajúce citlivé údaje alebo podporujúce informačné služby dôležité z hľadiska bezpečnosti musia byť chránené pred odpočúvaním alebo poškodením.

Zariadenia by sa mali správne udržiavať, aby sa zabezpečila ich trvalá integrita a - v prípade bezpečnostných systémov - dostupnosť.

Bezpečnostné opatrenia by sa mali uplatňovať na zariadenia mimo pracoviska (prenosný počítač, mobilný telefón, vreckové zariadenie, dátový nosič) s prihliadnutím na rôzne riziká práce mimo priestorov vývojára. Používanie takéhoto zariadenia sa musí obmedziť na činnosti, ktoré priamo nesúvisia s TOE, a musí ho schváliť vedenie.

Všetky zariadenia obsahujúce pamäťové médiá sa pred likvidáciou alebo opätovným použitím mimo priestorov investora skontrolujú, aby sa zabezpečilo, že všetky citlivé údaje boli bezpečne odstránené.

Zariadenie, informácie alebo softvér sa nesmú prenášať mimo pracoviska bez predchádzajúceho povolenia.

Príklady

Zariadenia sú umiestnené v priestoroch, ktoré minimalizujú zbytočný prístup do bezpečnostných zón. Je umiestnené tak, aby sa zabránilo neoprávnenému pozorovaniu.

Sieťová kabeláž je chránená pred neoprávneným odpočúvaním alebo poškodením tým, že sa vyhýba trasám vedúcim cez verejné priestory. Vedenie káblov v káblových kanáloch.

Prístup k prepínačom a patch panelom je obmedzený.

Utajované informácie, údaje a materiál sa pred údržbou odstránia. Všetka údržba sa zaznamenáva s uvedením dátumu, času a zúčastnených pracovníkov.

Je definovaný a zavedený postup pre povolenie odvozu majetku spoločnosti mimo pracoviska. Kontroly na mieste s cieľom odhaliť neoprávnené premiestnenie sa vykonávajú v súlade s príslušnými právnymi predpismi a nariadeniami.

9.4 Riadenie komunikácie a prevádzky

9.4.1 Celkový cieľ

Prevádzka a komunikácia súvisiaca s TOE, ako aj s podpornými infraštruktúrami a zdrojmi sa chráni pred vnútornými a vonkajšími hrozbami.

9.4.2 Prevádzkové postupy a zodpovednosti

Cieľ

Operácie súvisiace s TOE musia byť chránené proti neúmyselnému alebo úmyselnému zneužitiu spracovateľských zariadení alebo nesprávne vykonávanie operácií.

Infraštruktúra používaná na ochranu integrity a/alebo dôvernosti TOE musí byť zabezpečená.

Zásady

Prevádzkové postupy sa zdokumentujú, udržiavajú a sprístupnia všetkým používateľom, ktorí ich potrebujú.

Mali by byť zavedené formálne zodpovednosti a postupy riadenia na zabezpečenie uspokojivej kontroly zariadení, softvéru alebo postupov a všetkých súvisiacich zmien.

Postup definuje úroveň oddelenia medzi vývojovým, testovacím a prevádzkovým prostredím a opisuje zavedené kontroly.

Bezpečnostné opatrenia

Vývojár by mal zaviesť primeranú úroveň oddelenia medzi rozvojovým, testovacím a prevádzkovým prostredím.

Správne používanie spracovateľského zariadenia a vykonávanie operácií by mala uľahčovať aktuálna dokumentácia prevádzkových postupov.

Spracovateľské zariadenia by mali podliehať prísnym procesom riadenia zmien; zmeny by malo schvaľovať vedenie. Po vykonaní zmien by sa mal uchovávať denník auditu obsahujúci všetky relevantné informácie.

Používaniu alebo modifikácii aktív bez oprávnenia alebo zistenia by sa malo zabrániť oddelením povinností a oblastí zodpovednosti. Do úvahy by sa mali vziať tieto položky:

- Iniciovanie udalosti by malo byť oddelené od jej autorizácie.
- Pri navrhovaní kontrol by sa mala zohľadniť možnosť tajnej dohody.
- Vždy, keď je ťažké oddeliť, mali by sa zvážiť iné kontrolné mechanizmy, ako je monitorovanie činností, audítorské záznamy a dohľad vedenia.

Príklady

Prevádzkové postupy a zdokumentované postupy pre systémové činnosti sú formálne dokumenty.

K dispozícii sú zdokumentované postupy pre systémové činnosti spojené so zariadeniami na spracovanie informácií a komunikáciu, ako sú postupy spúšťania a vypínania počítačov, zálohovania, údržby zariadení, manipulácie s médiami, riadenia počítačovej miestnosti a manipulácie s poštou a bezpečnosti.

V pracovných postupoch sú uvedené pokyny na podrobné vykonanie každej úlohy.

Kontroly zmien zohľadňujú tieto položky:

- Identifikácia a zaznamenávanie významných zmien;
- Plánovanie a testovanie zmien;
- Posúdenie potenciálnych vplyvov takýchto zmien vrátane vplyvov na bezpečnosť;
- Formálny postup schvaľovania navrhovaných zmien;
- Oznámenie podrobností o zmene všetkým príslušným osobám;
- Záložné postupy vrátane postupov a zodpovedností za prerušenie a obnovu po neúspešných zmenách a nepredvídaných udalostiach.

Prístup do systému kontroly prístupu je oddelený od manipulácie s fyzickými preukazmi, napr. pridelenými personálnym pracovníkom a bezpečnostným pracovníkom.

9.4.3 Riadenie poskytovania služieb treťou stranou

Cieľ

Pri použití služieb tretích strán sa zachováva dôvernosť a/alebo integrita TOE a jeho časti.

Zásady

V politikách riadenia zmlúv a dodávateľov sa vymedzia úlohy a zodpovednosti za riadenie vzťahov s tretími stranami.

Bezpečnostné opatrenia

Zodpovednosť za riadenie vzťahu s treťou stranou by mala byť pridelená určenej osobe alebo tímu pre riadenie služieb.

Zmluvy o poskytovaní služieb a pracovné výkazy by mali prejsť interným schvaľovacím procesom vývojára. Musí byť zapojený bezpečnostný manažér a zohľadnená akákoľvek spätná väzba.

Služby tretích strán by sa mali monitorovať a preskúmavať s cieľom skontrolovať, či sa dodržiavajú bezpečnostné podmienky dohôd a či sa riadne riešia bezpečnostné incidenty a problémy. Správa by sa mala uchovávať ako dôkaz.

9.4.4 Plánovanie a akceptácia systému

Cieľ

Plánovanie systémov minimalizuje riziká zlyhania systému pre všetky systémy podporujúce dôvernosť a/alebo integritu TOE a jeho časti.

Zásady

Definuje sa a zdokumentuje proces plánovania komunikačných a prevádzkových systémov.

Stanovia sa skúšobné postupy a kritériá prijatia pre nové systémy spracovania, modernizácie a nové verzie.

Bezpečnostné opatrenia

Využívanie zdrojov by sa malo monitorovať a nastavovať tak, aby sa zabezpečila požadovaná dostupnosť a výkonnosť systému.

Nové systémy spracovania, aktualizácie a nové verzie by sa mali pred prijatím otestovať, aby sa zabezpečilo splnenie všetkých kritérií prijatia. Migrácia do výroby by mala vyžadovať formálnu akceptáciu. Bezpečnostný manažér musí byť zapojený a vypočutý.

Prijatie môže zahŕňať formálny certifikačný a akreditačný proces na overenie, či boli bezpečnostné požiadavky riadne splnené.

9.4.5 Ochrana pred škodlivým a mobilným kódom

Cieľ

Integrita systémov a softvéru podporujúceho informácie súvisiace s TOE musí byť chránená pred škodlivým kódom v prípade potreby.

Zásady

Zásady zakazujú používanie nepovoleného softvéru.

Politika definuje povinné ochranné opatrenia na ochranu pred rizikami spojenými so získavaním súborov a softvéru buď z externých sietí, alebo prostredníctvom nich, alebo na akomkoľvek inom médiu.

Musia byť definované postupy a zodpovednosti manažmentu pre ochranu systémov pred škodlivým kódom vrátane školení o ich používaní, upozorňovaní, hlásení a zotavovaní sa z útokov škodlivého kódu.

Bezpečnostná politika definuje povolené operácie s mobilným kódom.

Bezpečnostné opatrenia

Zavedú sa kontrolné mechanizmy detekcie, prevencie a obnovy na ochranu pred škodlivým kódom a vhodné postupy na zvýšenie informovanosti používateľov.

Počítače a všetky ostatné zariadenia a materiály poskytnuté vývojárom sa musia používať len na firemné účely; výnimky možno definovať pre používanie smart telefónov. Sťahovanie alebo ukladanie neschváleného softvéru alebo údajov nie je povolené.

Pravidelne sa vykonáva kontrola softvéru a obsahu údajov pripojených systémov podporujúcich

kritické obchodné procesy; prítomnosť akýchkoľvek neschválených súborov alebo neoprávnených zmien by sa mala formálne prešetriť.

Softvér na detekciu a opravu škodlivého kódu by mal byť nainštalovaný a pravidelne aktualizovaný, aby bolo možné preventívne alebo bežne kontrolovať počítače a médiá.

Ak je používanie mobilného kódu povolené, konfigurácia zabezpečí, aby povolený mobilný kód fungoval v súlade s jasne definovanou bezpečnostnou politikou a aby sa zabránilo spusteniu neautorizovaného mobilného kódu.

Prístup k mobilnému kódu na externých webových stránkach musí byť obmedzený, napr. na proxy serveroch. Na strane klienta by sa mal pomocou mechanizmu obmedzených/dôveryhodných stránok prehliadača udeliť prístup k webovým stránkam obsahujúcim mobilný kód len po formálnom schválení.

9.4.6 Záložný cieľ

Integrita, dostupnosť a - ak sa vyžaduje - dôvernosť informácií a bezpečnostných systémov súvisiacich s TOE (minimálne

Údaje súvisiace s TOE, kontrola prístupu a súbory denníkov správcu) sa zabezpečia, ak sa používa záložný systém.

Zásady

V zdokumentovanom postupe schválenom bezpečnostným manažérom sa definujú operácie bezpečného vytvárania, ukladania a ničenia záloh, pričom sa zabezpečí rovnaká úroveň bezpečnosti ako v prípade pôvodných údajov.

Bezpečnostné opatrenia

Mali by byť k dispozícii primerané záložné zariadenia, aby sa zabezpečilo, že po havárii alebo zlyhaní média bude možné obnoviť všetky dôležité informácie a softvér pri zachovaní dôvernosti a integrity TOE a jeho časti.

Záložné opatrenia by sa mali pravidelne testovať, aby sa zabezpečilo, že spĺňajú požiadavky dohodnutej politiky zálohovania.

V prípade kritických systémov by sa záložné opatrenia mali vzťahovať na všetky systémové informácie, aplikácie a údaje potrebné na obnovu všetkých systémov súvisiacich s TOE a bezpečnostných systémov v prípade havárie.

Príklady

Určí sa doba uchovávania základných informácií a prípadná požiadavka na trvalé archivovanie informácií.

Pravidelné denné, týždenné a mesačné zálohovanie na dátových nosičoch (HDD, DVD, pásky) využívajú malé subjekty. Veľké subjekty zvyčajne zálohujú údaje prostredníctvom online systémov na vzdialených miestach alebo zrkadlia údaje na redundantných horúcich systémoch.

Bezpečnostné prostredie, v ktorom sú umiestnené zálohy, poskytuje rovnakú úroveň bezpečnosti ako prevádzkové prostredie.

9.4.7 Riadenie bezpečnosti siete

Cieľ

Sieťová bezpečnosť zabezpečuje primeranú ochranu údajov a informácií súvisiacich s TOE a bezpečnostnou infraštruktúrou.

Zásady

Vývojár špecifikuje bezpečnosť siete z hľadiska sieťovej architektúry a preventívnych a detekčných opatrení. Politika obmedzí sieťovú prevádzku cez vstupný bod do siete rozvojovej oblasti na minimum.

Bezpečnostné opatrenia

Bezpečnosť sieťovej infraštruktúry je založená na implementácii týchto bezpečnostných opatrení:

- Obmedzenie prístupu len na oprávnené osoby.
- Kontrola vstupných bodov, obmedzenie dopravy na minimum.
- Oddelenie od ostatných sietí buď fyzicky, alebo pomocou technológií VLAN, chránené opatreniami na kontrolu prístupu a vhodnými pravidlami brány firewall.
- Fyzické oddelenie hardvéru (napr. servera, firewallu, smerovača, patch panelu atď.) a administratívy do riadne zabezpečených priestorov zodpovedajúcich úrovni bezpečnosti rozvojovej oblasti.
- Silná autentizačná schéma definovaná pre prístup k sieti.
- Zabezpečená konfigurácia vývojových počítačov s kontrolovanou, reštriktívnou používateľskou bezpečnostnou politikou, ktorá zabraňuje inštalácii ďalších, neautorizovaných funkcií.
- Použitie mechanizmu medzi hranicou podnikovej/verejnej siete a IT systémami rozvojovej oblasti, ktorý poskytuje aktuálnu ochranu komerčnej úrovne proti logickým útokom.
- Žiadne bezdrôtové pripojenie pre vývojové siete.

Pri implementácii sieťových kontrol by sa mali zohľadniť aj tieto položky:

- Prevádzková zodpovednosť za siete oddelená od počítačovej prevádzky, napr. sieťové operačné centrum pre správu sieťových zariadení a miestnu správu serverov;
- Špeciálne kontroly na zabezpečenie dôvernosti a integrity údajov prenášaných cez verejné siete alebo cez bezdrôtové siete a na ochranu pripojených systémov a aplikácií; špeciálne kontroly na udržanie dostupnosti sieťových služieb a pripojených počítačov, pokiaľ ide o bezpečnostné systémy;
- Vhodné zaznamenávanie a monitorovanie umožňujúce zaznamenávanie činností súvisiacich s bezpečnosťou;
- Činnosti riadenia sa koordinujú s cieľom optimalizovať služby pre organizáciu a zabezpečiť, aby sa kontroly dôsledne uplatňovali v celej infraštruktúre spracovania.
- Členovia rozvojového prostredia by nemali mať administrátorské práva na IT systémy, s ktorými pracujú.

Nemalo by byť možné prezerať a/alebo upravovať konfiguračné položky mimo definovanej rozvojovej oblasti, a to ani v rámci podnikovej siete.

Prístup k vývojovým sieťam by mal byť obmedzený na zabezpečeného klienta dodaného vývojárom. Vývojové siete spracúvajúce obmedzené informácie musia umožňovať vzdialený prístup len na zabezpečeného klienta špeciálne určeného na tento účel prostredníctvom zabezpečenej siete VPN. Vývojové siete spracúvajúce citlivé, kritické alebo veľmi kritické informácie nesmú umožniť vzdialený prístup z prostredia mimo vývojovej siete.

Bezpečnostné prvky, úrovne služieb a požiadavky na správu všetkých sieťových služieb by mali byť identifikované a zahrnuté v každej zmluve o sieťových službách bez ohľadu na to, či sa tieto služby poskytujú interne alebo externe.

Vývojár by mal rozdeliť povinnosti pri správe IT (správa siete, servera, klienta, aplikácie). Súbory protokolov správcu by mali byť zabezpečené mimo dosahu správcu.

Príklady

V typickom nastavení je sieť chránená pomocou:

- Brány firewall aplikačnej vrstvy s obmedzujúcimi pravidlami
- Kontrola prípustnosti siete
- Systémy detekcie/prevencie narušenia
- Ochrana proti vírusom/malvéru

Bežné služby (AD, DNS, licenčné servery atď.) sú umiestnené v DMZ. Správa siete, servera a klienta je oddelená.

Prístup k vývojovým sieťam je možný len pomocou tenkých klientov (terminálov) alebo tvrdých klientov, ktorí účinne zabraňujú kopírovaniu sieťového obsahu (napr. žiadne vstupy a výstupy okrem monitora, klávesnice a myši).

9.4.8 Manipulácia s médiami

Pamäťové médiá sa používajú na ukladanie údajov a na ich prenos z jedného miesta na druhé. Médiami môžu byť pásky, HDD, USB kľúče, CD/DVD/BD, smartfóny, smart karty a akékoľvek iné nosiče údajov.

Cieľ

V záujme ochrany integrity a/alebo dôvernosti údajov a informácií súvisiacich s TOE musia byť všetky médiá chránené proti neoprávnenému zverejneniu, modifikácii, odstráneniu, krádeži, zničeniu alebo poškodeniu.

Zásady

Mali by sa zaviesť vhodné prevádzkové postupy na ochranu dokumentov, počítačových médií, mobilných zariadení, vstupných/výstupných údajov a systémovej dokumentácie pred neoprávneným zverejnením, zmenou, odstránením a zničením.

Ak sa vyžaduje dôvernosť a/alebo integrita, musia byť zavedené postupy na správu vymeniteľných médií.

Všetky postupy a úrovne oprávnenia by mali byť jasne zdokumentované.

Formálne postupy bezpečnej likvidácie médií minimalizujú riziko úniku citlivých informácií k neoprávneným osobám. Postupy bezpečnej likvidácie médií obsahujúcich utajované skutočnosti by mali zodpovedať stupňu utajenia týchto skutočností.

Bezpečnostné opatrenia

Médiá by mali byť kontrolované a fyzicky chránené. Bezpečnostné opatrenia by mali zahŕňať vhodné označovanie médií, skladovanie, bezpečnú prepravu, likvidáciu a manipuláciu, ktoré sú potrebné a nevyhnutné na ochranu všetkých foriem médií používaných na uchovávanie údajov.

Utajované údaje (vyhradené, citlivé a kritické) sa počas uloženia na prenosnom dátovom nosiči a počas prepravy šifrujú.

Médiá sa bezpečne a spoľahlivo zlikvidujú, keď už nie sú potrebné, pričom sa použijú formálne postupy.

Povolenie na prenosné médiá by sa malo udeliť len vtedy, ak je to zjavne potrebné. Médiá by mali byť uložené v trezore alebo v bezpečnom prostredí v súlade so špecifikáciami vývojára. Mala by sa zaviesť registrácia vymeniteľných médií a proces autorizácie odstránenia, aby sa znížila možnosť straty údajov a zabezpečil sa auditný záznam.

Médiá obsahujúce neverejné informácie by sa mali bezpečne uchovávať a likvidovať. Poskytovatelia služieb zberu a likvidácie dokumentov, zariadení a médií by sa mali vyberať opatrne.

Likvidáciu citlivých položiek by mali sledovať zamestnanci vývojára a podľa potreby ju zaznamenať, aby sa zachoval auditný záznam.

Pri zhromažďovaní médií určených na likvidáciu by sa mal zohľadniť agregačný efekt, ktorý môže zmeniť množstvo necitlivých informácií na citlivé informácie.

Príklady

Súpis poskytuje aktuálny stav všetkých dátových médií používaných na činnosti súvisiace s TOE.

Schvaľovací proces pre jednotky vymeniteľných médií zabezpečuje, že povolenie sa udeľuje len v odôvodnených prípadoch. O odstránení sa vedú záznamy a udržiava sa auditný záznam.

Všetky médiá sú v čase, keď sa nepoužívajú, uložené v trezore. Vyradené optické disky (CD, DVD, BD) sa skartujú.

HDD sa anonymizujú podľa DoD 5220.22-M (3 prechody) na ďalšie použitie v rámci organizácie.

Proces ničenia sa zaznamenáva a nahráva na kamerový systém. Likvidáciu citlivých položiek sledujú

dôveryhodní zamestnanci vývojára.

9.4.9 Výmena informácií

Cieľ

Pri výmene informácií a údajov v rámci organizácie alebo s akýmkoľvek externým subjektom sa zachováva ich integrita a v prípade potreby aj dôvernosť.

Zásady

Formálne politiky, postupy a opatrenia na výmenu informácií sa definujú a zavádzajú s cieľom chrániť výmenu informácií prostredníctvom používania všetkých typov komunikačných zariadení.

Bezpečnostné opatrenia

Prenos údajov do/z zabezpečených sietí je možný len prostredníctvom zabezpečeného mechanizmu s autorizovanými prístupovými účtami. Zavedú sa vhodné opatrenia na oddelenie externých sietí od zabezpečených sietí.

Ak sa vyžaduje dôvernosť a integrita TOE a jeho častí, prenos súvisiacich informácií a údajov sa šifruje a podpisuje. Ak sa vyžaduje len integrita TOE a jeho častí, prenos súvisiacich informácií a údajov sa podpíše.

Mali by sa uzavrieť dohody o výmene informácií a softvéru medzi vývojárom a externými stranami. V takýchto dohodách o výmene by mali byť uvedené politiky, postupy a normy vývojára. Bezpečnostný obsah každej dohody by mal odrážať citlivosť príslušných obchodných informácií.

Informácie zahrnuté do elektronického zasielania správ by mali byť primerane chránené. Bezpečnostné aspekty by mali zahŕňať nasledujúce položky:

- Ochrana správ pred neoprávneným prístupom (heslo, šifrovanie) alebo modifikáciou;
- Zabezpečenie správneho adresovania a prepravy správy;
- Zabezpečenie autentickosti správy, t. j. odosielateľ/autor správy by mal byť jednoznačný;
- Silná autentizácia obmedzujúca prístup z verejne prístupných sietí, napr. klientsky certifikát a VPN.

Na prepravu dátových nosičov a dokumentov by sa mali používať len kuriéri schválení spoločnosťou.

Príklady

Výmena dokumentov alebo tlačených kópií je chránená použitím uzamknutých kontajnerov alebo osobným doručením. Obal, ktorý je zabezpečený proti neoprávnenej manipulácii, odhalí akýkoľvek pokus o získanie prístupu.

V prípade vysokých bezpečnostných požiadaviek môže byť účinnou ochranou rozdelenie zásielky na viac ako jednu dodávku a preprava po rôznych trasách.

9.4.10 Služby elektronického obchodu

Neuplatňuje sa

9.4.11 Monitorovanie

Cieľ

Neoprávnené činnosti spracovania sa zisťujú.

Zásady

V politike sa podrobne uvedú opatrenia na monitorovanie, najmä zaznamenávanie a posudzovanie súborov denníkov.

Bezpečnostné opatrenia

S cieľom umožniť odhalenie neoprávnených spracovateľských činností a pomôcť pri vyšetrovaní sa vytvárajú a počas stanoveného obdobia uchovávajú tieto súbory denníkov:

- Činnosti používateľov, výnimky a udalosti súvisiace so zabezpečením informácií.
- Činnosti správcu systému a systémového operátora.
- Odmietnuté pokusy o prihlásenie alebo narušenia zabezpečenia (zapnutím funkcie protokolu bezpečnostných udalostí všetkých klientov).
- Systémové činnosti súvisiace so sieťou z radičov domény, firewallov alebo proxy serverov.

Zariadenia na zaznamenávanie a informácie o záznamoch musia byť chránené proti neoprávnenej manipulácii a neoprávnenému prístupu. Súbory denníkov správcu systému by sa mali uchovávať mimo dosahu príslušného správcu, resp. prevádzkovateľa systému a aspoň raz mesačne by sa mali kontrolovať, či sa v nich nevykonávajú podozrivé činnosti.

Príklady

Platobné schémy vyžadujú trojmesačné obdobie uchovávania online a ročné obdobie uchovávania offline súborov denníka auditu.

9.5 Kontrola prístupu do informačných systémov

9.5.1 Celkový cieľ

Prístup (logický a fyzický) k informačným systémom vrátane prístupu k obchodným procesom, k sieťam, k operačným systémom, k aplikáciám a k informáciám sa kontroluje a obmedzuje na základe potreby vedieť.

Používatelia, používateľské roly a zodpovednosti používateľov sa spravujú a kontrolujú.

9.5.2 Obchodná požiadavka na kontrolu prístupu

Cieľ

Prístup k informáciám, zariadeniam na spracovanie informácií a obchodným procesom sa riadi na základe bezpečnostných požiadaviek.

Zásady

Na základe obchodných požiadaviek (bezpečnostné potreby na ochranu dôvernosti a/alebo integrity TOE) sa stanoví, zdokumentuje a pravidelne reviduje politika riadenia prístupu. V tejto politike sa podrobne uvedú pravidlá kontroly prístupu pre každú rolu (používateľa alebo skupinu používateľov).

Bezpečnostné opatrenia

Prístup sa udeľuje len na základe potreby vedieť.

Úlohy riadenia prístupu pre prístup do priestorov aj prístup do systémov by mali byť oddelené, napr. žiadosť o prístup, autorizácia prístupu a správa prístupu.

Príklady

Politika riadenia prístupu zohľadňuje:

- bezpečnostné požiadavky na obchodné činnosti vývojárov;
- politiky šírenia a autorizácie informácií, napr. zásada potreby poznať a úrovne bezpečnosti a klasifikácie informácií;
- konzistentnosť medzi politikami riadenia prístupu a klasifikácie informácií v rôznych systémoch a sieťach;
- príslušné právne predpisy a všetky zmluvné záväzky týkajúce sa ochrany prístupu k údajom alebo službám;

- správa prístupových práv v distribuovanom a sieťovom prostredí, ktoré rozpoznáva všetky dostupné typy pripojení.

Role v procese autorizácie prístupu sú oddelené. Žiadosti schvaľuje manažér žiadateľa a vlastník systému a/alebo údajov, autorizáciu realizuje bezpečnostný manažér (fyzický prístup), resp. správca IT (logický prístup). Systém kontroly prístupu spravuje jeho vlastník (bezpečnostný manažér, vlastník aplikácie, správca systému).

9.5.3 Správa prístupu používateľov

Cieľ

Prístup do informačných systémov majú len oprávnení používatelia.

Zásady

Stanoví sa a zdokumentuje politika týkajúca sa riadenia prístupu používateľov. Podrobne sa v nej uvádza, ako sa udeľujú prístupové práva a oprávnenia a aké roly sa používajú.

Stanoví sa a zdokumentuje politika týkajúca sa kvality hesiel.

Bezpečnostné opatrenia

Postupy sa vzťahujú na všetky fázy životného cyklu prístupu používateľov, od počiatočnej registrácie nových používateľov až po konečné zrušenie registrácie používateľov, ktorí už nepotrebujú prístup k informačným systémom a službám. Osobitná pozornosť sa venuje potrebe kontroly prideľovania privilegovaných prístupových práv.

Všetci používatelia majú jedinečný identifikátor určený len na ich osobné použitie a na preukázanie deklarovanej totožnosti používateľa sa zvolí vhodná autentizačná technika. Toto je povinné pre všetky typy používateľov (vrátane pracovníkov technickej podpory, operátorov, správcov siete, programátorov systému a správcov databázy).

Musí byť zavedený formálny postup registrácie a zrušenia registrácie používateľov na udeľovanie a zrušenie prístupu do všetkých informačných systémov a služieb.

Postup kontroly prístupu pre registráciu a zrušenie registrácie používateľa by mal zahŕňať:

- používanie jedinečných identifikátorov používateľov (napr. používateľských účtov), ktoré umožňujú prepojenie používateľov a zodpovednosť za ich činnosť; používanie skupinových identifikátorov je povolené len v prípade, že je potrebné z obchodných alebo prevádzkových dôvodov, a musí byť schválené a zdokumentované; pre takéto skupinové identifikátory sa určia zodpovedné osoby;
- kontrola, či má používateľ oprávnenie od vlastníka systému na používanie informačného systému alebo služby; vhodné môže byť aj samostatné schválenie prístupových práv od vedenia;
- kontrola, či je úroveň udeleného prístupu primeraná obchodnému účelu a či je v súlade s bezpečnostnou politikou organizácie, napr. či neohrozuje oddelenie povinností;
- poskytnutie písomného vyhlásenia používateľom o ich prístupových právach;
- vyžadovať od používateľov, aby podpísali vyhlásenie, že rozumejú podmienkam prístupu;
- zabezpečiť, aby poskytovatelia služieb neposkytovali prístup, kým sa neukončia autorizačné postupy;
- vedenie formálnej evidencie všetkých osôb registrovaných na používanie služby, napr. v systéme Active Directory;
- okamžité odstránenie alebo zablokovanie prístupových práv používateľov, ktorí zmenili rolu alebo pracovné miesto alebo opustili organizáciu;
- pravidelná kontrola a odstraňovanie alebo blokovanie nadbytočných ID používateľov a účtov;
- zabezpečenie toho, aby sa ID používateľov nevydávali iným používateľom.

Prideľovanie a používanie oprávnení je obmedzené a kontrolované.

Viacpoužívateľské systémy, ktoré vyžadujú ochranu pred neoprávneným prístupom, musia mať prideľovanie oprávnení kontrolované prostredníctvom formálneho procesu autorizácie.

Zohľadňujú sa tieto kroky:

- sa určia prístupové oprávnenia spojené s každým systémom, napr. operačným systémom,

systémom správy databáz a každou aplikáciou, a používatelia, ktorým sa musia prideliť;
- oprávnenia sa prideľujú používateľom na základe potreby ich používania
- proces autorizácie a vedie sa záznam o všetkých pridelených oprávneniach. Oprávnenia sa udeľujú až po ukončení autorizačného procesu;
- by sa mal podporovať vývoj a používanie systémových postupov, aby sa predišlo potrebe udeľovať používateľom oprávnenia;
- by sa mal podporovať vývoj a používanie programov, ktoré sa vyhýbajú potrebe spúšťania s oprávneniami.
- Prideľovanie hesiel sa kontroluje prostredníctvom formálneho procesu riadenia. Tento proces musí zohľadňovať tieto požiadavky:
- ak sa od používateľov vyžaduje, aby si sami udržiavali svoje heslá, mali by mať na začiatku k dispozícii bezpečné dočasné heslo, ktoré si musia okamžite zmeniť;
- zaviesť postupy na overenie totožnosti používateľa pred poskytnutím nového, náhradného alebo dočasného hesla;
- dočasné heslá sa používateľom poskytujú bezpečným spôsobom; treba sa vyhnúť používaniu tretích strán alebo nechránených (čistých textových) správ elektronickej pošty;
- dočasné heslá musia byť pre jednotlivca jedinečné a nesmú sa dať uhádnuť;
- heslá sa nikdy neukladajú do počítačových systémov v nechránenej forme;
- po inštalácii systémov alebo softvéru sa zmenia predvolené heslá dodávateľa.

Ak sa vyžaduje silná autentizácia a overenie totožnosti, mali by sa použiť metódy autentizácie, ktoré sú alternatívne k heslám, ako napríklad kryptografické prostriedky, smart karty, tokeny alebo biometrické prostriedky.

Systémy na správu hesiel by mali byť interaktívne a mali by zabezpečovať kvalitné heslá.

Systém správy hesiel by mal:

- ukladať súbory s heslami oddelene od systémových údajov aplikácie;
- ukladať a prenášať heslá v chránenej (napr. šifrovanej alebo hashovanej) forme.

Vedenie pravidelne preskúmava prístupové práva používateľov pomocou formálneho procesu. Pri preskúmaní prístupových práv sa zohľadnia tieto usmernenia:

- prístupové práva používateľov by sa mali pravidelne prehodnocovať, napr. po 6 mesiacoch;
- prístupové práva používateľov by sa mali preskúmať po akýchkoľvek zmenách, ako je povýšenie, degradácia alebo ukončenie pracovného pomeru;
- prideľovanie oprávnení sa pravidelne kontroluje, aby sa zabezpečilo, že neboli získané neoprávnené oprávnenia;
- zmeny privilegovaných účtov sa zaznamenávajú na účely pravidelnej kontroly.

Príklady

Nevhodné používanie oprávnení na správu systému (akákoľvek funkcia alebo prostriedok informačného systému, ktorý umožňuje používateľovi zrušiť kontroly systému alebo aplikácie) môže byť hlavným faktorom, ktorý prispieva k zlyhaniu alebo narušeniu systémov.

Heslá sú bežným prostriedkom na overenie identity používateľa pred tým, ako sa mu udelí prístup do informačného systému alebo služby podľa jeho oprávnenia. K dispozícii sú aj iné technológie na identifikáciu a autentizáciu používateľa, ako je biometria, napr. overovanie odtlačkov prstov, overovanie podpisov a používanie hardvérových tokenov, napr. smart kariet, ktoré sa považujú - ak je to vhodné - za náhradu alebo doplnenie hesiel.

Je potrebné pravidelne prehodnocovať prístupové práva používateľov, aby sa zachovala účinná kontrola prístupu k údajom a informačným službám.

Od používateľov sa vyžaduje, aby podpísali vyhlásenie o zachovaní dôvernosti osobných hesiel; toto podpísané vyhlásenie je súčasťou pracovných podmienok.

9.5.4 Povinnosti používateľa

Cieľ

Zodpovednosť používateľov za udržiavanie účinnej kontroly prístupu musí byť jasne definovaná a používatelia si musia byť vedomí svojich zodpovedností.

Zásady

V politike sa podrobne uvedie zodpovednosť používateľov za udržiavanie účinných kontrol prístupu, najmä pokiaľ ide o používanie hesiel a bezpečnosť používateľského vybavenia.

Politika hesiel vyžaduje, aby používatelia pri výbere a používaní hesiel dodržiavali správne bezpečnostné postupy.

Bezpečnostné opatrenia

Vývojár musí pri výbere a používaní hesiel dodržiavať správne bezpečnostné postupy. V politike hesiel sa od všetkých používateľov vyžaduje, aby:

- uchovávať heslá v tajnosti;
- vyhnúť sa vedeniu záznamov;
- meniť heslá v pravidelných intervaloch alebo vždy, keď sa objaví akýkoľvek náznak možného ohrozenia systému alebo hesla;
- vybrať kvalitné heslá;
- zmeniť dočasné heslá pri prvom prihlásení;
- nezahŕňajte heslá do žiadneho automatizovaného procesu prihlasovania, napr. uložené v makre alebo funkčnom kľúči;
- nezdieľajte heslá jednotlivých používateľov;
- nepoužívajte to isté heslo na pracovné a nepracovné účely.

Používatelia zabezpečia, aby bezobslužné zariadenia mali vhodnú ochranu.

V prípade potreby musia byť všetci používatelia oboznámení s bezpečnostnými požiadavkami a postupmi na ochranu bezobslužného zariadenia, ako aj so svojimi povinnosťami pri vykonávaní takejto ochrany.

Používateľom by sa malo odporučiť, aby:

- ukončiť aktívne relácie po ich ukončení, pokiaľ ich nie je možné zabezpečiť vhodným uzamykacím mechanizmom,
- napr. šetrič obrazovky chránený heslom;
- odhlásenie počítačov mainframe, serverov a kancelárskych počítačov po skončení relácie (t. j. nielen vypnutie obrazovky počítača alebo terminálu);
- zabezpečte počítače alebo terminály pred neoprávneným použitím zámkom na kľúč alebo rovnocenným ovládacím prvkom, napr. prístupom pomocou hesla (CTRL-ALT-DEL v systéme Windows), keď sa nepoužívajú;
- chrániť údaje uložené na prenosnom zariadení šifrovaním trvalého úložiska; ak údaje nie sú šifrované, prenosné zariadenie (notebook) by malo byť zabezpečené fyzickými opatreniami (napr. káblovým zámkom Kensington lock alebo uložené v uzamknutej skrini), keď sa nepoužíva;
- uchovávať dátové médiá uzamknuté, pokiaľ nie sú zašifrované.

Prijíma sa politika čistého stola pre dokumenty a vymeniteľné pamäťové médiá a politika čistej obrazovky pre zariadenia na spracovanie informácií, aby sa znížilo riziko narušenia bezpečnosti, podvodu a krádeže informácií, ku ktorým prispievajú dokumenty alebo médiá bez dozoru.

Zásady čistého stola a čistej obrazovky by mali poskytovať všetkým používateľom usmernenia týkajúce sa zaobchádzania s dokumentmi, údajmi a médiami s ohľadom na ich utajenie.

Príklady

Zásady používania hesiel vyžadujú, aby používatelia:

- vyberte kvalitné heslá s dostatočnou minimálnou dĺžkou (aspoň 8 znakov), napr. aspoň jeden znak z 3 z nasledujúcich 4 kategórií:
  - Malé písmená (a...z)
  - Veľké písmená (A...Z)
  - Číselné znaky (0...9)
  - Špeciálne znaky (!"$%&/()=?*.);
- uchovávať heslá v tajnosti;
- bezpečne ukladať heslá pomocou schváleného trezora na heslá;

- meniť heslá v pravidelných intervaloch, napr. každých 90 dní;
- zmeniť dočasné heslá pri prvom prihlásení;
- nezahŕňajte heslá do žiadneho automatizovaného procesu prihlasovania, napr. uložené v makre alebo funkčnom kľúči;
- nezdieľajte heslá jednotlivých používateľov;
- nepoužívajte to isté heslo na pracovné a nepracovné účely.

Neobsluhovaní klienti alebo pracovné stanice sú chránené aktivovaným, uzamknutým šetričom obrazovky.

Zariadenia nainštalované v užívateľských priestoroch, napr. pracovné stanice alebo súborové servery, majú špecifickú ochranu pred neoprávneným prístupom, ak sú ponechané dlhší čas bez dozoru.

9.5.5 Kontrola prístupu do siete

Cieľ

Zabráni sa neoprávnenému prístupu k sieťovým službám.

Zásady

Stanoví sa a zdokumentuje politika týkajúca sa riadenia prístupu k sieti. Podrobne opisuje architektúru siete, sieťové pripojenia, riadenie prístupu do siete a ďalšie bezpečnostné opatrenia.

Musia sa definovať a zdokumentovať špecializované procesy a usmernenia pre prístup obchodných partnerov a prepojenia s obchodnými partnermi.

Bezpečnostné opatrenia

K sieti sa môžu pripojiť len zariadenia ovládané vývojárom.

Musí sa zabezpečiť, aby prístup používateľov k sieťam a sieťovým službám nemohol ohroziť bezpečnosť sieťových služieb tým, že:

- vhodné rozhrania medzi sieťou organizácie a sieťami iných organizácií a verejnými sieťami;
- vhodné mechanizmy autentizácie používateľov a zariadení;
- kontrola prístupu používateľov k informačným službám.

Správy Syslog brány firewall by sa mali pravidelne analyzovať a v prípade potreby prijať opatrenia.

Ak je povolený vzdialený prístup do sietí vývojárov, na kontrolu prístupu vzdialených používateľov sa používajú vhodné metódy autentizácie. Ak sa vyžaduje dôvernosť citlivých, kritických alebo veľmi kritických informácií, nesmie byť možný vzdialený prístup do bezpečnostných sietí, najmä do sietí, v ktorých sa pracuje s TOE alebo jeho časťami alebo súvisiacimi konštrukčnými informáciami.

Ak sa vyžaduje dôvernosť obmedzených informácií alebo len integrita, môže sa povoliť vzdialený prístup s vhodnými bezpečnostnými opatreniami, ktoré zabezpečia integritu a prípadne aj dôvernosť na rovnakej úrovni sieťovej bezpečnosti ako v priestoroch vývojára.

Automatická identifikácia zariadenia by sa mala používať ako prostriedok na overovanie pripojení z konkrétnych miest a zariadení. Táto kontrola by sa mala doplniť ďalšími technikami na autentizáciu používateľa zariadenia.

Identifikácia zariadenia sa používa len ako doplnok k overeniu používateľa, nie ako náhrada.

Fyzický a logický prístup k diagnostickým a konfiguračným portom musí byť kontrolovaný. Porty, služby a podobné zariadenia nainštalované na počítači alebo sieťovom zariadení, ktoré nie sú osobitne potrebné na obchodné funkcie, by sa mali vypnúť alebo odstrániť.

Skupiny informačných systémov, informačných služieb alebo používateľov by mali byť v sieťach oddelené, napr. v rôznych bezpečnostných zónach alebo sieťových vetvách.

Ak sa vyžaduje dôvernosť a/alebo integrita, na všetky bezpečnostné zóny alebo vetvy siete všetkých úrovní sa vzťahujú tieto požiadavky na vysokej úrovni;

- Všetky prepojenia medzi bezpečnostnými zónami a sieťovými pobočkami plánuje a kontroluje ústredný orgán, ktorý zahŕňa bezpečnostného manažéra;

- Vzájomné prepojenie distribuovaných častí bezpečnostnej zóny alebo vetvy siete musí byť zapuzdrené/chránené použitím bezpečných sieťových techník, napr. bezpečnej VPN;
- Zodpovednosť za prepojenia a za údaje spracúvané v rámci samotných bezpečnostných zón by mala byť oddelená, aby sa zaviedol princíp štyroch očí (to znamená, že jedna osoba nesmie mať možnosť vytvoriť dátový kanál smerom von alebo dovnútra).

V prípade zdieľaných sietí, najmä tých, ktoré presahujú hranice organizácie, by sa mala obmedziť možnosť používateľov pripojiť sa k sieti v súlade s predpismi o riadení prístupu a požiadavkami podnikových aplikácií.

Prístupové práva používateľov k sieti sa udržiavajú a aktualizujú podľa požiadaviek predpisov o riadení prístupu.

Možnosť pripojenia používateľov možno obmedziť prostredníctvom sieťových brán, ktoré filtrujú prevádzku, napr. pomocou vopred definovaných tabuliek alebo pravidiel (firewall aplikačnej vrstvy).

Pre siete sa zavedú kontroly smerovania, aby sa zabezpečilo, že počítačové spojenia a informačné toky neporušujú politiku riadenia prístupu podnikových aplikácií. Kontrola smerovania musí byť založená na mechanizmoch pozitívnej kontroly zdrojovej a cieľovej adresy. Bezpečnostné brány by mali využívať aspoň jednu z týchto možností:

- firewallov na overovanie zdrojových a cieľových adries na sieťovej vrstve;
- proxy servera na overenie zdrojovej a cieľovej adresy na aplikačnej vrstve;
- SOCKS proxy server na autentizáciu používateľov.

Zdieľané siete, najmä tie, ktoré presahujú hranice organizácie, si môžu vyžadovať dodatočné kontroly smerovania. To platí najmä v prípade, keď sú siete zdieľané s používateľmi tretích strán (mimo organizácie).

Príklady

Prístup k sieti je riadený systémami NAC (Network Access Control), ktoré umožňujú prístup len pre spravované zariadenia. NAC môže byť základný (pomocou miestneho identifikátora zariadenia, napr. adresy MAC) alebo silný (pomocou certifikátu stroja a účtu počítača v aktívnom adresári).

Sieť vývojára je oddelená od ostatných sietí pomocou DMZ s firewallmi na oboch koncoch.

Kaskádovanie sietí zabezpečuje, aby bol prístup do siete udelený z príslušnej úrovne zabezpečenia. Pripojení klienti sú členmi príslušnej klientskej domény systému Windows a možno ich identifikovať pomocou certifikátov.

Identifikácia zariadenia sa používa, ak je dôležité, aby sa komunikácia mohla iniciovať len z určitého miesta alebo zariadenia. Identifikátor udáva, či je alebo nie je povolené pripojenie tohto zariadenia k určitej sieti. Na zachovanie bezpečnosti identifikátora zariadenia môže byť potrebné zvážiť fyzickú ochranu zariadenia.

Zamestnanci a obchodní partneri s notebookmi nainštalovanými a spravovanými IT oddelením vývojára (strojové certifikáty) majú umožnený úplný sieťový prístup k intranetu, súborovému serveru a serveru Exchange, zatiaľ čo obchodní partneri a dodávatelia bez zariadenia vývojára majú len obmedzený prístup k niektorým aplikáciám umiestneným v DMZ.

Potenciálne kontroly prístupu k diagnostickým a konfiguračným portom zahŕňajú použitie zámku na kľúč a podporných postupov na kontrolu fyzického prístupu k portu. Príkladom takéhoto podporného postupu je zabezpečenie toho, aby boli diagnostické a konfiguračné porty prístupné len na základe dohody medzi manažérom počítačovej služby a personálom hardvérovej/softvérovej podpory, ktorý si vyžaduje prístup.

9.5.6 Kontrola prístupu k operačnému systému

Cieľ

Zabráni sa neoprávnenému prístupu k operačným systémom.

Zásady

Stanoví sa a zdokumentuje politika, ktorá opisuje opatrenia prijaté na zabránenie neoprávnenému prístupu k operačným systémom.

Bezpečnostné opatrenia

Bezpečnostné zariadenia sa používajú na obmedzenie prístupu k operačným systémom na oprávnených používateľov. Tieto zariadenia by mali byť schopné:

- autentizácia oprávnených používateľov v súlade s definovanou politikou riadenia prístupu;
- zaznamenávanie úspešných a neúspešných pokusov o overenie systému;
- zaznamenávanie používania špeciálnych systémových oprávnení;
- vydávanie alarmov pri porušení bezpečnostných zásad systému.

Prístup k operačným systémom sa riadi bezpečným postupom prihlasovania.

Postup prihlasovania do operačného systému musí byť navrhnutý tak, aby sa minimalizovala možnosť neoprávneného prístupu. Postup prihlasovania by preto mal poskytovať minimum informácií o systéme, aby sa zabránilo poskytnutiu zbytočnej pomoci neoprávnenému používateľovi.

Používanie obslužných programov, ktoré by mohli byť schopné prekonať systémové a aplikačné kontroly, musí byť obmedzené na základe potreby a prísne kontrolované.

Funkcia časového limitu by mala vymazať obrazovku relácie a prípadne neskôr aj ukončiť relácie aplikácie a siete po definovanom čase nečinnosti. Časové oneskorenie by malo odrážať bezpečnostné riziká oblasti, klasifikáciu spracúvaných informácií a používaných aplikácií a riziká súvisiace s používateľmi zariadenia.

Kontroly času pripojenia by sa mali zvážiť pre citlivé počítačové aplikácie, napr. tie, ktoré majú prístup k TOE a jeho častiam, aby sa zabezpečila dodatočná bezpečnosť pre vysoko rizikové siete alebo aplikácie.

Príklady

Obmedzenou formou časového limitu je šetrič obrazovky chránený heslom, ktorý je súčasťou inštalácie systému Windows. Vyčistí obrazovku a zabráni neoprávnenému prístupu, ale neukončí relácie aplikácie alebo siete.

9.5.7 Kontrola prístupu k aplikáciám a informáciám

Cieľ

Integrita a - ak je to potrebné - dôvernosť údajov a informácií súvisiacich s TOE a bezpečnostné systémy musia byť chránené prostredníctvom účinnej kontroly prístupu k aplikáciám a informáciám.

Zásady

V politike sa podrobne uvedú opatrenia prijaté na obmedzenie prístupu k aplikáciám a informáciám a na izoláciu systémov s citlivým, kritickým alebo veľmi kritickým obsahom.

Bezpečnostné opatrenia

Prístup používateľov a podporného personálu k funkciám informačného a aplikačného systému je obmedzený v súlade s definovanými zásadami kontroly prístupu.

Zásada "need-to-know" sa uplatňuje v celom aplikačnom prostredí, napr. prístupové práva špecifické pre projekt, obmedzený prístup k pracovným podielom.

Systémy s citlivým, kritickým alebo veľmi kritickým obsahom musia mať vyhradené (izolované) počítačové prostredie.

Aplikácie a systémy s citlivým, kritickým alebo veľmi kritickým obsahom (napr. vývojové siete, sieť IT Administration Network) nesmú byť prevádzkované v zdieľaných prostrediach. Potrebné zdieľané služby (napr. Active Directory, Netinstall, licenčný server, drop box) musia byť nainštalované v DMZ. Údaje by sa mali prenášať prostredníctvom mechanizmov drop box.

9.5.8 Mobilná výpočtová technika a práca na diaľku

Cieľ

Údaje a informácie súvisiace s TOE a bezpečnostné systémy musia byť pri používaní mobilnej výpočtovej techniky a zariadení pre prácu na diaľku primerane chránené.

Zásady

Mala by byť zavedená politika a mali by sa prijať vhodné bezpečnostné opatrenia na ochranu pred rizikami spojenými s používaním mobilnej výpočtovej techniky (notebook, prenosné zariadenia) a komunikačných zariadení (smartfóny atď.).

V prípade potreby sa vypracuje a zavedie politika, prevádzkové plány a postupy pre vzdialený prístup a tele prácu.

Bezpečnostné opatrenia

Ak sa vyžaduje dôvernosť citlivých, kritických alebo veľmi kritických informácií, mobilná výpočtová technika TOE alebo jej častí alebo súvisiacich konštrukčných informácií nesmie byť možná.

Ak sa vyžaduje dôvernosť obmedzených informácií alebo len integrita, mobilná výpočtová technika sa môže povoliť s vhodnými bezpečnostnými opatreniami, ktoré zabezpečia integritu a prípadne aj dôvernosť na rovnakej úrovni sieťovej bezpečnosti ako v priestoroch vývojára.

Práca na diaľku s prístupom k TOE alebo jeho častiam, informáciám súvisiacim s TOE a súvisiacim bezpečnostným systémom je povolená len pre prostredia s verejným alebo obmedzeným obsahom, ak sa v nich nenachádza citlivý, kritický alebo veľmi kritický obsah. Prostredie pre prácu na diaľku (priestory, IT atď.) musí spĺňať všetky požiadavky týkajúce sa integrity a prípadne dôvernosti stanovené v tomto dokumente. Ak je práca na diaľku povolená, musia byť zavedené procesy na zabezpečenie integrity počas všetkých činností práce na diaľku.

Pri používaní mobilných počítačových zariadení na verejných miestach (aj v priestoroch organizácie), v rokovacích miestnostiach a iných nechránených priestoroch mimo priestorov organizácie je potrebné postupovať opatrne. Mala by sa zaviesť ochrana, ktorá zabráni neoprávnenému prístupu k informáciám uloženým a spracúvaným týmito zariadeniami alebo ich zverejneniu, napr. pomocou kryptografických techník.

Teleworking využíva komunikačné technológie, ktoré umožňujú zamestnancom pracovať na diaľku z miesta mimo prostredia vývojárov. Mobilné zariadenia musia byť chránené proti logickým útokom počas prístupu do externých sietí v rovnakom rozsahu, ako je to zabezpečené v sieti vývojárov.

Príklady

Vzdialený prístup z domácej kancelárie do kancelárskeho prostredia vývojára je možný na kontrolu e-mailov a používanie bežných kancelárskych nástrojov. Prístup k citlivým špecifikáciám, poznámkam k aplikáciám, atď. nie je povolený.

9.6 Získavanie, vývoj a údržba informačných systémov

9.6.1 Celkový cieľ

Bezpečnosť je neoddeliteľnou súčasťou informačných systémov. Informačné systémy musia byť zabezpečené na takej úrovni, aby sa zabezpečila integrita a dôvernosť TOE a aby sa zabezpečila dostupnosť a riadne fungovanie bezpečnostných systémov.

Informačné systémy zahŕňajú operačné systémy, infraštruktúru, podnikové aplikácie (napr. rozvojové prostredia, systémy riadenia konfigurácie) a služby, či už hotové produkty alebo aplikácie vyvinuté používateľom.

9.6.2 Bezpečnostné požiadavky na informačné systémy (informatívne)

Cieľ

Bezpečnostné požiadavky by sa mali určiť a odsúhlasiť pred obstaraním IT systémov. Bezpečnosť by mala byť neoddeliteľnou súčasťou požiadaviek na obstarávanie informačných systémov.

Zásady

Politika obstarávania by mala definovať kroky potrebné na zmiernenie rizík vyplývajúcich z používaných systémov IT (hardvér a softvér).

Vývoj softvéru, implementácia a využívanie aplikácií vyvinutých vývojárom alebo v jeho mene by mali byť podrobne opísané.

Mala by sa definovať inštalácia a overovanie hotových produktov.

Bezpečnostné opatrenia

Všetky bezpečnostné požiadavky by sa mali identifikovať vo fáze požiadaviek projektu a mali by sa zdôvodniť, odsúhlasiť a zdokumentovať ako súčasť celkového obchodného odôvodnenia informačného systému.

Vo vyhláseniach o obchodných požiadavkách na nové informačné systémy alebo na vylepšenia existujúcich informačných systémov by sa mali špecifikovať požiadavky na bezpečnostné kontroly.

Pri nákupe produktov by sa mal dodržiavať formálny proces testovania a získavania. Zmluvy s dodávateľom by sa mali zaoberať identifikovanými bezpečnostnými požiadavkami. Ak bezpečnostná funkcionalita navrhovaného produktu nespĺňa špecifikovanú požiadavku, malo by sa pred nákupom produktu prehodnotiť zavedené riziko a súvisiace kontroly. Ak sa dodáva dodatočná funkcia, ktorá spôsobuje bezpečnostné riziko, táto funkcia by sa mala vypnúť alebo by sa mala prehodnotiť navrhovaná štruktúra kontroly.

9.6.3 Správne spracovanie v aplikáciách

Cieľ

Zabráni sa chybám, strate, neoprávnenej úprave alebo zneužitiu informácií v systémoch IT.

Musí byť zabezpečená integrita a/alebo dôvernosť TOE a jeho častí.

Zásady

V politike sa podrobne uvedú opatrenia zavedené na zabezpečenie integrity a autentickosti údajov týkajúcich sa TOE alebo správneho fungovania bezpečnostných systémov.

Bezpečnostné opatrenia

V aplikáciách vrátane aplikácií vytvorených používateľom by mali byť navrhnuté vhodné kontrolné mechanizmy na zabezpečenie správneho spracovania. Tieto kontroly by sa mali určiť na základe bezpečnostných zámerov, iných bezpečnostných požiadaviek a posudzovania rizika. Mali by zahŕňať validáciu vstupných údajov, interného spracovania a výstupných údajov.

Systémy a aplikácie sa zvyčajne vytvárajú na základe predpokladu, že po vykonaní vhodnej validácie, overovania a testovania bude výstup vždy správny. Tento predpoklad však nie je vždy platný, t. j. systémy, ktoré boli testované, môžu za určitých okolností stále produkovať nesprávny výstup.

<u>Overovanie vstupných údajov (informatívne)</u>

Údaje vkladané do aplikácií s vplyvom na bezpečnosť a/alebo integritu TOE a jeho častí by sa mali validovať, aby sa zabezpečilo, že tieto údaje sú správne a primerané.

V prípade potreby by sa malo zvážiť automatické preskúmanie a overenie vstupných údajov, aby sa znížilo riziko chýb a zabránilo útokom.

Kontrola vnútorného spracovania (informatívne)

Návrh a implementácia aplikácií by mali zabezpečiť, aby sa znížilo riziko zlyhania spracovania, ktoré vedie k strate integrity alebo dôvernosti. Do aplikácií by sa mali začleniť overovacie kontroly, aby sa zistilo akékoľvek poškodenie informácií v dôsledku chýb pri spracovaní alebo úmyselné.

Integrita správy (informatívne)

Integrita komunikácie elektronickej pošty by sa mala zabezpečiť použitím funkcie šifrovania a podpisovania založenej na vhodných kryptografických algoritmoch a vhodných protokoloch.

Overovanie výstupných údajov (informatívne)

Výstup údajov z aplikácie by sa mal overiť, aby sa zabezpečilo, že spracovanie uložených informácií je správne a primerané okolnostiam.

Príklady

Kontrola zadávania údajov zvyčajne zahŕňa tieto kroky:

- duálne zadávanie alebo iné vstupné kontroly, ako je kontrola hraníc alebo obmedzenie polí na určité rozsahy vstupných údajov, s cieľom odhaliť chyby;
- pravidelná kontrola obsahu kľúčových polí alebo dátových súborov s cieľom potvrdiť ich platnosť a integritu;
- kontrola vstupných dokumentov v tlačenej podobe, či v nich nedošlo k neoprávneným zmenám (všetky zmeny vo vstupných dokumentoch by mali byť autorizované);
- postupy reakcie na chyby validácie;
- postupy na testovanie hodnovernosti vstupných údajov;
- vymedzenie povinností všetkých pracovníkov zapojených do procesu zadávania údajov;
- vytvorenie záznamu o činnostiach súvisiacich s procesom zadávania údajov.

Kontrola interného spracovania môže zahŕňať:

- používanie funkcií pridať, upraviť a odstrániť na vykonávanie zmien údajov;
- postupy, ktoré zabránia spusteniu programov v nesprávnom poradí alebo spusteniu po zlyhaní predchádzajúceho spracovania;
- používanie vhodných programov na obnovu po poruchách, aby sa zabezpečilo správne spracovanie údajov;
- ochranu pred útokmi.

Integrita elektronickej poštovej komunikácie sa dá zabezpečiť pomocou funkcie šifrovania a podpisovania založenej na kľúčoch PGP alebo certifikátoch S/MIME.

Výstupná validácia môže zahŕňať:

- kontroly vierohodnosti na testovanie, či sú výstupné údaje primerané;
- kontrola zosúladenia s cieľom zabezpečiť spracovanie všetkých údajov;
- poskytnutie dostatočných informácií čitateľovi alebo systému následného spracovania na určenie presnosti, úplnosti, správnosti a klasifikácie informácií;
- postupy reakcie na výstupné validačné testy;
- vymedzenie povinností všetkých pracovníkov zapojených do procesu výstupu údajov;
- vytvorenie záznamu o činnostiach v procese validácie výstupných údajov.

9.6.4 Kryptografické kontroly

Cieľ

Dôvernosť, autentickosť a integrita informácií sa chráni kryptografickými prostriedkami. Kryptografické kľúče sa spravujú a chránia pred prezradením, modifikáciou, stratou a zničením.

Zásady

Vypracuje sa, implementuje a udržiava politika používania kryptografických kontrol na ochranu

informácií.

Bezpečnostné opatrenia

Kryptografické kontroly by sa mali používať na dosiahnutie rôznych bezpečnostných cieľov vrátane:

- dôvernosť: používanie šifrovania informácií na ochranu citlivých, kritických alebo veľmi kritických informácií, či už uložených alebo prenášaných;
- integrita/autentickosť: používanie digitálnych podpisov alebo kódov na autentizáciu správ na ochranu autentickosti a integrity uložených alebo prenášaných citlivých alebo kritických informácií;
- nepopieranie: použitie kryptografických techník na získanie dôkazu o výskyte alebo nevýskyte udalosti alebo akcie.

Šifrovacie kľúče musia byť založené na otvorených algoritmoch a musia byť odvodené z náhodných s dostatočnou entropiou, aby sa zabránilo útokom hrubou silou.

Správa kľúčov musí byť zavedená tak, aby podporovala vývojára pri používaní kryptografických techník.

Všetky kryptografické kľúče musia byť chránené proti modifikácii, strate a zničeniu. Okrem toho je potrebné chrániť tajné a súkromné kľúče pred neoprávneným prezradením. Zariadenia používané na generovanie, uchovávanie a archiváciu kľúčov musia byť fyzicky chránené.

Príklady

Kľúčové procesy riadenia zvyčajne zahŕňajú:

- generovanie kľúčov
- generovanie a získavanie certifikátov verejného kľúča;
- distribúciu kľúčov určeným používateľom vrátane spôsobu aktivácie kľúčov po ich prijatí;
- ukladanie kľúčov vrátane spôsobu, akým oprávnení používatelia získavajú prístup ku kľúčom;
- zmena alebo aktualizácia kľúčov vrátane pravidiel, kedy sa majú kľúče zmeniť a ako sa to vykoná;
- zaobchádzanie s kompromitovanými kľúčmi;
- zrušenie kľúčov;
- obnovenie kľúčov;
- archivačné kľúče, napr. pre archivované alebo zálohované informácie;
- zničenie kľúčov;
- zaznamenávanie a auditovanie kľúčových činností súvisiacich s riadením.

9.6.5 Bezpečnosť systémových súborov

Cieľ

Operačné systémy a aplikácie musia byť zabezpečené a chránené proti neúmyselnej zmene. Prístup k zdrojovému kódu programu je obmedzený.

Zásady

Práva správcu sa upravia v pravidlách, v ktorých sa opíše spôsob ich udeľovania, monitorovania a odoberania. Prístup predajcov a servisných partnerov sa podrobne opíše v politike.

Politika definuje inštaláciu softvéru v operačných systémoch vrátane prístupu vývojárov k aktualizáciám a záplatám.

V prípade potreby sa v politike opíše generovanie a využívanie testovacích údajov.

Bezpečnostné opatrenia

Kontrola prevádzkového softvéru

Aby sa minimalizovalo riziko poškodenia prevádzkových systémov, mali by sa pri kontrole zmien zohľadniť nasledujúce témy:

- aktualizáciu prevádzkového softvéru, aplikácií a programových knižníc vykonávajú správcovia IT

na základe interných procesov IT.
- Používatelia nesmú inštalovať softvér, ktorý nie je schválený vývojárom.
- Proces pridávania nového softvéru by mal zahŕňať definované scenáre testovania a vydávania.
- Záplaty a aktualizácie by sa mali poskytovať včas. V produkčných prostrediach by sa mali definovať servisné okná, ktoré umožnia aktualizácie vysoko dostupných systémov.

Pri každom rozhodnutí o prechode na novú verziu by sa mali zohľadniť obchodné požiadavky na zmenu a bezpečnosť verzie, t. j. zavedenie nových bezpečnostných funkcií alebo počet a závažnosť bezpečnostných problémov, ktoré sa týkajú tejto verzie.

Fyzický alebo logický prístup pre dodávateľov by sa mal udeliť len na účely podpory na nevyhnutný čas. Činnosti dodávateľa sa monitorujú.

Počítačový softvér sa môže spoliehať na externe dodávaný softvér a moduly, ktoré by sa mali monitorovať a kontrolovať, aby sa zabránilo neoprávneným zmenám, ktoré by mohli spôsobiť bezpečnostné nedostatky.

Ochrana testovacích údajov systému

Testovacie údaje sa starostlivo vyberajú, chránia a kontrolujú.

Je potrebné vyhnúť sa používaniu prevádzkových databáz obsahujúcich citlivé informácie na účely testovania. Ak sa na účely testovania musia použiť citlivé informačné systémy, všetky citlivé údaje a obsah by sa mali pred použitím odstrániť alebo upraviť na nepoznanie.

Kontrola prístupu k zdrojovému kódu programu

Prístup k zdrojovému kódu programu a súvisiacim položkám (ako sú vývojové nástroje, testovacie prípady atď.) by mal byť prísne kontrolovaný, aby sa zachovala integrita TOE.

TOE a jeho časti sa riadia systémom CM.

9.6.6 Bezpečnosť v procesoch vývoja a podpory

Cieľ

Bezpečnosť aplikácií, nástrojov a informácií sa zachováva.

Bezpečnostné aplikácie a aplikácie s vplyvom na TOE sa kontrolujú.

Aplikácie vyvinuté vývojárom alebo v jeho mene musia byť plne v súlade so špecifikáciou a nesmú obsahovať žiadne bezpečnostné nedostatky.

Zásady

Proces vydávania vývojových aplikácií a nástrojov musí byť zdokumentovaný.

Musí byť definovaná a účinná politika riadenia zmien.

Zachovanie dôvernosti v aplikáciách, nástrojoch a sieťach sa zdokumentuje.

Bezpečnostné opatrenia

Postupy kontroly zmien

Postupy kontroly zmien musia byť zdokumentované a presadzované s cieľom minimalizovať poškodenie informačných systémov. Zavádzanie nových systémov a významných zmien existujúcich systémov by sa malo riadiť formálnym procesom dokumentácie, špecifikácie, testovania, kontroly kvality a riadenej implementácie.

Tento proces by mal zahŕňať posudzovanie rizík, analýzu vplyvu zmien a špecifikáciu potrebných bezpečnostných kontrol. Tento proces by mal tiež zabezpečiť, aby neboli ohrozené existujúce bezpečnostné a kontrolné postupy, aby mali podporní programátori prístup len k tým častiam systému, ktoré sú potrebné pre ich prácu, a aby sa získala formálna dohoda a schválenie každej zmeny.

Technická kontrola aplikácií po zmenách operačného systému

Pri zmene operačných systémov alebo aplikácií sa monitorujú kritické aplikácie, aby sa zabezpečilo, že nedôjde k negatívnemu vplyvu na bezpečnosť.

Pridelí sa zodpovednosť za monitorovanie zraniteľností a vydávanie záplat a opráv zo strany dodávateľov.

Obmedzenia týkajúce sa zmien softvérových balíkov

Úpravy softvérových balíkov s vplyvom na TOE a jeho časti (napr. vývojové nástroje, testovacie prípady) by sa nemali vykonávať, mali by sa obmedziť na nevyhnutné zmeny a všetky zmeny by sa mali prísne kontrolovať.

Softvérové balíky dodávané dodávateľom by sa mali používať bez úprav, pokiaľ je to možné a uskutočniteľné. Ak sú potrebné zmeny, pôvodný softvér by sa mal zachovať a zmeny by sa mali aplikovať na jasne identifikovanú kópiu. Mal by sa zaviesť proces správy aktualizácií softvéru, aby sa zabezpečilo, že pre všetok autorizovaný softvér budú nainštalované najaktuálnejšie schválené opravy a aktualizácie aplikácií. Všetky zmeny by mali byť plne otestované a zdokumentované, aby ich bolo možné v prípade potreby opätovne aplikovať na budúce aktualizácie softvéru.

Únik informácií

Ak sa vyžaduje dôvernosť informácií, je potrebné zabrániť možnostiam úniku informácií. Externý vývoj softvéru (informatívne)

Vývojár by mal monitorovať a kontrolovať externe zadávaný vývoj softvéru.

Ak sa vývoj softvéru zadáva externe, mali by sa zohľadniť tieto body:

- licenčné dohody, vlastníctvo kódu a práva duševného vlastníctva;
- dohody o úschove v prípade zlyhania tretej strany;
- zmluvné požiadavky na kvalitu a bezpečnosť kódu;
- testovanie pred inštaláciou s cieľom odhaliť škodlivý kód.

Príklady

V typickej oblasti s vysokým stupňom zabezpečenia je prenos odchádzajúcich údajov obmedzený na určené osoby a zaznamenaný. Ak je používanie mobilných dátových médií, napr. zariadení USB, nevyhnutné, je obmedzené na osoby so schválenými oprávneniami, napr. pomocou nástrojov na ochranu portov. Údaje sa pred opustením zabezpečenej siete zašifrujú. Na kontrolu vývoja softvéru sa široko používajú postupy bezpečného životného cyklu vývoja.

9.6.7 Technické riadenie zraniteľnosti (informatívne)

Cieľ

Riziká vyplývajúce zo zneužitia zverejnených technických zraniteľností by sa mali zmierniť.

Zásady

Zásady by mali podrobne popisovať prístup vývojára k aktualizáciám a opravám.

Bezpečnostné opatrenia

Existujú dve hlavné odlišné témy: zverejnené technické zraniteľnosti zakúpeného softvéru a systémov a vlastnoručne vyvinuté systémy s nesprávnou implementáciou bezpečnostných opatrení.

Mali by sa včas získať informácie o technických zraniteľnostiach používaných informačných systémov, vyhodnotiť vystavenie vývojára takýmto zraniteľnostiam a prijať vhodné opatrenia na riešenie súvisiacich rizík.

Ak sa vyžaduje dôvernosť a/alebo integrita, bezpečnosť by mala byť neoddeliteľnou súčasťou projektov vývoja softvéru a systémov.

9.7 Riadenie incidentov informačnej bezpečnosti

9.7.1 Celkový cieľ

Účinné riadenie incidentov informačnej bezpečnosti zabezpečuje primeranú úroveň bezpečnosti.

9.7.2 Hlásenie udalostí a nedostatkov v oblasti informačnej bezpečnosti

Cieľ

Všetky incidenty a nedostatky súvisiace s bezpečnosťou sa nahlasujú bezpečnostnému manažérovi spôsobom, ktorý umožňuje včasné nápravné opatrenia, ktoré sa majú prijať.

Zásady

Vývojár musí mať politiku riadenia bezpečnostných incidentov, ktorá poskytuje vhodné postupy spätnej väzby na zabezpečenie včasnej komunikácie o bezpečnostných incidentoch. Mali by byť definované najmä minimálne kritériá na nahlásenie udalosti.

Bezpečnostné opatrenia

Udalosti týkajúce sa informačnej bezpečnosti sa čo najrýchlejšie nahlasujú prostredníctvom príslušných riadiacich kanálov

Všetci zamestnanci, dodávatelia a používatelia informačných systémov a služieb z radov tretích strán sú povinní zaznamenať a nahlásiť akékoľvek zistené alebo podozrivé bezpečnostné nedostatky v systémoch alebo službách.

Správa sa adresuje bezpečnostnému manažérovi, podľa možnosti s dôkazmi. V závislosti od kontextu môže byť potrebné reagovať okamžite, alebo počkať na rozhodnutie bezpečnostného manažéra.

9.7.3 Riadenie incidentov a zlepšení v oblasti informačnej bezpečnosti

Cieľ

Incidenty informačnej bezpečnosti sa účinne riešia a zlepšenia sa zavádzajú včas.

Zásady

Stanovia sa povinnosti a postupy riadenia, aby sa zabezpečila rýchla, účinná a riadna reakcia na bezpečnostné incidenty.

Bezpečnostné opatrenia

Všetky bezpečnostné incidenty sa okamžite nahlasujú bezpečnostnému manažérovi. Okrem okamžitého riešenia sa všetky reakcie na bezpečnostné incidenty dohodnú s bezpečnostným manažérom.

Každý bezpečnostný incident by sa mal zdokumentovať v zabezpečenom prostredí s kontrolovaným prístupom. Záznamy by sa mali uchovávať.

Incidenty informačnej bezpečnosti by sa mali analyzovať, mali by sa z nich odvodiť nápravné a preventívne opatrenia a výsledky by sa mali uvádzať v pravidelnej bezpečnostnej správe.

Príklady

V príslušnej politike sú opísané očakávané typy incidentov, príslušné opatrenia na ich zvládnutie a zmiernenie. Typy, objemy a náklady na incidenty informačnej bezpečnosti sa kvantifikujú a monitorujú.

Ak následné konanie proti osobe alebo organizácii po bezpečnostnom incidente zahŕňa právne kroky (občianskoprávne alebo trestnoprávne), dôkazy sa zhromažďujú, uchovávajú a predkladajú v súlade s pravidlami pre dôkazy stanovenými v príslušných jurisdikciách (napr. trestný poriadok, právne predpisy o ochrane osobných údajov, účasť zamestnaneckej rady).

9.8 Riadenie kontinuity činností

9.8.1 Celkový cieľ

Riadenie kontinuity činností zabezpečuje nepretržitú dostupnosť procesov, systémov a nástrojov potrebných na udržanie požadovanej úrovne bezpečnosti a/alebo integrity TOE a jeho časti.

9.8.2 Bezpečnostné aspekty riadenia kontinuity činností

Cieľ

V prípade incidentov sa zachováva integrita a v prípade potreby aj dôvernosť TOE a jeho častí, nehody a krízové situácie.

Zásady

Pre kontinuitu činností v celej organizácii sa vytvorí a udržiava riadený proces, ktorý rieši bezpečnostné požiadavky.

Plány kontinuity činností sa zdokumentujú a zavedú s cieľom zachovať alebo obnoviť prevádzku a zabezpečiť dostupnosť informácií na požadovanej úrovni a v požadovanom časovom rozsahu po prerušení alebo zlyhaní bezpečnostne relevantných procesov.

Bezpečnostné opatrenia

Vývojár je zodpovedný za plánovanie kontinuity činností v príslušnom podniku v rámci svojej podnikateľskej zodpovednosti. Všetky existujúce systémy, štruktúry a procesy projektovania, výroby, logistiky a dodávateľského reťazca musia plánovať dostatočnú pohotovosť na primerané zmiernenie účinkov katastrof, prerušenia činnosti a/alebo rizík identifikovaných v súlade s postupmi posudzovania rizík.

Identifikujú sa udalosti, ktoré môžu spôsobiť prerušenie obchodných procesov, spolu s pravdepodobnosťou a vplyvom takýchto prerušení a ich dôsledkami pre TOE alebo jeho časti.

Pokiaľ ide o IT a informačnú bezpečnosť, proces by sa mal týkať ochrany siete, počítačových centier vrátane hardvéru, systémov kontroly prístupu a monitorovacích a poplašných systémov.

Ak sa vyžaduje dôvernosť, pozornosť sa venuje ochrane TOE v prípade incidentu. To by malo okrem iného zahŕňať:

- Automatické vypínanie IT systémov;
- Automatické zatváranie núdzových východov;
- Nasadenie dodatočného bezpečnostného personálu.

Mal by sa zachovať jednotný rámec plánov kontinuity činností, aby sa zabezpečila konzistentnosť všetkých plánov, dôsledné riešenie bezpečnostných požiadaviek a určenie priorít pre testovanie a údržbu.

Plány kontinuity činností by sa mali pravidelne testovať a aktualizovať, aby sa zabezpečila ich aktuálnosť a účinnosť.

9.9 Súlad (informatívne)

Cieľ

Malo by sa predchádzať porušovaniu akýchkoľvek zákonných, regulačných alebo zmluvných povinností súvisiacich s TOE.

Zásady

V politike by mal byť podrobne opísaný prístup vývojárov k identifikácii príslušných právnych predpisov, zákonných, regulačných a zmluvných požiadaviek, práv duševného vlastníctva tretích strán a iných platných predpisov.

Bezpečnostné opatrenia

Je potrebné identifikovať príslušné právne predpisy, zákonné, regulačné a zmluvné požiadavky, práva duševného vlastníctva tretích strán a iné platné predpisy.

Vývojár by mal touto úlohou poveriť vhodne vyškolených zamestnancov alebo využiť externých poskytovateľov služieb.

29. PRÍLOHA 3: UPLATNENIE CC NA INTEGROVANÉ OBVODY

ÚČEL

V tejto prílohe sa uvádza podrobné uplatnenie všetkých tried bezpečnostných záruk na konkrétny typ produktov, t. j. integrované obvody.

KONKRÉTNY STAV

Žiadne.

KRÍŽOVÝ ODKAZ NA KAPITOLU(-Y), V KTOREJ(-ÝCH) SÚ TIETO PRVKY VYHLÁSENÉ ZA UPLATNITEĽNÉ

Kapitola 8, ŠPECIFICKÉ KRITÉRIA A METÓDY HODNOTENIA.

1 ÚVOD

Zložité mikročipy, ktoré dokážu spracúvať informácie, bohužiaľ prinášajú riziká a nebezpečenstvá, ale aj obrovské výhody. Závislosť na bezproblémovom fungovaní, ako aj na efektívnosti ochranných opatrení, ktoré boli vykonané na úrovni systému a čipu, veľmi vzrástla.

Je preto potrebné uvedomiť si, že sa rozšírili možnosti testovania dôležitých informačných systémov vrátane hardvéru podľa prijatých kritérií, aby boli bezpečnostné záruky opatrení transparentnejšie pre výrobcu, prevádzkovateľa a používateľa.

Táto príloha slúži ako príručka na uplatňovanie CC na hardvérové komponenty v súvislosti s integrovanými obvodmi. Tento dokument bude zaujímavý najmä pre výrobcov, hodnotiteľov a certifikátorov.

1.1 Cieľ

Bezpečnostné vlastnosti hardvérových aj softvérových produktov možno certifikovať v súlade s CC. S cieľom dosiahnuť spoločné porozumenie a zabezpečiť, aby sa CC používal pre hardvérové integrované obvody spôsobom, ktorý je v súlade so „state of the art“ hodnotenia hardvéru, poskytujú nasledujúce kapitoly okrem spoločnej metodiky hodnotenia [CEM] aj usmernenie k jednotlivým aspektom pracovných balíkov záruky CC.

Toto usmernenie sa vzťahuje na hardvér jednotlivých integrovaných obvodov. Zahŕňa úrovne záruky definované v CC, t. j. EAL1 až EAL5. Ide o hodnotenia úrovne, ktoré sa dnes používajú pre hardvérové integrované obvody. Toto usmernenie sa zaoberá najmä súčasnými úrovňami IC EAL4 až EAL5
a rozšíreniami, ako je AVA_VAN.5.

1.2 Slovník

Nasledujúce pojmy sú definované v časti 1 CC.

BiCMOS Bipolárny komplementárny polovodič na báze oxidu kovu, špecifická polovodičová technológia

CAD Počítačom podporovaný dizajn

CMOS Komplementárne polovodiče na báze oxidov kovov, špecifická polovodičová technológia

Die	jednotlivý integrovaný obvod na waferi (množné číslo "kocky")
EPROM	Erasable Programmable Read Only Memory
E2PROM	Elektricky vymazateľná programovateľná pamäť
HDL	Jazyk na opis hardvéru
HW	Hardvér
IC	Integrovaný obvod, integrované elektronické obvody v mikročipe
SW	Softvér
Wafer	Kremíkový plátok na výrobu čipov

2 POŽIADAVKY NA BEZPEČNOSTNÚ ZÁRUKU INTEGROVANÝCH OBVODOV

2.1 Úvod

Pri uplatňovaní CC na hardvérové komponenty možno uvažovať o dvoch typoch objektov hodnotenia (TOE):

- TOE vyrobený zo série diskrétnych súčiastok na doske plošných spojov alebo ako hybrid prostredníctvom rôznych alebo viacerých kociek na jednom nosiči;
- TOE vyrobený ako samostatný integrovaný obvod (IC).

Nasledujúce usmernenie týkajúce sa aspektov bezpečnostnej záruky CC pre TOE sa vzťahuje na hardvér jednotlivých integrovaných obvodov.

Logické funkcie v integrovanom obvode môžu byť vo všeobecnosti implementované v jednoduchých štruktúrach PLD (Programmable Logic Device), štruktúrach FPGA (Field Programmable Gate Array), ako ASIC (Application Specific Integrated Circuit) alebo ako zákaznícky integrovaný obvod.

Pokiaľ ide o bezpečnostné aplikácie, inteligentné pamäťové integrované obvody s pevne zabudovanou bezpečnostnou logikou (napr. karty verejnej dopravy, kontrola prístupu do budov alebo integrované obvody založené na mikrokontroléroch v konštrukcii ASIC (napr. integrované obvody elektronických peňaženiek) sa používajú najmä na základné komponenty bezpečnostnej funkcionality.

Súčasná pamäť v integrovaných obvodoch je založená na bunkách EPROM, E2PROM alebo flash. To umožňuje nevolatilné ukladanie údajov. Bezpečnostnú logiku možno využiť na implementáciu identifikácie a autentizácie, kontroly prístupu a vnútorných sekvenčných kontrol IC.

Integrované obvody na báze mikrokontrolérov ponúkajú možnosť vykonávať nezávisle komplexné procesy riadené operačným systémom integrovaného obvodu. Položky, ktoré tiež patria k uvedenej funkčnosti, zahŕňajú funkcie a služby zodpovednosti, ako je šifrovanie, generovanie náhodných čísel a digitálny podpis, funkčnosť, ktorá je implementovaná v hardvéri aj softvéri.

Mechanizmy ochrany softvéru a operačných údajov v rôznych pamätiach a vnútorných sekvenciách sa realizujú prostredníctvom hardvéru integrovaného obvodu (napr. prostredníctvom určitých technických opatrení a technologických prvkov) s cieľom podporiť logickú funkčnosť.

Operačný systém mikrokontroléra IC je obsiahnutý (umiestnený) v pamäti ROM a/alebo E2PROM a je chránený pred odhalením a modifikáciou počas prevádzkovej fázy technickými alebo technologickými vlastnosťami hardvéru. Zatiaľ čo technologické vlastnosti sú vlastné TOE, technické vlastnosti závisia od konštrukcie TOE.

2.2 Prístup CC k hodnoteniu

CC predpisuje celý rad činností bezpečnostných záruk, ako sú špecifické TOE, analýza návrhu, dokumentácia návodu, analýza zraniteľnosti, penetračné testy na jednej strane a preskúmanie rozvojového a produkčného prostredia na strane druhej. Aj keď existujú rozdiely v používanej terminológii, v zásade sú si tieto dva súbory kritérií veľmi podobné, pokiaľ ide o špecifikáciu požiadaviek bezpečnostných záruk a ich základnú filozofiu.

Jedinečnou vlastnosťou CC je zavedenie koncepcie ochranného profilu. Ochranný profil možno

charakterizovať ako všeobecný bezpečnostný zámer pre konkrétnu triedu TOE (napr. bezpečnostné IC, ako v prípade [BSI-CC- PP-0084-2014][34], ktorý definuje uznávanú normu, na ktorú možno uplatniť nárok na zhodu. Hoci nie je povinné vyhlasovať zhodu s ochranným profilom , dostupnosť takýchto noriem poskytuje možnosť opätovne použiť hodnotený materiál v bezpečnostnom zámere, čím sa vývojárovi výrazne uľahčuje proces tvorby tohto konkrétneho hodnotiaceho výstupu. Pre používateľa zhoda
s jedným PP viacerými ST (t. j. rôznymi produktmi) umožňuje porovnávať tieto produkty na rovnakom základe. Najmä v prípade, že pre danú oblasť existuje jeden dobre zavedený ochranný profil , ide o silný mechanizmus, ktorý používateľovi poskytuje väčší výber a lepšiu hospodárnosť.

Ochranný profil (PP) môže byť definovaný, hodnotený a certifikovaný pred skutočným hodnotením TOE a môže byť uvedený v rámci bezpečnostného zámeru skutočného hodnotenia TOE. Existujú dva typy zhody: preukázateľná a prísna. V preukázateľnom prípade sa tvrdí, že požiadavky bezpečnostných funkcionalít (SFR) bezpečnostného zámeru sú podobné požiadavkám v PP. V prípade prísnej zhody je ST v súlade s PP len vtedy, ak je v súlade so všetkými časťami PP. V PP, na ktorý sa odkazuje, sa stanovuje požadovaná úroveň zhody. V oblasti bezpečnostných IC je najbežnejšia prísna zhoda.

Nasledujúce kapitoly obsahujú usmernenia pre hardvérové TOE, ktoré sa musia hodnotiť podľa spoločných kritérií (CC).

Hodnotenie IC zahŕňa tieto činnosti:

- Bezpečnostný zámer
- Vývoj
- Skúšky
- Usmernenie vrátane prevádzky
- Podpora počas celého životného cyklu vrátane správy konfigurácie a dodávok
- Posudzovanie zraniteľnosti.

Uvedené činnosti zodpovedajú určitým triedam záruk definovaným v časti 3 CC. V nasledujúcej tabuľke je uvedené rozdelenie a mapovanie tried záruk/skupín záruk.

[34] Ochranný profil bezpečnostnej platformy IC s rozširujúcimi balíkmi.

Tabuľka 1 Rozdelenie a mapovanie skupiny záruk

Trieda záruk	Skupina záruk	Skrátený názov
Trieda APE: Hodnotenie ochranného profilu		APE[35]
Trieda ASE: Hodnotenie bezpečnostných zámerov		ASE[36]
Trieda ADV: Vývoj	Bezpečnostná architektúra Funkčná špecifikácia TOE návrh Zobrazenie implementácie Vnútorné TSF (Trusted Security Functions) Modelovanie bezpečnostnej politiky	ADV_ARC ADV_FSP ADV_TDS ADV_IMP ADV_INT ADV_SPM
Trieda ATE: Skúšky	Pokrytie Hĺbka Funkčná skúška Nezávislé skúšanie	ATE_COV ATE_DPT ATE_FUN ATE_IND
Trieda AGD: Sprievodná dokumentácia	Používateľská príručka Postup prípravy	AGD_OPE AGD_PRE
Trieda ALC: Podpora životného cyklu	Schopnosti CM Rozsah CM Dodávka Bezpečnosť vývoja Odstraňovanie chýb Definícia životného cyklu Nástroje a techniky	ALC_CMC ALC_CMS ALC_DEL ALC_DVS ALC_FLR ALC_LCD ALC_TAT
Trieda AVA: Posudzovanie zraniteľnosti	Analýza zraniteľnosti	AVA_VAN

Skupiny záruk CC sú rozdelené do určitých hierarchických komponentov záruk. Tieto komponenty sú zamerané na vopred definované balíky hodnotenia úrovní záruky (EAL) (EAL1 až EAL7). Kombinácia určitých komponentov záruk vytvára jeden z preddefinovaných balíkov EAL, ako je uvedené v CC časť 3, kapitola 8.

Na vykonanie hodnotenia TOE sa môže použiť balík EAL, ktorý je vopred definovaný CC (v súlade s časťou 3). Okrem toho je možné balík EAL rozšíriť alebo rozšíriť (podrobnosti nájdete v CC, časť 1).

Nasledujúca diskusia poskytuje návod, ako používať komponenty záruk CC časť 3 triedy záruk pre hardvérové IC TOE (napr. bezpečnostnú platformu IC).

Na hodnotenie TOE sa odporúča použiť jeden z preddefinovaných balíkov EAL. Vo väčšine prípadov je pre hodnotenie hardvérového integrovaného obvodu (napr. bezpečnostnej platformy integrovaného obvodu) potrebné rozšírenie vybraného balíka EAL, aby sa splnili špecifické ciele (napr. pre posúdenie zraniteľnosti na vysokej úrovni). V takom prípade musia byť splnené všetky požiadavky na závislosť, ako sú uvedené v časti 3 CC. Nasledujúca diskusia sa bude týkať aspektov rozšírenia v rámci príslušných odsekov.

2.3 Ochranný profil CC (trieda APE)

Na rozdiel od ST, ktorý opisuje implementačne orientovanú bezpečnosť, PP opisuje abstraktné bezpečnostné požiadavky. Napríklad požiadavka na generátor náhodných čísel (RNG) s nešpecifikovanou kvalitou by mohla byť vyjadrená v PP a vyhovujúci ST by potom mohol uvádzať, na akej úrovni kvality konkrétny TOE poskytuje náhodné čísla.

Väčšina usmernení platných pre ST platí rovnako dobre aj pre PP (pozri nasledujúcu kapitolu), napríklad definícia rozsahu a hraníc TOE, environmentálne predpoklady, hrozby, bezpečnostné ciele.

Referenčný PP týkajúci sa IC a v súlade s CC je [BSI-CC-PP-0084-2014]. Vypracovala ho komunita výrobcov polovodičov a využíva bohaté skúsenosti v oblasti bezpečnosti smart kariet. Ďalšie PP nájdete na webovej stránke o európskych certifikačných schémach kybernetickej bezpečnosti, ktorú

[35] Trieda záruk APE je rozdelená do niekoľkých skupín (pozri časť 3 CC).
[36] Trieda záruk ASE sa delí na niekoľko skupín (pozri časť 3 CC).

spravuje agentúra ENISA.

2.4 CC Bezpečnostný zámer (trieda ASE)

2.4.1 Ciele

Bezpečnostný zámer (ST) pre TOE je základom pre hodnotenie a dohodne sa na ňom vývojár a hodnotiteľ. Publikum, ktorému je ST určený, sa neobmedzuje len na osoby zodpovedné za výrobu TOE a jeho hodnotenie, ale môže zahŕňať aj osoby zodpovedné za riadenie, marketing, nákup, inštaláciu, konfiguráciu, prevádzku a používanie TOE.

V prílohe A k časti 1 CC sa podrobne opisujú požiadavky na obsah a prezentáciu ST.

Bezpečnostný zámer zahŕňa:

- presný opis bezpečnostného problému, ktorý rieši TOE, a jeho prostredia z hľadiska hrozieb, všetkých predpokladov, organizačných bezpečnostných politík a zamýšľaného použitia;
- opis bezpečnostných cieľov pre TOE a pre prostredie s cieľom určiť, či bezpečnostné ciele čelia identifikovaným hrozbám, dosahujú identifikované organizačné bezpečnostné politiky a dodržiavajú stanovené predpoklady.
- Nároky na ochranný profil, ak existujú;
- opis požiadaviek bezpečnostných funkcionalít a požiadaviek bezpečnostných záruk TOE;
- súhrnnú špecifikáciu toho, ako TOE implementuje požiadavky bezpečnostných funkcionalít;
- odôvodnenie, ktoré poskytuje zdôvodnenie transformácie bezpečnostného problému na bezpečnostné ciele a bezpečnostné požiadavky.

V nasledujúcich častiach sú uvedené pripomienky týkajúce sa jednotlivých požiadaviek.

2.4.2 Vstup

Vývojár poskytne dokument "Bezpečnostný zámer".

2.4.3 Požiadavky

Popis TOE

Bezpečnostný zámer musí obsahovať presný opis objektu hodnotenia (TOE) z hľadiska hardvéru, softvérových a firmvérových komponentov. Dôležitý je aj odkaz na technologické parametre. V opise TOE sa výslovne uvedie povaha akéhokoľvek špecializovaného testovacieho softvéru (buď vstavaného softvéru, alebo softvéru mimo integrovaného obvodu).

Opíšu sa aj všeobecné bezpečnostné charakteristiky hardvéru. Vhodné by bolo uviesť odkaz na technický list hardvéru. Uvedú sa všetky možné konfigurácie alebo zamýšľané použitie čipu.

TOE musí byť jasne identifikovaná a oddelená od svojho technického a prevádzkového prostredia. ST musí jednoznačne odkazovať na TOE.

Keďže hardvérové časti integrovaného obvodu je fyzicky aj funkčne ťažké od seba oddeliť bez ďalších informácií, nie je možné vylúčiť časti hardvéru z TOE; preto je rozumné definovať celý hardvér integrovaného obvodu ako TOE. V prípade, že niektoré časti integrovaného obvodu sú mimo TOE, musí existovať jasné logické a fyzické rozhranie. Vhodné je zahrnúť do TOE softvér/firmvér, ktorý je silne hardvérovo orientovaný. Bolo by rozumné pozrieť sa na IC ako na celok a nielen na hardvér alebo len na softvér.

Bezpečnostné prostredie

Bezpečnostné prostredie TOE zahŕňa prevádzkové prostredie po dodaní, ako aj technické prostredie v rôznych fázach životného cyklu TOE.

Preto sa vyžaduje presný opis životného cyklu TOE alebo by sa naň malo odkazovať. Musia sa definovať hranice TOE z hľadiska životného cyklu.

V bezpečnostnom zámere sa výslovne uvedie, ktoré fázy životného cyklu patria do rozsahu hodnotenia a ktoré sú z neho vylúčené; fázy, v ktorých sa TOE vyvíja a vyrába, vždy patria do rozsahu hodnotenia.

Na rozdiel od čisto softvérových TOE, ako je to v uvedených prípadoch, je toto určenie možné len s presnými znalosťami výrobného procesu. Toto tvrdenie má však priamy vplyv aj na scenáre hrozieb a útokov pri prevádzke TOE, ktoré by sa mohli prijať v rámci hodnotenia TOE. V prípade integrovaného obvodu TOE by hranica pre hodnotenie mohla byť po testovaní integrovaného obvodu ako matrice (najskôr) alebo po dokončení balenia a súvisiacich testov. Prípadne môže bezpečnostný zámer zahŕňať ďalšie fázy IC, ako je montáž mikromodulov, fázy pred personalizáciou a personalizácia.

V CC sa výslovne vyžaduje, aby sa hrozby charakterizovali z hľadiska identifikovaného pôvodcu hrozby, ohrozeného aktíva a útoku. Preto je potrebné definovať a vymenovať všetky subjekty z hľadiska rolí
a aktív, pre ktoré je potrebná špecifická ochrana buď zo strany TOE, alebo jeho prostredia, a s odkazom na fázy životného cyklu TOE.

Je potrebné identifikovať všetky predpoklady kladené na prostredie, ktoré musí TOE alebo jeho prostredie spĺňať.

Predpoklady týkajúce sa fungovania softvéru, ktorý nie je súčasťou TOE, sú nevyhnutné. Môžu zahŕňať:

- softvér na ochranu integrity, napr. na reakciu na senzory alebo na prerušenia časovača watchdog;
- implementácia algoritmov, ktoré sú odolné voči DPA;
- softvér na spracovanie chýb (napr. ochrana proti vyvolaniu chýb, aby sa umožnil útok diferenciálnou analýzou chýb na kryptografické kľúče).

Pokiaľ ide o prevádzkovú fázu TOE, opíšu sa všetky predpoklady týkajúce sa bezpečnostných aspektov prostredia, v ktorom sa TOE bude používať alebo sa má používať. Vo všeobecnosti pre bezpečnostný IC nie je potrebné definovať žiadny špecifický predpoklad pre TOE a jeho prostredie počas fázy koncového užívateľa (prevádzkové prostredie), pretože toto prostredie je verejné. Ak však TOE pozostáva len z hardvéru IC, môžu existovať dôležité bezpečnostné predpoklady pre fázu používania TOE.

Pokiaľ ide o fázy životného cyklu, ktoré sú mimo rozsahu hodnotenia, mali by existovať informácie o tom, kto môže TOE po dodaní používať a v akých prevádzkových režimoch je možné ho používať. V tejto súvislosti je potrebné preskúmať činnosti všetkých pracovníkov, ktorí prichádzajú do kontaktu s TOE po dodaní. Preto je potrebné definovať konkrétne predpoklady správania sa takéhoto personálu a identifikovať príslušné operačné úlohy. Poznámka: hardvér môže pridať rôzne úlohy, ktoré sú špecifické pre IC, napr. môžu existovať rôzne prístupy k personalizácii a aktivovaniu; takéto úlohy špecifické pre hardvér môže byť potrebné zdokumentovať mimo ST.

Ako príklad konkrétnych aktív pre bezpečnostný IC to môže zahŕňať:

- špecifické údaje IC vrátane personalizačných údajov a kryptografických kľúčov,
- vstavaný softvér pre smart karty,
- špecializovaný softvér IC,
- špecifické aplikačné údaje, ako sú kľúče, autentizačné údaje alebo informácie o riadení prístupu.

Mohlo by byť užitočné rozlišovať medzi primárnymi aktívami - ako sú údaje uložené a prevádzkované vstavaným softvérom bezpečnostného integrovaného obvodu, samotný vstavaný softvér bezpečnostného integrovaného obvodu, keď je uložený a v prevádzke, a bezpečnostné služby poskytované TOE pre vstavaný softvér bezpečnostného integrovaného obvodu - a sekundárnymi aktívami, ktoré by sa v prípade kompromitácie mohli zneužiť na kompromitáciu primárneho aktíva. Sekundárne aktíva nemajú žiadnu vlastnú hodnotu ako také, ale ich hodnota sa odvodzuje od primárnych aktív. Toto rozlíšenie by umožnilo oddeliť aktíva vysokej a nízkej úrovne, čo by zasa pomohlo štruktúrovať vyhlásenie o hrozbách, a tým viedlo k lepšiemu pochopeniu bezpečnostných cieľov a bezpečnostných požiadaviek, ktoré má IC spĺňať.

CC však neukladajú povinnosť identifikovať aktíva nízkej úrovne alebo sekundárne aktíva, aby sa nimi riadil výber bezpečnostných cieľov a požiadaviek. Napríklad SFR na ochranu integrity sa môžu zahrnúť jednoducho preto, aby pomohli dosiahnuť bezpečnostný cieľ ochrany vysokoúrovňového alebo primárneho aktíva - s odôvodnením bezpečnostných požiadaviek, ktoré vysvetľuje účel takýchto SFR.

Opíšu sa predpokladané hrozby pre aktíva. KÚ vyžadujú, aby hrozby definované v ST, neboli zamerané na identifikované bezpečnostné ciele, ale aby boli riešené bezpečnostnými cieľmi. Treba tiež poznamenať, že CC výslovne vyžaduje, aby sa hrozby charakterizovali z hľadiska identifikovaného pôvodcu hrozby, ohrozeného aktíva a útoku (opisujúc také aspekty, ako sú použité metódy útoku, využité zraniteľnosti a príležitosti).

Ide o opis škôd na majetku, a nie o opis ciest útoku, ktoré nebolo možné v ST dokončiť. Hrozby by sa mohli opísať v zmysle:

- neoprávnené zverejnenie majetku;
- neoprávnené používanie majetku;
- neoprávnené úpravy majetku.

Aby bolo možné pochopiť hrozby definované pre prostredie TOE v určitých fázach životného cyklu, musí byť opísané rozvojové a produkčné prostredie TOE.

Okrem logických funkcií môžu byť počas prevádzkovej fázy TOE napadnuté aj technické a technologické vlastnosti. Preto je možné formulovať zodpovedajúce hrozby pre definované aktíva (napr. výber objektov aj prostredníctvom fyzických útokov, prevádzka TOE mimo špecifických parametrov, ako je napätie, frekvencia a teplota).

Pokiaľ ide o určenie konkrétnych hrozieb, je potrebné poznamenať, že útoky na IC počas výrobných procesov, a najmä počas fáz testovania, sú možné a musia sa zohľadniť pre príslušné fázy životného cyklu v rámci príslušnej triedy záruk ALC. Môžu viesť k zraniteľnostiam pri vývoji TOE, ktoré hodnotiteľ identifikuje počas vykonávania hodnotiacich činností pre triedu ALC.

Špecifikácie organizačných bezpečnostných politík v podstate závisia od aplikácií, do ktorých je TOE začlenená. Vo všeobecnosti platí, že pri hodnotení čisto hardvérového bezpečnostného IC nie je potrebné definovať žiadnu špecifickú organizačnú bezpečnostnú politiku.

Bezpečnostné ciele

CC vyžaduje, aby boli v rámci ST špecifikované bezpečnostné ciele pre TOE aj prostredie, ktoré sú potrebné na boj proti hrozbám a na dodržanie identifikovaných predpokladov a bezpečnostných politík organizácie.

Ciele musia byť jasne stanovené tak, aby bolo možné ich jasne priradiť k príslušným hrozbám. Mohli by byť odvodené z nasledujúcich bodov:

- odolnosť voči fyzickej manipulácii;
- odolnosť proti fyzickej sonde;
- ochrana pred únikom informácií (prirodzeným aj spôsobeným útočníkom);
- ochrana testovacej funkcie;
- ukladanie údajov testovacím personálom;
- poskytovanie náhodných čísel.

Technické a technologické vlastnosti IC nad rámec cieľov, t. j. tie, ktoré zabezpečujú vlastnú ochranu, sa budú riešiť v rámci hodnotiacej činnosti ADV_ARC. Autor ST sa môže rozhodnúť, že tieto vlastnosti zdôrazní používateľom v súhrnnej špecifikácii TOE (ako súčasť ASE_TSS.2).

Okrem toho môžu byť potrebné špecifické bezpečnostné ciele pre prostredie, aby sa zabezpečilo, že sa dodržia predpoklady týkajúce sa závislostí od softvéru.

Bezpečnostné ciele pre prostredie v rámci určitých fáz životného cyklu môžu byť splnené opatreniami pre prostredie TOE vyhodnotenými požiadavkami bezpečnostných záruk procesu vývoja TOE. (napr. bezpečnosť vývoja).

Bezpečnostné požiadavky

Bezpečnostné požiadavky sa definujú v rámci ST s použitím funkčných komponentov a komponentov záruk špecifikovaných v častiach 2 a 3 CC. V niektorých prípadoch, ak nie sú použiteľné preddefinované komponenty funkcionalít časti 2 CC, môžu sa v rámci ST definovať nové komponenty špecifické pre IC.

Vyžaduje sa, aby boli požiadavky bezpečnostných funkcionalít (SFR) a požiadavky bezpečnostných záruk (SAR) na TOE potrebné na splnenie identifikovaných bezpečnostných cieľov TOE.

SAR

Požadovaná úroveň potenciálu útoku pre analýzu zraniteľnosti je vyjadrená v požiadavkách CC výberom určitého komponentu záruk AVA_VAN. Tento komponent definuje základnú úroveň ochrany TOE z hľadiska potenciálu útoku, na základe ktorého sa bude posudzovať analýza zraniteľnosti TOE.

Nezávislá analýza zraniteľností hodnotiteľov vychádza z informácií získaných zo všetkých ostatných hodnotiacich činností a presahuje rámec opisu bezpečnostnej architektúry (často vnímanej ako "analýza zraniteľností vývojára"). Hlavným zámerom analýzy hodnotiteľa je určiť, či je TOE odolné voči útokom na prienik, ktoré vykoná útočník so základným (pre AVA_VAN.1 a AVA_VAN.2), rozšíreným základným (pre AVA_VAN.3), stredným (pre AVA_VAN.4) alebo vysokým (pre AVA_VAN.5) potenciálom útoku.

Napríklad na zabezpečenie odolnosti proti vysokému potenciálu útoku pri analýze zraniteľnosti na úrovni EAL4 musí byť trieda AVA rozšírená o AVA_VAN.5. Okrem toho sa v rámci SAR musia vyžadovať komponenty, od ktorých závisí AVA_VAN.5. Ďalšie informácie o potenciáli útoku sú uvedené v prílohe 7, UPLATNENIE POTENCIÁLU ÚTOKU NA SMART KARTY A PODOBNÉ ZARIADENIA.

SFR

Určité usmernenie o používaní takýchto komponentov v PP alebo ST pre IC by mohlo byť užitočné, hoci v súčasnosti existuje množstvo PP pre IC, na ktoré sa možno užitočne odvolať (potreba dodržiavať takéto PP môže vopred určiť, ktoré funkčné komponenty sa musia použiť v ST).

Možné bezpečnostné funkčné požiadavky (SFR) podľa časti 2 CC pre IC zahŕňajú napríklad komponenty z týchto tried: FIA, FMT, FCS, FDP a FPT.

Je dôležité, aby vybrané funkčné komponenty boli prispôsobené v rozsahu potrebnom na preukázanie splnenia bezpečnostných cieľov TOE. To platí pre PP aj ST (ale najmä pre prvé menované, kde operácie na funkčných komponentoch môžu zostať nedokončené, a tak vzniknú SFR, ktoré sú príliš všeobecné).

Ďalším problémom je požiadavka CC, aby sa SFR skutočne dali testovať. Usmernenia k testovaniu nájdete v časti ATE nižšie.

Komponenty FPT_PHP sa používajú na vyjadrenie požiadaviek na ochranu TOE pred útokmi fyzickej manipulácie a vyžadujú, aby TOE implementovalo funkcie na reakciu na tieto útoky - či už prostredníctvom:

- poskytnutie schopnosti odhaliť útok (FPT_PHP.1) alebo
- zisťovanie a oznamovanie útoku (FPT_PHP.2) alebo
- automatická reakcia na útok (FPT_PHP.3).

Výber týchto komponentov sa môže prispôsobiť situácii na mieste. Napríklad automatická reakcia na útok (FPT_PHP.3) sa môže spresniť ako predpoklad, že kedykoľvek môže dôjsť k útoku, a preto sa kedykoľvek poskytnú protiopatrenia, pretože technické vlastnosti TOE nemusia byť schopné odhaliť útok, ale sú trvalo aktivované na mieste. Vyžaduje sa napríklad trvalá ochrana proti diferenciálnej analýze výkonu, ktorá zabezpečí, aby SFR nemohol byť kedykoľvek porušený alebo obídený.

Pri hodnotení zloženého TOE (hardvér integrovaného obvodu a softvér: operačný systém, aplikačný softvér a špecializovaný softvér integrovaného obvodu) môže byť vhodné vybrať funkčné komponenty pre politiku riadenia toku informácií pomocou funkčných komponentov zo skupín FDP_IFC a FDP_IFF. Tieto komponenty sa vzťahujú na určité časti softvéru, ktoré sú súčasťou TOE (napríklad takéto požiadavky sa kladú na operačný systém, a teda na integrovanú platformu pozostávajúcu z IC a OS; v [BSI-CC-PP-0084-2014] sa takéto komponenty vzťahujú na špecializovaný softvér IC).

ST alebo PP môže upraviť vybrané komponenty časti 2 CC tak, aby boli pre smart karty zmysluplnejšie (je však potrebné poznamenať, že takéto upravené požiadavky je potrebné overiť v praxi), ako napr:

- odchýlka od komponentu FAU_GEN.1, ktorý sa týka generovania údajov o audite, aby sa vylúčila požiadavka na dátum a čas v zázname o audite. Táto požiadavka je však dosiahnuteľná len vtedy, ak existuje externý dôveryhodný zdroj času a v zázname možno zachovať dôveryhodnosť;
- zdokonalenie FPT_TST.1, vlastné spracovanie, ktoré zahŕňa funkcie blokovania kariet.

Operácie na základe požiadaviek

Bezpečnostný zámer musí explicitne vykonávať všetky operácie (priradenie, iterácia, výber a spresnenie) bezpečnostných požiadaviek. Tieto operácie sa môžu týkať požiadaviek bezpečnostných funkcionalít, ako aj požiadaviek bezpečnostných záruk. Vykonávajú sa minimálne všetky operácie priradenia a výberu požiadaviek bezpečnostných funkcionalít.

Autor bezpečnostného zámeru vyberie pre každý výber príslušnú položku v zozname výberov. Pre každé priradenie autor bezpečnostného zámeru uvedie príslušnú položku. Všetky usmernenia by sa mohli nachádzať v prílohách časti 2 CC.

V prípade integrovaných obvodov je dôležité, aby sa hodnotenie zaoberalo bezpečnostnými aspektmi návrhu a implementácie, ktoré nemusia mať nevyhnutne funkčný charakter.

Súhrnná špecifikácia TOE (TSS)

Súhrnná špecifikácia TOE poskytuje opis na vysokej úrovni, ako TOE implementuje funkčné požiadavky (SFR) definované v ST. Autor ST sa môže rozhodnúť, že v súhrnnej špecifikácii TOE (ako súčasť ASE_TSS.2) zdôrazní technické a technologické vlastnosti IC pre používateľov.

Tvrdenia PP

Bezpečnostný zámer výslovne vyhlási súlad s každým ochranným profilom , ak je to uplatniteľné. V tomto prípade musí ST výslovne vyhlásiť zhodu.

[BSI-CC-PP-0084-2014], ktorý vyvinula komunita výrobcov polovodičov, by mohol byť uvedený[37] v bezpečnostnom zámere.

Treba poznamenať, že nároky na čiastočný súlad s PP nie sú podľa OZ prípustné. Súlad s PP môže byť preukázateľný alebo prísny, ako je definované v ochrannom profile, na ktorý sa odkazuje. V oblasti Security IC sa uprednostňuje prísny súlad s PP.

V prípade akéhokoľvek súladu s PP nemusí bezpečnostný zámer opakovať vyhlásenia o bezpečnostných požiadavkách obsiahnutých v PP, ktoré sú pre bezpečnostný zámer nezmenené. Napriek tomu by mohlo byť jednoduchšie mať samostatný dokument.

Ak však PP obsahuje nedokončené operácie, čo je prípad [BSI-CC-PP-0084-2014], za dokončenie týchto operácií zodpovedá autor bezpečnostného zámeru.

Odôvodnenie

Bezpečnostný zámer je základom pre stanovenie pohľadu na efektívnosť, pretože uvádza zamýšľané použitie IC, operačné prostredie, predpokladané hrozby, ciele, požiadavky funkcionalít a požiadavky bezpečnostných záruk a súhrnnú špecifikáciu TOE, ako sa uvádza vyššie.

CC vyžaduje zdôvodnenie, ktoré preukáže, že TOE v súlade s ST bude účinne riešiť všetky relevantné aspekty "bezpečnostného problému" definovaného vo vyhlásení o bezpečnostnom probléme. Odôvodnenie ST predstavuje analýzu postupným spôsobom:

- po prvé, musí sa preukázať, že bezpečnostné ciele pre TOE a jeho prostredie sú vhodné na boj proti identifikovaným hrozbám (prenesené určitými scenármi útokov) a podporujú všetky identifikované politické potreby a predpoklady. V prípade potreby môžu mať význam scenáre fyzických útokov na hardvér. Podstatné sú predpoklady týkajúce sa prevádzky softvéru;
- po druhé, musí sa preukázať, že bezpečnostné požiadavky sú vhodné na splnenie bezpečnostných cieľov TOE, vzájomne sa podporujú a vytvárajú integrovaný a účinný celok (záväznosť). Analýza by preto mala zvážiť kombinácie SFR, kde niektoré z nich môžu byť logické a iné technologické
  a technické požiadavky. Analýza by mala zvážiť aj vzťahy medzi požiadavkami bezpečnostných záruk a cieľmi operačného prostredia určitých fáz životného cyklu, ako sú fázy integrácie zloženého produktu a personalizácie.

[37] Zoznam platných PP nájdete na webovej stránke o európskych systémoch certifikácie kybernetickej bezpečnosti, ktorú spravuje agentúra ENISA.

V závislosti od rozsahu TOE je potrebné zohľadniť väzbu hardvérových a firmvérových funkcií. V prípade integrovaného obvodu by mal bezpečnostný zámer opisovať predpoklady týkajúce sa prevádzky softvéru.

Podrobné aspekty zaoberajúce sa problematikou nepriamych útokov na IC (napr. obchádzanie alebo popieranie TSF) by mali byť súčasťou hodnotenia zraniteľnosti (pozri triedu AVA). Vývojár to podporuje svojím názorom na to, ako sa čelí nepriamym útokom vo forme obchádzania alebo falšovania (v opise bezpečnostnej architektúry, hodnotenom v triede ADV_ARC).

Pri hodnotení zloženého TOE by sa mala analýza zaoberať vzájomnými vzťahmi medzi softvérovými a hardvérovými časťami TOE, aby sa preukázalo, že sa navzájom podporujú pri plnení bezpečnostného zámeru pre zložený TOE. To bude zahŕňať nielen diskusiu o závislostiach integrovaného obvodu od softvéru, ako sú uvedené vyššie, ale aj o závislostiach softvéru od hardvéru vrátane aspektov odolnosti voči neoprávnenej manipulácii.

Analýza sa väčšinou vykonáva poskytnutím mapovania v kombinácii s neformálnymi argumentmi mapovaných položiek a vysvetlením vzťahov medzi určitými položkami.

2.5 Vývoj (Trieda Adv)

Trieda záruk ADV definuje požiadavky na postupné spresňovanie bezpečnostnej funkcionality TOE (TSF) od požiadaviek bezpečnostných funkcionalít TOE (SFR) v ST až po skutočnú implementáciu a definuje požiadavky na opis architektonicky orientovaných prvkov a vnútornej štruktúry TOE (ADV_ARC, ADV_INT). Každá z výsledných zobrazení TSF poskytuje informácie, ktoré pomáhajú hodnotiteľovi určiť, či boli splnené funkčné požiadavky TOE.

Technický opis TOE je vždy sprevádzaný mapovaním vyššej úrovne na nižšiu úroveň zobrazení TOE.

2.5.1 Architektúra (ADV_ARC)

2.5.1.1 Ciele

CC Časť 3 predstavuje skupinu bezpečnostných záruk Security Architecture (ADV_ARC). Jej cieľ je opísaný takto:

"Cieľom tejto skupiny je, aby vývojár poskytol opis bezpečnostnej architektúry TSF. To umožní analýzu informácií, ktoré v spojení s ostatnými dôkazmi predloženými pre TSF potvrdia, že TSF dosahuje požadované vlastnosti. Popisy bezpečnostnej architektúry podporujú implicitné tvrdenie, že bezpečnostnú analýzu TOE možno dosiahnuť preskúmaním TSF; bez spoľahlivej architektúry by bolo potrebné preskúmať celú funkcionalitu TOE."

Skupina ADV_ARC vyžaduje, aby bezpečnostná architektúra TOE opisovala princípy vlastnej ochrany, oddelenia domén a neobchádzateľnosti. Bezpečnostná architektúra musí opisovať aj bezpečnú inicializáciu bezpečnostnej funkcie TOE (TSF).

2.5.1.2 Vstup

Opis bezpečnostnej architektúry sa sprístupní na všetkých EAL od EAL2. Vývojár poskytne opis bezpečnostnej architektúry TSF na úrovni podrobnosti zodpovedajúcej opisu abstrakcií presadzujúcich SFR opísaných v dokumente návrhu TOE.

Opis bezpečnostnej architektúry musí preukázať efektívnosť vlastnej ochrany a neprekonateľnosť.

2.5.1.3 Požiadavky

Neobchádzateľnosť je vlastnosť, že bezpečnostná funkcionalita špecifikovaná v SFR je vždy vyvolaná a nemôže byť obídená, ak je to vhodné pre daný mechanizmus (pozri prílohu A k CC časť 3, odsek 517). CC časť 3, A.1.2.3 pojednáva o obchádzateľnosti presadzovania SFR prostredníctvom rôznych rozhraní a o informáciách uvedených vo funkčnej špecifikácii (ADV_FSP) a návrhu TOE (ADV_TDS) o operáciách a informáciách dostupných prostredníctvom týchto rozhraní. To zahŕňa všetky logické a fyzické programovacie a komunikačné rozhrania IC, ako aj povrch IC.

Vlastná ochrana sa vzťahuje na schopnosť TSF chrániť sa pred manipuláciou zo strany externých

subjektov, ktorá môže viesť k zmenám TSF, takže už nebude spĺňať SFR. Vlastná ochrana TSF sa dosiahne prostredníctvom:

- vlastná ochrana mechanizmov TSF: schopnosť mechanizmu TSF chrániť sa pred priamymi útokmi s cieľom zasahovať do tohto mechanizmu, manipulovať s ním alebo ho znefunkčniť;
- väzba mechanizmov TSF: schopnosť mechanizmov TSF spolupracovať spôsobom, ktorý sa navzájom podporuje a vytvára integrovaný a účinný celok.

Príkladom vlastnej ochrany mechanizmu TSF je ochrana proti fyzickému skúmaniu bezpečnostného integrovaného obvodu s cieľom manipulovať s funkciami TSF alebo ich vypnúť. V niektorých prípadoch musí mechanizmus fyzickej ochrany odolávať takýmto útokom nezávisle od akéhokoľvek iného mechanizmu TSF. V iných prípadoch mechanizmus fyzickej ochrany takéto útoky zistí a operačný systém na ne reaguje vstupom do bezpečného stavu.

Príkladom väzby mechanizmov TSF v prípade smart kariet je kombinácia hardvérových a softvérových mechanizmov TSF:

- na zabezpečenie stabilného správneho vykonávania vstavaného softvéru za stanovených prevádzkových podmienok;
- na zistenie chýb pri vykonávaní spôsobených rušením;
- prejsť do zabezpečeného stavu, ak zistené chyby nemožno automaticky opraviť.

Opis bezpečnostnej architektúry musí opisovať, ako je proces inicializácie TSF bezpečný (pozri ADV_ARC.1.3C). Informácie uvedené v opise bezpečnostnej architektúry týkajúce sa inicializácie TSF sú zamerané na komponenty TOE, ktoré sa podieľajú na uvedení TSF zo stavu "down" (napr. vypnutie) do počiatočného bezpečného stavu (t. j. keď sú všetky časti TSF funkčné) (porovnaj odsek 529 CEM). TSF môže mať časti, ktoré zabezpečujú svoju bezpečnostnú funkciu, keď TOE nie je v prevádzke. Napr. fyzická ochrana bezpečnostného integrovaného obvodu musí odolávať útokom neoprávnenej manipulácie podľa FPT_PHP.3, aj keď je napájanie vypnuté. Ostatné časti TSF sa môžu aktivovať počas spustenia TOE pred aktiváciou príslušnej funkcie TOE alebo súčasne s ňou. Napr. snímače musia kontrolovať podmienky prostredia pre normálnu bezpečnú prevádzku bezpečnostného IC v čase spustenia operačného systému smart karty. Operačný systém musí skontrolovať integritu uložených údajov TSF pred tým, ako sa na ne spoľahne. V prípade bezpečnostného integrovaného obvodu sa proces bezpečnej inicializácie TSF vzťahuje na zapnutie, vstup a prebudenie z úsporného režimu alebo akéhokoľvek druhu resetu.

Oddelenie domén je vlastnosť, ktorou TSF vytvára samostatné bezpečnostné domény pre seba a pre každú nedôveryhodnú aktívnu entitu, ktorá má pracovať s jeho zdrojmi, a potom udržiava tieto domény navzájom oddelené tak, aby žiadna entita nemohla pracovať v doméne inej entity (pozri CC časť 3, odseky 515, 524 a 578). Bezpečnostné domény sa vzťahujú na prostredia, ktoré poskytuje TSF na použitie potenciálne škodlivými entitami (porovnaj CEM, odsek 527). Prostredie, ktoré poskytuje TSF IC subjektu na programovom rozhraní, môže zahŕňať zdroje, ako napr.

- vstupné a výstupné porty/rozhrania na interakciu s externými subjektmi (používateľmi) alebo procesmi (subjektmi) integrovaného obvodu alebo vstavaného softvéru;
- adresný priestor na prístup k operačnej pamäti a funkčným registrom;
- príkazy CPU alebo kryptografických koprocesorov, ktoré má subjekt k dispozícii na vykonanie;
- služby poskytované TSF, ako je generovanie náhodných čísel.

TSF môže používať špecifické zdroje len pre svoju vlastnú bezpečnostnú oblasť, ako napr. senzory na ochranu pred poruchami prostredia, ktoré sú mimo kontroly vstavaného softvéru. TSF môže zdieľať zdroje s inými subjektmi, ako napr. generátor náhodných čísel, ktorý TSF používa na náhodný výpočet kryptografického koprocesora a ktorý používa vstavaný softvér na generovanie kľúčov. TSF môže kontrolovať prístup k prostriedkom entít rôznych bezpečnostných domén, ktoré však nepoužíva, ako sú privilegované príkazy CPU. TSF môže poskytovať bezpečnostné funkcie vstavanému softvéru na vynútenie oddelenia ich domén, napr. jednotke správy pamäte.

2.5.2 Funkčná špecifikácia (ADV_FSP)

2.5.2.1 Ciele

Funkčná špecifikácia opisuje rozhrania TSF (TSFI) a musí byť úplnou a presnou inštanciou požiadaviek bezpečnostných funkcionalít TOE definovaných v ST.

Cieľom skupiny ADV_FSP je opis a analýza vonkajšieho rozhrania k TOE. Očakáva sa, že používatelia TOE budú komunikovať s TSF prostredníctvom tohto rozhrania. TSFI pozostáva zo všetkých prostriedkov, ktorými používatelia vyvolávajú službu z TSF (poskytnutím údajov, signálov, energie alebo fyzikálnych účinkov, ktoré TSF spracúva), a z príslušných odpovedí na tieto vyvolania služby. Tieto vyvolania služieb a odpovede sú prostriedkami prekračovania hraníc TSF (pozri [CC] časť 3, oddiel A.2.1). Všetky rozhrania, ktoré prekračujú hranicu TSF, vrátane rozhraní na subsystémy TOE, ktoré nie sú TSF, sa považujú za TSFI. Opis TSFI poskytuje potrebné informácie na vykonanie testovania.

Komponenty ADV_FSP.2 a vyššie popisujú všetky TSFI vo zvyšujúcej sa miere podrobnosti. Pri komponentoch nižšej úrovne môžu vývojári zamerať svoju dokumentáciu (a hodnotitelia svoju analýzu) na aspekty TOE, ktoré sú z hľadiska bezpečnosti relevantnejšie, prostredníctvom charakterizácie TSFI ako SFR-vynucujúce, SFR-relevantné a SFR-neinterferujúce. Komponenty ADV_FSP.4 a vyššie, ktoré sa zvyčajne používajú pre bezpečnostné IC, opisujú všetky rozhrania na rovnakej úrovni detailov
a umožňujú hlbšiu analýzu, či rozhrania neposkytujú funkcie spôsobom, ktorý je v rozpore s SFR definovaným v ST.

2.5.2.2 Vstup

Bez ohľadu na EAL musí vývojár poskytnúť funkčnú špecifikáciu.

Externé rozhrania sú zvyčajne opísané v technickom liste integrovaného obvodu. Vo väčšine prípadov je relevantná norma ISO (7816). Okrem toho sa uvedie opis matrice.

2.5.2.3 Požiadavky

Funkčná špecifikácia zvyčajne používa terminológiu vývojárov. Úroveň podrobnosti požadovanej pre špecifikáciu musí byť v korelácii s pokrytím funkčných skúšok (ATE_COV) a s opisom vonkajšieho rozhrania v rámci sprievodnej dokumentácie (AGD_OPE / AGD_PRE).

Špecifikácia funkčných detailov bezpečnostných funkcií TOE musí byť uvedená vo funkčnej špecifikácii. Podrobnejšie úrovne znázornenia mapujú tieto funkčné detaily na definované subsystémy alebo moduly.

Externé rozhrania bezpečnostného integrovaného obvodu možno klasifikovať ako :

- Programové rozhrania - logické rozhranie so softvérom/firmvérom, ktorý je uložený v IC a nie je súčasťou TOE, ale ktorý beží na uvažovanom hardvéri IC (napr. spustenie prerušenia prostredníctvom hardvéru, testovacie softvérové rozhrania).
- Komunikačné rozhranie - logické rozhrania (napr. inštrukčná sada, špecifikácia registrov špeciálnych funkcií, mapa pamäte) a fyzické rozhrania integrovaného obvodu (kontakty integrovaného obvodu so sériovým vstupom/výstupom a napájacím alebo bezkontaktným rozhraním alebo oboma), ktoré zaručujú spojenie s vonkajším svetom v rámci operačného prostredia a operačného systému/prostredia programovania aplikácií.
- Povrch IC - explicitne definovaný súvislý obvod, ktorý určuje fyzické hranice TOE a obsahuje všetky hardvérové, softvérové a/alebo firmvérové komponenty TOE. Povrch IC sa opíše a preskúma
  z hľadiska fyzickej ochrany (pozri SFR skupiny FPT_PHP) a úplnosti opisu logického a fyzického rozhrania vrátane oblastí vyžarovania a ožiarenia.

V prípade integrovaného obvodu sa opíše fyzický vstupný alebo výstupný bod TOE (porty), ktorý poskytuje prístup k TOE pre fyzické signály zobrazované logickými rozhraniami vrátane napájania. Port môže poskytovať viac informácií, ako je potrebné pre TSFI. Tieto dodatočné informácie môžu obchádzať bezpečnostné funkcie zámerne poskytované prostredníctvom tohto rozhrania (napr. bočným kanálom). Jednoduché pozorovanie externých rozhraní z hľadiska ich logického správania pravdepodobne nebude postačujúce. Externe nastaviteľné prevádzkové parametre a ich limity by sa mali tiež preskúmať, pretože môžu viesť k priamym útokom alebo zraniteľnostiam. Funkčná špecifikácia musí sledovať SFR na TSFI.

Vyhradený testovací softvér IC sa môže dodať ako súčasť TOE na podporu testovania TOE počas výroby a nemusí byť použiteľný po dodaní TOE. V takom prípade sa špecializovaný testovací softvér IC (alebo jeho časti) považuje len za "testovací nástroj", ktorý neposkytuje bezpečnostné funkcie pre prevádzkovú fázu TOE. Ich použitie musí byť opísané v riadiacej dokumentácii pre testera, ale nie

nevyhnutne vo funkčnej špecifikácii. Musí sa však overiť, či sa po dodaní TOE nedá zneužiť: hodnotí sa to podľa CC časti 3 skupiny záruk AVA_VAN.

Funkčná špecifikácia špecifikuje prevádzkové podmienky bezpečnostného IC. Tieto podmienky zahŕňajú okrem iného frekvenciu hodín, napájanie a teplotu. Bezpečnostný IC by mal reagovať na porušenie prevádzkových podmienok ohrozujúcich správne vykonávanie vstavaného softvéru vstupom do bezpečného stavu.

Poloformálny zápis

V norme EAL5 sa vyžaduje, aby bola funkčná špecifikácia poloformálna. Uvedený príklad, poloformálny opis funkčnej špecifikácie môže mať podobu

- tabuľky, kde je každý stĺpec priradený konkrétnemu bitu konkrétneho registra a neformálny text vysvetľuje ich účinok;
- blokové diagramy, pričom všetky blokové diagramy používali skratky a šípky na definovanie smeru toku údajov;
- matematický vzorec, napr. booleovský logický výraz opisujúci kombináciu signálov alebo nerovnica na špecifikáciu kontroly rôznych prahových hodnôt;
- pseudokód používaný podobne ako v programovacom jazyku, ktorý neobsahuje žiadne nejasné štruktúry;
- assemblerový kód popisujúci programové sekvencie na špecifikáciu správania a zamýšľaného použitia konkrétnych komponentov.

Neformálna dokumentácia technických a technologických vlastností, ako aj ich začlenenie do štruktúry a realizácie ŠPS sú nevyhnutné.

2.5.3 TOE návrh (ADV_TDS)

2.5.3.1 Ciele

Cieľom týchto požiadaviek je poskytnúť kontext pre opis TSF, ako aj dôkladný opis TSF. Projektová dokumentácia musí poskytovať dostatočné informácie na určenie hraníc TSF a na opis toho, ako TSF realizuje SFR.

Požiadavky na návrh majú poskytnúť informácie (zodpovedajúce danej úrovni záruky), aby bolo možné určiť, či sú bezpečnostné funkčné požiadavky splnené.

Návrh TOE poskytuje opis TOE a TSF z hľadiska subsystémov ako hlavných štrukturálnych jednotiek s funkčnou koherenciou, poskytuje opis interakcie týchto štrukturálnych jednotiek a je správnou realizáciou funkčnej špecifikácie.

Návrh TOE poskytuje opis TSF z hľadiska modulov ako najkonkrétnejší opis funkčnosti. Opis modulov musí poskytovať dostatočné podrobnosti, aby bol vývojár schopný implementovať túto časť TOE opísanú modulom bez ďalších rozhodnutí o návrhu.

2.5.3.2 Vstup

Informácie o návrhu TOE sa sprístupňujú na všetkých EAL od EAL2.

2.5.3.3 Požiadavky

TOE vs. TSF

Návrh TOE opisuje štruktúru TOE z hľadiska subsystémov a identifikuje subsystémy TSF. TSF zahŕňa všetky časti TOE, ktoré prispievajú k splneniu SFR v ST (vcelku alebo čiastočne), a bezpečnostné architektonické princípy vlastnej ochrany TSF, izolácie domény, neobchádzateľnosti a bezpečnej inicializácie (pozri ADV_ARC). Žiadna časť TOE, ktorá nie je súčasťou TSF, nesmie brániť TSF v splnení SFR v ST.

Ak sú subsystémy TOE oddelené od subsystémov TSF, odôvodnenie jasnosti a efektívnosti oddelenia by malo byť založené na logických a fyzických závislostiach. Maximálna nezávislosť subsystémov v rámci IC TOE by mohla byť možná, ak by neexistovali žiadne alebo len minimálne fyzické prekrývania a logické závislosti medzi jednotlivými subsystémami a rozhrania by boli jasne definované.

Základná štruktúra TSF z hľadiska subsystémov a modulov:

Výber definície subsystému zo strany vývojára a na úrovni ADV_TDS.3 alebo vyššej spresnenie na moduly TSF v rámci každého subsystému sú dôležitým faktorom, aby bol návrh TOE užitočný na pochopenie zamýšľanej prevádzky TSF. Počet subsystémov a modulov v rámci subsystémov spolu s opisom ich vzájomného pôsobenia, rozhraní a účelu modulov musí byť vhodný a dostatočný na to, aby hodnotiteľ získal potrebnú úroveň pochopenia toho, ako sa zabezpečuje funkčnosť TSF.

Ak sa návrh integrovaného obvodu riadi klasickým procesom hardvérových výkresov, proces vývoja v podstate závisí od použitých technológií (konkrétnej metódy a nástrojov) a možno ho opísať spresnením návrhu z hľadiska subsystémov na dostatočnú úroveň podrobnosti z hľadiska modulov na realizáciu TOE. Ak sa návrh integrovaného obvodu riadi prostredníctvom jazyka na opis hardvéru (HDL), dekompozícia je podobná tým, ktoré sa používajú pri klasickom vývoji softvéru. Konštrukčné plány
a funkčné opisy, ktoré sú výsledkom použitia nástroja HDL a nástroja CAD, sa môžu použiť priamo počas konštrukcie návrhu TSF, ale je potrebné ich plne prezentovať len pre ADV_TDS.4 alebo vyšší.

Návrh TOE poskytuje špecifikáciu návrhu na najvyššej úrovni z hľadiska subsystémov TOE a TSF. Na podporu týchto požiadaviek sa môže považovať za kompletnú knihu údajov obsahujúcu úplný opis čipu. Bloková schéma, ktorá vzniká vo fáze návrhu a koncepcie, ako aj neformálny opis môžu byť neoddeliteľnou súčasťou opisu návrhu TOE z hľadiska subsystémov. Zvyčajne sa dokumentácia potrebná pre subsystémy môže opísať ako mapovanie hlavných architektonických komponentov na fyzické zariadenia vykonávajúce špecifické funkcie (napr. CPU, RAM, ROM, zbernica a I/O prvky)
a interakcie medzi subsystémami.

V mnohých prípadoch môžu byť komponenty, ktoré predstavujú všeobecnú štruktúru IC TOE, definitívnymi logickými jednotkami; prípadne sú dokonca implementované ako fyzická jednotka na IC. Príklady zahŕňajú: pamäť, rozhranie dátová/adresová zbernica-pamäť, aritmetický blok, kontaktné rozhranie, časovač strážneho psa, snímače s logikou analýzy, ovládacie prvky pre napätie napájanie, logické bloky na kontrolu prístupu alebo autentizáciu pre pamäťové IC s bezpečnostnou logikou, blok mikrokontroléra na mikrokontroléroch IC.

Návrh TOE na úrovni ADV_TDS.3 alebo vyššej si vyžaduje zdokonalenie subsystémov TSF do modulov. Moduly sú podrobne opísané z hľadiska funkcie, ktorú poskytujú (účel); rozhraní, ktoré predstavujú; návratových hodnôt z týchto rozhraní; rozhraní (prezentovaných inými modulmi), ktoré používajú; a opisu spôsobu, akým poskytujú svoju funkciu (jedným z možných spôsobov opisu funkcie je algoritmický opis) (pozri CC časť 3, oddiel A.4.2).

Forma popisu funkcií a spôsob, akým ich modul poskytuje, závisí od danej funkcie. Napr. návrh TOE môže poskytovať algoritmický opis výpočtu kryptografického koprocesora, ako aj neformálny opis fyzikálneho princípu použitého pre senzor alebo zdroj šumu fyzikálneho generátora náhodných čísel.

Konštrukčné prvky potrebné na konštrukciu TOE sú:

- logické plány (ktoré sa skladajú napríklad z analógových buniek, štandardných buniek, hradiel, tranzistorov a diód) alebo zodpovedajúce HDL-zobrazenia s cieľom realizovať jednotlivé funkcie, ako aj bezpečnostné mechanizmy;
- špecifikácia fyzického návrhu, ktorá opisuje požiadavky na organizáciu fyzických komponentov (napr. umiestnenie modulov, poradie vrstiev, špecifikácie smerovania).

V prípade integrovaného obvodu sa skutočná logika a plány rozloženia odvodia z modulov, pričom oddelenie modulov musí spĺňať požiadavky na testovanie. Rozhrania medzi modulmi musia byť opísané obzvlášť starostlivo, pretože v integrovanom obvode medzi nimi existujú silné závislosti. Funkcionalita, ktorá prebieha paralelne, by sa mala zohľadniť pri opise rozhraní. Časovanie rozhraní modulov by sa malo opísať, ak sú prístupné zvonku (napr. podložky) pre testy.

Keďže bezpečnostné vlastnosti integrovaného obvodu TOE môžu pozostávať z logickej funkčnosti, ako aj z technických a technologických vlastností, je potrebné zdokumentovať všeobecnú štruktúru architektonických komponentov, ako aj vysvetliť technickú a technologickú štruktúru (všeobecné pravidlá usporiadania fyzického návrhu: technológia, počet vrstiev, smerovanie zberníc), pretože sú dôležité pre bezpečnostné vlastnosti hardvéru. Ochranná vrstva by sa napríklad mohla považovať za zložku všeobecnej štruktúry fyzického zloženia TOE.

Opis TSF z hľadiska subsystémov a modulov, ktoré posilňujú SFR, podporujú SFR a nezasahujú do SFR

Návrh TOE musí označiť subsystémy TSF - a navyše na úrovni ADV_TDS.3 a vyššej moduly - ako SFR-enforcing, SFR-supporting a SFR-non-interfering. Pri komponentoch nižších úrovní môžu vývojári zamerať svoju dokumentáciu (a hodnotitelia svoju analýzu) na aspekty TOE, ktoré sú z hľadiska bezpečnosti relevantnejšie, t. j. počnúc komponentmi posilňujúcimi SFR a pokračujúc komponentmi podporujúcimi SFR až po komponenty nezasahujúce do SFR. Je potrebné poznamenať, že aj keď sa vyžaduje viac alebo dokonca úplné informácie na vyšších úrovniach komponentov, nevyžaduje sa, aby sa všetky tieto informácie analyzovali na rovnakej úrovni podrobnosti. Vo všetkých prípadoch by sa mal klásť dôraz na to, či boli potrebné informácie poskytnuté a analyzované.

Mapovanie SFR na fyzické subsystémy nemusí byť jednoduché (napr. ktorý subsystém skutočne spracováva bezpečnostné funkcie, CPU alebo CPU v spojení s jeho pridruženou pamäťou a zbernicou?). Je to preto, že v rámci samotného integrovaného obvodu existujú silné závislosti medzi rôznymi fyzickými komponentmi na úrovni implementácie, ktoré komplikujú účinné oddelenie v zmysle kritérií. V dôsledku toho je väčšinou potrebné a pre niektoré hardvérové TOE môže byť jednoduchšie klasifikovať všetky subsystémy IC TOE na úrovni vysokoúrovňového návrhu ako SFR-vykonávajúce.

Napríklad firmvér testovacej pamäte ROM by sa mohol klasifikovať ako "SFR-neinterferujúci subsystém", pretože neprispieva k SFR (ale je potrebný pre test výrobcu) a je deaktivovaný v prevádzkovej fáze TOE. Ďalším príkladom, v závislosti od špecifickej bezpečnostnej funkcie TOE, môže byť štandardná periférna jednotka, napr. časovač, ak je možné zobraziť oddelenie.

Dôkazy o spôsobe poskytovania SFR

Hodnotiteľ určí, či je návrh presnou a úplnou inštanciou všetkých požiadaviek bezpečnostných funkcionalít (pozri ADV_TDS.x.2E). Priradenie SFR subsystémom alebo dokonca modulom môže byť obzvlášť náročné, pretože jednotlivé komponenty nezabezpečujú len realizáciu jednej SFR a medzi komponentmi môžu existovať veľmi silné interakcie a závislosti. Mapovanie SFR ST prostredníctvom funkčnej špecifikácie na fyzické subsystémy a moduly nemusí byť jednoduché, ako bolo uvedené vyššie. Z tohto dôvodu má osobitný význam opis funkčného toku bezpečnostných funkcií implementujúcich SFR do definovaných subsystémov.

SFR ST vyjadrujúce bezpečnostné vlastnosti by sa mohli realizovať a sledovať na základe technologických vlastností TOE opísaných v návrhu.

Poloformálny zápis

Pri stupni EAL5 sa vyžaduje, aby bol návrh TOE poloformálny. Poloformálny opis návrhu TOE môže mať podobu blokových schém zapojenia alebo dokumentov v jazyku opisu hardvéru (HDL - hardware description language). V mnohých prípadoch by sa však na úrovni podrobného návrhu najprv použil jazyk opisu hardvéru.

Významné grafické znázornenie technických alebo technologických vlastností ako súčasť bezpečnostných mechanizmov TOE možno považovať za ekvivalent poloformálneho znázornenia.

Neformálna dokumentácia technických a technologických vlastností, ako aj ich integrácia do štruktúry a realizácia bezpečnostných mechanizmov sú nevyhnutné.

2.5.4 Zobrazenie implementácie (ADV_IMP)

2.5.4.1 Ciele

Cieľom týchto požiadaviek je určiť, či je zobrazenie implementácie dostatočná na splnenie SFR ST a či je správnou realizáciou návrhu TOE vo forme, ktorú môže hodnotiteľ analyzovať.

Je to najmenej abstraktné zobrazenie TSF a zachytáva podrobné vnútorné fungovanie TSF z hľadiska zdrojového kódu, hardvérových diagramov a/alebo jazyka návrhu hardvéru alebo údajov o rozložení atď.

2.5.4.2 Vstup

Vývojár sprístupní zobrazenie implementácie na všetkých úrovniach od EAL4.

2.5.4.3 Požiadavky

Implementačné zastúpenie pre bezpečnostný IC

Implementačné zobrazenie TOE zodpovedá nasledujúcemu:

- hardvérové schémy pre analógové bloky;
- Výpisy HDL pre všetky syntetizované komponenty;
- v prípade potreby zdrojový kód všetkého vyhradeného/vstavaného softvéru;
- informácie o fyzickom návrhu, ako sú plány rozloženia a masky, ktoré opisujú implementáciu fyzických komponentov.

Úplné informácie o realizácii a usporiadanie sa hodnotiteľovi sprístupnia vo forme, ktorú používajú vývojoví pracovníci. V konkrétnych prípadoch to bude znamenať, že hodnotiteľ použije nástroje vývojára na preskúmanie zobrazenia implementácie (napr. simulačné nástroje, prehliadač rozloženia).

Plány rozloženia (fyzický návrh) opisujú usporiadanie fyzických komponentov a smerovanie signálov vzhľadom na procesné masky a určujú metalizačné masky.

Plány masiek sú potrebné pre technologický proces. Plány masiek sa musia uvádzať len v určitých prípadoch, ak sú potrebné pre následné analýzy, ako sú analýzy zraniteľnosti.

Rozloženie je potrebné na kontrolu správnosti realizácie technických a technologických vlastností. Rozloženie naznačuje jednoduchosť montáže fyzických útokov (napríklad prístupnosť metalizačnej vrstvy).

Technická a technologická štruktúra TOE sa má spresniť, aby bolo možné vykonať analýzu efektívnosti počas skúmania fyzických útokov na TOE (napr. informácie o rozložení konkrétnych buniek môžu byť potrebné, ak sú vystavené určitým útokom, ako je FIB).

Úprava parametrov výrobného procesu sa v tejto fáze určí na základe špecifických vlastností technológie a pomocou nástrojov CAD.

Vzorka zhody medzi návrhom TOE a zobrazenou implementáciou TSF

Hodnotiteľ vykoná analýzu zastúpenia implementácie s dvoma cieľmi:

- analyzovať správnosť zobrazenej implementácie a návrhu TOE, t. j. sledovateľnosť mechanizmov implementujúcich SFR, a bezpečnostné architektonické princípy vlastnej ochrany TSF, domény
- izolácia, neobchádzateľnosť a bezpečná inicializácia). Táto analýza využíva mapovanie medzi návrhom TOE a vzorkovanou alebo celou zobrazenou implementáciou vo forme schém/layoutov, ktoré sa poskytujú na tento účel;
- porozumieť implementácii TOE s cieľom špecifikovať potenciálne zraniteľnosti a cesty útoku.

Pri EAL4 (ADV_IMP.1) hodnotiteľ vyberie tie časti opisu návrhu TOE, ktoré sú zaujímavé (najmä tie, ktoré sú rozhodujúce pre analýzu zraniteľnosti), aby overil, či zobrazenie implementácie presne odráža opis uvedený v opise návrhu TOE.

Pokiaľ ide o porozumenie implementácii na úrovni ADV_IMP.1, pokiaľ ide o porozumenie implementácii, musí byť zdokumentovaný, poskytnutý a preukázaný reťazec zostavovania od návrhu TDS TOE po IC vzorku implementácie TOE (ADV_IMP.1.2D a ADV_IMP.1.3C). Na podporu analýzy zhody medzi návrhom TOE a zobrazením implementácie by sa mali použiť informácie o rozložení, ako aj výstupy návrhu TOE pre subsystémy a moduly. Musia sa opísať prepojenia medzi dokumentáciou TDS
a analógovými blokmi a zdokumentovať rozhrania

Napríklad požiadavka FPT_TST.1 (autotesty pri spustení a potom pravidelne) sa môže dosiahnuť pomocou snímačov prostredia, ktoré sú zase reprezentované bezpečnostnou logikou a hardvérovými schémami. V tomto prípade by bolo potrebné sledovať prevádzkové podmienky obálky prostredníctvom rôznych úrovní zobrazenia FPT_TST.1 a dôkazov testovania.

Na úrovni ADV_IMP.2 musí požadovaný opis vzťahov medzi celou zobrazenie implementácie

a návrhom TOE zahŕňať zdôvodnenie vzťahov medzi modulmi a technickými a technologickými štruktúrami TOE, ako aj medzi hardvérovými a firmvérovými časťami TOE.

2.5.5 Vnútorné TSF (ADV_INT)

2.5.5.1 Ciele

Táto skupina ADV_INT sa zaoberá hodnotením vnútornej štruktúry TSF. TSF, ktorého vnútorná štruktúra je dobre štruktúrovaná, sa ľahšie implementuje a je menej pravdepodobné, že bude obsahovať chyby, ktoré by mohli viesť k zraniteľnostiam; takisto sa ľahšie udržiava bez zavádzania chýb.

2.5.5.2 Vstup

Vývojár poskytne interný opis a odôvodnenie. Vývojár navrhne a implementuje celý TSF tak, aby mal dobre štruktúrované vnútorné prvky na úrovni EAL5 až EAL7.

2.5.5.3 Požiadavky

Vlastnosť "dobre štruktúrovaný" závisí od konkrétnej technológie použitej pre TOE a zvyčajne pochádza z priemyselných noriem pre túto technologickú disciplínu. V CC časť 3, oddiel A.3, a v CEM, oddiel 11.6.1, sú opísané kritériá na posúdenie tejto vlastnosti pre softvér. Pre hardvérové časti TSF zobrazené v jazyku na opis hardvéru (HDL) platia podobné kritériá ako pre softvér.

TSF bezpečnostného IC je dobre štruktúrovaný, ak štruktúra TSF zabezpečuje minimalizáciu zložitosti:

- logické a fyzické rozhrania medzi modulmi tak, aby návrh TSF zabezpečil do značnej miery nezávislé moduly, ktoré sa vyhýbajú zbytočným interakciám;
- funkčnosť modulu, čo umožňuje hodnotiteľovi, ako aj vývojárovi sústrediť sa len na tú funkčnosť, ktorá je potrebná na uplatnenie SFR, čo ďalej prispieva k zrozumiteľnosti a znižuje pravdepodobnosť chýb pri návrhu alebo implementácii.

Časť 3 CC, oddiel A.3.1, charakterizuje modularitu softvéru takto: *"softvér napísaný modulárnym dizajnom pomáha dosiahnuť zrozumiteľnosť tým, že objasňuje, aké závislosti má modul na iných moduloch (coupling), a tým, že do modulu zahŕňa len úlohy, ktoré sú navzájom silne prepojené (cohesion)"*.

Maximálna nezávislosť modulov (opísaná podľa ADV_TDS.3 alebo vyššej) v rámci IC TOE by mohla byť možná, ak by neexistovali žiadne alebo len minimálne fyzické prekrývania a logické závislosti medzi jednotlivými modulmi a rozhrania by boli jasne definované. Existujú rozhrania, ktoré sú nevyhnutne zložité a nemožno ich minimalizovať, napríklad zbernice.

Všimnite si, že požiadavky na dobre štruktúrovanú vnútornú štruktúru TSF nie sú v rozpore s bezpečnostným rozložením IC, ktoré skrýva štruktúru na implementačnej úrovni, aby sa zvýšila bariéra pre fyzické útoky (napr. náhodné umiestnenie modulov, lepená logika).

Vývojár zdôvodňuje charakteristiky použité na posúdenie významu pojmu "dobre štruktúrovaný", ktorý sa používa v opise vnútorných údajov a v procese vývoja. Hodnotiteľ preskúma odôvodnenie, aby zistil, či identifikuje základ pre určenie, či je TSF dobre štruktúrovaný (pozri pracovnú jednotku ADV_INT.1-1). Prijatie špecifických kritérií TOE pre to, či je dobre štruktúrovaná, by sa malo dohodnúť s hodnotiacim orgánom pred vykonaním analýzy.

2.6 Modelovanie bezpečnostnej politiky (ADV_SPM)

2.6.1 Ciele

Hodnotenie modelov bezpečnostných politík (SPM), ktoré sa vzťahujú na EAL6 a EAL7, sa týka najmä formálnych bezpečnostných politík.

Cieľ požiadaviek je teda dvojaký: určiť, či model bezpečnostnej politiky jasne a konzistentne opisuje pravidlá a charakteristiky bezpečnostnej politiky TOE, a posilniť opis formálnym dôkazom.

Model bezpečnostnej politiky sa považuje za model, ktorý štrukturálne formalizuje bezpečnostnú funkcionalitu s dostatočným vysvetľujúcim textom, ako aj poskytuje potrebný rámec na vykonanie formálneho dôkazu zhody medzi funkčnou špecifikáciou a príslušnými politikami modelu bezpečnostnej politiky.

Na tento účel sa model bezpečnostnej politiky TOE neformálne abstrahuje od jeho realizácie zohľadnením navrhovaných bezpečnostných požiadaviek ST. Neformálna abstrakcia sa považuje za úspešnú, ak sa ukáže, že zásady (alias pravidlá) TOE sú vynútiteľné jeho vlastnosťami (pozri ADV_SPM.1.2C). Účel formálnych metód spočíva vo zvýšení prísnosti presadzovania; neformálne argumenty sú vždy náchylné na chyby, najmä ak sa vzťahy medzi subjektmi, objektmi a operáciami čoraz viac rozširujú. S cieľom minimalizovať riziko nezabezpečených príchodov do stavu sa preto vlastnosti a pravidlá SPM mapujú na ich formálne náprotivky ako znaky a vlastnosti v rámci určitého formálneho rámca, ktorého rigoróznosť a sila sa potom môže použiť na odvodenie bezpečnostných vlastností v zmysle teorém.

Štruktúrované zobrazenie bezpečnostných politík modelov bezpečnostných politík sa preto používajú na poskytnutie väčšej bezpečnostnej záruky, že funkčná špecifikácia zodpovedá bezpečnostným politikám modelu bezpečnostnej politiky a nakoniec aj bezpečnostným funkčným požiadavkám TOE.

Formálny náprotivok v zmysle princípov a funkcií preto podporuje korešpondenčné mapovanie medzi funkčnou špecifikáciou, modelom bezpečnostnej politiky a modelovanými bezpečnostnými politikami.

2.6.2 Vstup

Vývojár poskytne model bezpečnostnej politiky TOE na EAL6 a EAL7.

2.6.3 Požiadavky

Formálny bezpečnostný model je formálny opis bezpečnostnej politiky pomocou vhodných formálnych jazykov. Používa sa na abstraktnej úrovni nezávisle od implementácie TOE v hardvéri alebo softvéri.

Ako návod na formálne požiadavky na technické a technologické vlastnosti (napr. náročnosť reverzného inžinierstva alebo prevádzky mimo obálky) môže pomôcť modelovanie ochrany integrovaného obvodu proti neoprávnenému zverejneniu aktív, neoprávnenému použitiu aktív a neoprávnenej modifikácii aktív z hľadiska bariér v kombinácii so stavmi bezpečnosti integrovaného obvodu počas rôznych fáz životného cyklu. V mnohých prípadoch sa zdá, že na splnenie požiadaviek je najvhodnejší konečný stavový stroj.

Vývojár zvyčajne vopred určí aktíva a použije abstrakciu, ktorá sa postará o všetky požadované bezpečnostné funkcie. Môže sa rozhodnúť rozdeliť operácie IC na bezpečnostné stavy (napr. používateľský režim vs. systémový režim) a stavové prechody spolu so subjektmi, ktoré pôsobia na objekty a spôsobujú vznik stavových prechodov. Keďže príčina udalostí postupuje s časom, formálny systém by mal byť aspoň taký silný, aby implementoval matematickú indukciu na vylúčenie možnosti príchodu nezabezpečených stavov.

Formálne systémy vhodné pre ADV_SPM.1 zahŕňajú (ale nie sú obmedzené na) B-Method Isabelle, MetaMath a VSE

II. Formálny systém sa dohodne s hodnotiacim orgánom konkrétneho procesu hodnotenia.

CC nevyžaduje, aby sa formálne modelovali všetky bezpečnostné funkcie, ale len tie politiky, ktoré sa dajú modelovať podľa „state of the art“. Kontrola toku informácií a kontrola prístupu sú však takmer vždy zahrnuté do formálneho modelu a na to, aby sa tieto politiky nebrali do úvahy, sú potrebné silné argumenty.

2.7 Skúšky (TRIEDA ATE)

Trieda záruk ATE uvádza požiadavky na skúšanie, ktoré preukazujú, že TSF spĺňa požiadavky bezpečnostných funkcionalít TOE. CC rozlišuje v rámci tejto triedy štyri skupiny záruk: Pokrytie skúšok (z EAL2), hĺbka skúšok (z EAL3), funkčná skúška (z EAL2) a nezávislé skúšanie (z EAL1). Všimnite si, že skúšanie rieši aj mechanizmus definovaný v ADV_ARC v hĺbke skúšania.

2.7.1 Pokrytie (ATE_COV)

2.7.1.1 Ciele

Cieľom týchto požiadaviek je určiť, či je skúšanie (ako je zdokumentované) dostatočné na to, aby sa zistilo, že TSF bol systematicky skúšaný podľa funkčnej špecifikácie. Pokrytie sa týka úplnosti funkčných skúšok, ktoré vývojár vykonal na TOE.

2.7.1.2 Vstup

Vývojár poskytne dôkaz (v ATE_COV.1, EAL2) / analýzu (z ATE_COV.2, EAL3) o pokrytí skúšok. Táto analýza môže byť súčasťou samotnej testovacej dokumentácie alebo môže byť dodaná samostatne.

2.7.1.3 Požiadavky

Analýza pokrytia skúšok musí zohľadňovať mapovanie medzi skúškami (charakterizačnými a produkčnými skúškami) a TSF opísanými vo funkčnej špecifikácii (bezpečnostné funkcie). Analýza pokrytia musí preukázať, že sú pokryté všetky vlastnosti bezpečnostných funkcií.
Analýza musí preukázať a zdôvodniť, či bola TOE komplexne testovaná. Úplné pokrytie bezpečnostných funkcií a externých rozhraní sa vyžaduje na úrovni EAL3 a vyššej (ATE_COV.2). Od ATE_COV.3 (EAL6) musí analýza preukázať, že všetky externé rozhrania musia byť kompletne otestované. V prípade integrovaného obvodu to môže napríklad znamenať, že sa musí pokryť kompletný súbor inštrukcií procesora so všetkými parametrami.
Pokiaľ ide o pokrytie testov, je potrebné venovať pozornosť zahrnutiu bezpečnostných funkcií, ktoré vyplývajú z návrhu alebo technológie. Preto je potrebné poskytnúť dôkazy o tom, že technické a technologické vlastnosti špecifikované v FSP sú pokryté testami alebo inými vhodnými činnosťami (napr. kontrola rozloženia, masky a čipu).

2.7.2 Hĺbka (ATE_DPT)

2.7.2.1 Ciele

Cieľom týchto požiadaviek je určiť hĺbku skúšania. Hĺbková analýza sa zaoberá úrovňou podrobnosti, do ktorej vývojár testuje TOE. Skúšanie bezpečnostných funkcií je založené na rastúcej hĺbke informácií získaných z analýzy zobrazení TSF, napr. či vývojár skúšal TSF v porovnaní s jeho vysokoúrovňovým návrhom na úrovni EAL3.

2.7.2.2 Vstup

Vývojár poskytne analýzu (z ATE_DPT.1, EAL3) hĺbky skúšky. Táto analýza môže byť súčasťou samotnej testovacej dokumentácie alebo môže byť dodaná samostatne.

2.7.2.3 Požiadavky

Hĺbková analýza testovania, ktorá sa poskytuje pre tieto požiadavky, zohľadňuje mapovanie medzi skúškami (charakterizačnými a výrobnými skúškami) a vnútornými štruktúrami TSF. V závislosti od úrovne hodnotenia sa to vykonáva na:

- základná úroveň návrhu (ATE_DPT.1, na úrovni EAL3);
- úroveň návrhu subsystémov a modulov presadzujúcich bezpečnosť (ATE_DPT.2, na úrovni EAL4);
- úroveň návrhu subsystémov a modulov (ATE_DPT.3, na úrovni EAL5 - EAL6);
- úroveň návrhu subsystémov a modulov a úroveň zobrazenia implementácie (ATE_DPT.4, na úrovni EAL7).

Uplatnenie analýzy hĺbky testovania bude v rozhodujúcej miere závisieť od toho, ako sa pre IC používajú pojmy "subsystémy" a "modul" (pozri CC časť 3, body 276 a 277 a oddiel 2.5.3.3, Základná štruktúra TSF z hľadiska subsystémov a modulov).

Na preskúmanie hĺbky testu by sa mali použiť všetky výstupy poskytnuté na určitej úrovni (napr. blokové schémy, kód HDL, dokumenty o rozložení).

V prípade ATE_DPT.3 sa primeraná hĺbka testovania dosiahne, keď sa otestujú všetky inštrukcie a vetvy celého logického plánu oproti zdrojovému kódu HDL, ktoré patria do modulov vynucujúcich SFR.

Správnosť implementácie (integrácie) a pokrytie testov sa musí preukázať aj po výrobe (pozri ATE_FUN). Testovacie vektory musia byť vhodne zvolené tak, aby pokrývali požiadavky. Analýzy by

sa mali vykonávať týmto spôsobom.

Odôvodnenie hĺbky skúšania na úrovni implementácie sa môže vykonať s ohľadom na jednu z nasledujúcich položiek:

- Vývojár môže, ak je to možné, preukázať, že počas testovania prepol každý uzol modulu.
- Ak sa podľa logického plánu môžu moduly alebo ich časti testovať len paralelne, vývojár musí preukázať, že všetky spoje boli aspoň raz prepnuté prostredníctvom základných testovacích vektorov.
- Ak vývojár nezohľadnil pravidlá testovateľnosti alebo ak testovanie niektorých modulov nie je možné okamžite (testovanie časovača počas 24 hodín), obvod nemožno považovať za 100% otestovaný.
  V tomto prípade sa pokrytie testovaním dosiahne, ak vývojár dokáže preukázať, že všetky križovatky boli dosiahnuté prostredníctvom testovacích vektorov a že neexistujú podmienky, ktoré by ohrozovali bezpečnosť.

Ak sa na hodnotenie integrovaného obvodu používa EAL4, rozšírenie EAL4 o komponent ATE_DPT.3 by mohlo byť rozumné na získanie vyššej bezpečnostnej záruky, pretože nízkoúrovňový návrh bol aj tak poskytnutý a v prípade testovania technických a technologických vlastností je rozumný pohľad na nízkoúrovňový návrh testov.

2.7.3 Funkčná skúška (ATE_FUN)

2.7.3.1 Ciele

Cieľom týchto požiadaviek je určiť, či funkčné skúšanie vývojára preukazuje, že všetky TSFI fungujú tak, ako je špecifikované.

2.7.3.2 Vstup

Vývojár musí testovať TSF a zdokumentovať výsledky. Vývojár poskytne testovaciu dokumentáciu. Pri vykonávaní skúšok sú dôležité najmä dátové listy IC.

2.7.3.3 Požiadavky

Dokumentácia skúšok vývojára musí obsahovať podrobnosti o plánoch skúšok, cieľoch a výsledkoch (skutočných a očakávaných). Keďže ATE_FUN.1 sa používa na úrovni EAL2 až EAL5, množstvo informácií, ktoré sa musia uviesť, sa bude líšiť v závislosti od použitia ATE_COV a ATE_DPT.

Skúšky jednotlivých komponentov TOE alebo kontrola určitých technických alebo technologických vlastností by sa mohli realizovať len v určitom čase počas výrobného procesu alebo len v testovacom režime, pretože po skončení výroby TOE nie je možné logicky ani fyzicky pristupovať k príslušným fyzickým komponentom. Táto skutočnosť by sa mala zohľadniť pri plánovaní skúšok a mala by sa náležite zdokumentovať.

Plán skúšania

Plán skúšania musí uvádzať cieľ skúšok, ktorým je poskytnúť dôkaz o správnosti logiky pomocou simulácie s použitím nástroja HDL a otestovať správnosť implementácie. Keďže skúška je typom kontroly kvality, po simulácii sa musí preukázať, či bola implementácia úspešná. Jednotlivé skúšky na hotovom integrovanom obvode musia preukázať, že implementácia TSFI a mechanizmov je správna a že sú splnené požiadavky na časovanie. Počas skúšania špecifikovanej funkčnosti alebo počas skúšania modulov je potrebné venovať osobitnú pozornosť väzbe modulov, najmä ak existuje paralelná funkčnosť.

Pri testovaní hardvérového TOE sa zvyčajne vykonávajú dva hlavné kroky:

- skúšky prototypu TOE;
- akceptačné skúšky vykonané na každom TOE na konci výrobnej fázy.

Skúšky "prototypu TOE" sú charakterizačné testy, ktoré možno považovať za dôkaz správnej implementácie funkcií na presadzovanie bezpečnosti. Pri skúšaní hardvérových TOE by sa mal zohľadniť časový harmonogram. Skúšky sa môžu realizovať aj na úrovni návrhu pomocou nástrojov HDL (bez oneskorení, s odhadovanými záťažami/oneskoreniami a prípadne po rozložení) alebo vo

forme špeciálnych bezpečnostných skúšok po výrobe s použitím napr. špecifického softvéru, ktorý sa nachádza v TOE (testovací softvér v pamäti ROM a je súčasťou TOE alebo aplikačný testovací softvér v EEPROM, ktorý nie je súčasťou TOE).

Akceptačné skúšky musia potvrdiť a overiť správnu funkciu TOE a komponentov, z ktorých je TOE počas výroby vyrobený. Hodnotitelia preto musia skontrolovať výrobný proces vývojára, ktorý má implementované príslušné akceptačné skúšky. Akceptačné skúšky počas výroby sa zvyčajne vykonávajú pomocou špecifických hardvérových mechanizmov a príkazov implementovaných v testovacom softvéri na čipe.

Rôzne testovacie prostredia použité na hodnotenie sa opíšu v rámci plánu skúšok, napr.

- "Skúšky prototypu TOE:
  - charakterizačné testovacie prostredie
  - simulačné prostredie návrhu počas vývoja
  - prostredie na testovanie bezpečnosti
- akceptačné testovacie prostredie počas výroby.

Zariadenie, ktoré je potrebné pre testovací prípad, musí byť presne špecifikované so všetkými úpravami. To zahŕňa aj presnú identifikáciu testovacích knižníc pre simuláciu, ako aj ovládačový program pre testovacie zariadenie.

Na vykonanie alebo kontrolu výsledkov charakterizačných a akceptačných skúšok, pri ktorých je nevyhnutné špecializované skúšobné zariadenie, môže byť hodnotiteľ nútený byť svedkom a overovať skúšky namiesto ich osobného vykonania. Zvyčajne sa to uskutočňuje prostredníctvom návštevy konštruktéra/výrobcu integrovaného obvodu.

Ak chce vývojár vykonať bezpečnostné skúšky bez simulácie pomocou nástrojov HDL, všetky skúšky sa musia vykonať v reálnom čase, aby sa preukázalo, že implementácia je správna.

Knižnica testovacích programov poskytnutá vývojárom musí obsahovať testovacie programy a nástroje, ktoré umožnia opakovanie všetkých skúšok zahrnutých v testovacej dokumentácii (požadované pre ATE_IND). To môže okrem iného zahŕňať softvér ovládača s príslušným zariadením (testerom) potrebným na skúšanie čipu. To je potrebné aj na opakovanie skúšok. Je potrebné uviesť aj ďalšie nástroje, ktoré boli použité, ako napríklad logický analyzátor, osciloskop, ladiaci program, operačný systém atď.

Plán skúšania určuje rámec testovacích prípadov. V pláne skúšania je veľmi dôležitá presná špecifikácia a rozsah skúšaných prípadov, ako aj dokumentácia popisujúca všetky vstupné parametre a parametre prostredia IC. Tieto parametre sú čiastočne uvedené v dátových listoch. Preto musí byť dátový list neoddeliteľnou súčasťou testovacej dokumentácie.

Testovacie prípady sa môžu pri analógových a digitálnych obvodoch značne líšiť.

Plán skúšania by mal zahŕňať všetky konfigurácie integrovaného obvodu, ak sú špecifikované pre prevádzkové prostredie, napr. rôzne bezpečnostné stavy integrovaného obvodu, ako sú testovací režim a užívateľské režimy v závislosti od fáz životného cyklu, ktoré sa hodnotia.

Okrem funkčných skúšok za štandardných podmienok sa majú naplánovať aj testy (v prípade potreby testy v reálnom čase) za definovaných záťažových podmienok (teplota, frekvencia, napätie, testy cyklu EPROM atď.), pretože takéto podmienky by mohli nastať počas prevádzky TOE (porovnateľné s extrémnymi situáciami pre softvérové TOE, ktoré by mohli viesť k chybám počas behu).

Ak sa počas prevádzky TOE do funkčného toku dynamicky začleňuje externá HW alebo SW funkcionalita, potom by sa mal testovať vzťah externých komponentov na úrovni externého rozhrania.

Medzi testovacími prípadmi a TSFI a testovanými subsystémami, modulmi alebo rozhraniami sa uvedie mapovanie v závislosti od rozsahu a hĺbky skúšania.

Pri plánovaní skúšky je potrebné zohľadniť parametre skúšky. Môžu to byť napríklad:

- testovacie frekvencie s minimálnymi a maximálnymi limitmi
- napájacie napätie zodpovedajúce údajom v technickom liste
- skúšobné teploty
- testovacie vektory na výber testovacích oblastí v IC

Výsledky skúšok

Musí sa opísať spôsob, akým hardvér prezentuje výsledky skúšok (napr. zápis do registra alebo určitej oblasti pamäte, odoslanie cez linku externého rozhrania).

Výsledky skúšok, ktoré sa získajú na špeciálnom skúšobnom zariadení, musia byť prezentované vo forme, ktorá sa dá analyzovať (analógové skúšky, časové skúšky).

V prípade výsledkov skúšok týkajúcich sa paralelne prebiehajúcich funkcií je dôležité priradenie výsledkov ku konkrétnym subsystémom, modulom alebo bezpečnostným mechanizmom. Mali by sa vysvetliť závislosti výsledkov skúšok vyplývajúcich z paralelného spracovania funkcionality.

2.7.4 Nezávislé skúšanie (ATE_IND)

2.7.4.1 Ciele

Cieľom týchto požiadaviek je určiť, či sa TOE správa tak, ako je špecifikované, a získať dôveru vo výsledky testov vývojára nezávislým skúšaním podmnožiny TSF a vykonaním vzorky testov vývojára inou stranou ako vývojárom (napr. treťou stranou).

Táto skupina pridáva hodnotu zavedením skúšok, ktoré nie sú súčasťou skúšok vývojára.

2.7.4.2 Vstup

Vývojár poskytne TOE (z ATE_IND.1) a ekvivalentný súbor zdrojov (z ATE_IND.2). Hodnotiteľ poskytne testovaciu dokumentáciu.

2.7.4.3 Požiadavky

Ekvivalentný súbor zdrojov, ktoré musí vývojár poskytnúť z ATE_IND.2, môže zahŕňať samostatnú vzorku čipov z výroby, samostatný súbor testovacích vektorov a samostatný súbor testovacích údajov potrebných na testovanie.

Hodnotiteľ poskytne testovaciu dokumentáciu. Požiadavky na testovaciu dokumentáciu sú porovnateľné s požiadavkami na testovaciu dokumentáciu vývojára, pokiaľ ide o plán testov, postupy a očakávané
a skutočné výsledky.

Z hľadiska odbornosti musí byť hodnotiteľ schopný zopakovať testy vývojára a vykonať ďalšie testy. Na vykonanie testov potrebuje hodnotiteľ vektory testov, ktoré určujú priebeh testov. V prípade potreby musí byť hodnotiteľ schopný používať nástroje na hodnotenie, ktoré používa výrobca. V mnohých prípadoch to bude vzhľadom na dostupnosť nástrojov možné len vo vývojovom laboratóriu alebo počas výroby u výrobcu. V týchto prípadoch stačí, ak je hodnotiteľ svedkom skúšok u výrobcu.

Okrem funkčných skúšok za štandardných podmienok má hodnotiteľ vykonať aj skúšky (v prípade potreby skúšky v reálnom čase) za definovaných záťažových podmienok (teplota, frekvencia, napätie, skúšky cyklu EPROM atď.), pretože takéto podmienky môžu nastať počas prevádzky TOE a vývojár ich nemusí podrobne testovať.

Dodatočné testy hodnotiteľa sa musia vykonať aspoň na úrovni požadovanej v ATE_DPT. Hodnotitelia musia vykonať aj dodatočné skúšky na dokončenom integrovanom obvode (finálnej časti), pretože:

- chyby by mohli byť spôsobené technológiou a logické testy ich nemusia odhaliť (pozri proces starnutia v bode 322);
- rozptyl parametrov posilňujúcich bezpečnosť a parametrov dôležitých z hľadiska bezpečnosti nie je možné testovať prostredníctvom simulácie. Takýto rozptyl sa dá uskutočniť len prostredníctvom testovania viacerých integrovaných obvodov. Na tento účel musí hodnotiteľ vybrať vhodnú vzorku alebo sa spoľahnúť na výsledky testov kvality výrobcu. Napríklad rozptyl chyby v digitalizácii sa dá zistiť len vtedy, ak sa testuje niekoľko integrovaných obvodov, pretože montáž základných komponentov môže viesť k časovej odchýlke.

2.8 PODPORA ŽIVOTNÉHO CYKLU (TRIEDA ALC)

Trieda záruk ALC definuje požiadavky na určenie primeranosti bezpečnostného postupu, ktorý vývojár

používa na ochranu rozvojového a výrobného prostredia TOE. Tieto postupy zahŕňajú model životného cyklu, riadenie konfigurácie, riešenie bezpečnostných chýb, nástroje a bezpečnostné opatrenia používané počas vývoja TOE a činnosti súvisiace s dodávkou.

Ako je definované v § 139 časti 1 OZ, "vývoj" tu znamená vývoj a výrobu.

2.8.1 Schopnosti CM (ALC_CMC)

2.8.1.1 Ciele

Schopnosti riadenia konfigurácie definujú požiadavky zabezpečenia toho, aby vývojár jasne a jednoznačne identifikoval TOE pomocou automatizovaného konfiguračného systému. Systém CM zabezpečuje správnosť a úplnosť TOE počas vyhodnocovania a pred odoslaním zákazníkovi a zabraňuje akejkoľvek neoprávnenej modifikácii, pridaniu alebo vymazaniu konfiguračných položiek.

2.8.1.2 Vstup

Úrovne EAL4 a EAL5 vyžadujú ALC.CMC.4.

Investor poskytne dokumentáciu CM, ktorá obsahuje plán CM.

2.8.1.3 Požiadavky

Plán CM musí opisovať, ako sa používa systém CM (ALC_CMC.4.7C) a ako sa riadi modifikácia alebo pridávanie konfiguračných položiek TOE (ALC_CMC.4.8C) pomocou automatizovaných opatrení (ALC_CMC.4.4C).

Systém CM musí byť schopný automaticky generovať TOE (ALC_CMC.4.5C)

TOE musí byť označený jedinečným odkazom (ALC_CMC.4.1C) a všetky konfiguračné položky musia byť jednoznačne identifikované. (ALC_CMC.4.3C)

Konfiguračný systém a akceptačné postupy by sa mali zohľadňovať počas celého procesu vývoja a výroby TOE. Okrem všetkých relevantných dátových súborov pre všetky kroky vývoja musia byť v pozícii, aby mohli kontrolovať aj konštrukčné plány a hardvérové časti. V prípade potreby sa do toho majú zahrnúť aj rôzne miesta vývoja a výroby.

Hodnotiteľ by mal zabezpečiť, aby TOE obsahovalo jedinečný odkaz, aby bolo možné rozlíšiť rôzne verzie TOE. TOE môže poskytovať metódu, pomocou ktorej sa dá ľahko identifikovať. V prípade hardvérových TOE to môže byť číslo dielu fyzicky vyrazené na TOE. Okrem toho môže byť každá vrstva masky TOE fyzicky identifikovateľná pomocou akéhokoľvek druhu identifikátorov.

V niektorých prípadoch však môže byť potrebné, aby sa útok sťažil, označiť IC (alebo čipy v nich uložené) neviditeľnými logami alebo identifikátormi. V takýchto prípadoch však musí výrobca nájsť vhodne skrytú možnosť pre označenie na TOE, ako napríklad v neodstrániteľnej oblasti pamäte s prístupom len pre oprávnených používateľov.

Pracovná jednotka hodnotiteľov v ACM_CMC.4.5C/EAL4 na preskúmanie postupov tvorby TOE má za cieľ získať dôkazy o efektívnosti systému kontroly konfigurácie vzhľadom na rôzne verzie a zmeny TOE. Je potrebné preukázať, že systém kontroly konfigurácie podporuje proces generovania, aby pomohol znížiť pravdepodobnosť ľudskej chyby. Proces generovania teda využíva vhodné návrhové nástroje (HDL / CAD nástroje). Toto by sa malo opísať.

V prípade IC TOE pozostávajúceho z hardvéru a softvéru (napr. softvér testovacej pamäte, operačný systém, aplikačný softvér smart karty v závislosti od konkrétneho rozsahu TOE) sa pravdepodobne bude rozlišovať medzi kontrolou konfigurácie hardvéru a softvéru. Existuje ďalšia požiadavka na spojenie správnej dvojice hardvér - softvér, čo znamená, že sa musí použiť správna maska. To zase znamená, že systém kontroly konfigurácie musí byť schopný spravovať dvojice hardvér - softvér tvoriace TOE. Keďže všetky masky sa vytvárajú zo súborov s údajmi o maskách, musí sa zabezpečiť, aby sa masky vytvárali z ich správneho softvérového obrazu.

V závislosti od rozsahu TOE môže byť zostavenie správneho páru hardvér - softvér čiastočne

aspektom riadenia konfigurácie TOE alebo postupov dodávky (pozri ALC-DEL).

Túto pracovnú jednotku pre generovanie TOE nie je možné priamo prepojiť s technologickým procesom špecifického IC zákazníka, pretože tento proces nie je možné zopakovať v prospech hodnotiteľa.
V tomto prípade však hodnotiteľ musí vykonať audit kontroly konfigurácie v technologickom procese, aby zaručil, že sa používajú správne masky, ktoré patria ku konkrétnej verzii TOE, a že organizačné opatrenia sú v procese účinné.

V prípade programovateľných štandardných integrovaných obvodov (PLD, FPGA), v ktorých sa hardvérová konfigurácia programuje prostredníctvom firmvéru, môže byť pracovná jednotka podporovaná programovaním nového integrovaného obvodu. Hodnotiteľ potom vykoná porovnávacie testy funkcií novovytvoreného integrovaného obvodu s pôvodným TOE (čo sa dá prirovnať k "porovnávaniu súborov" pre opätovne vytvorený softvérový TOE).

2.8.2 Rozsah CM (ALC_CMS)

2.8.2.1 Ciele

Cieľom týchto požiadaviek je identifikovať položky, ktoré sa majú zahrnúť do zoznamu konfigurácií, a teda zaradiť do požiadaviek CM podľa ALC_CMC.

2.8.2.2 Vstup

EAL4 vyžaduje ALC_CMS.4 , EAL5 vyžaduje ALC_CMS.5. Vývojár poskytne zoznam konfigurácií TOE.

2.8.2.3 Požiadavky

Zoznam konfigurácie obsahuje samotný TOE, dôkazy o hodnotení požadované v SAR, časti, ktoré tvoria TOE, zobrazenie implementácie, správy o bezpečnostných chybách a stav riešenia (ALC-

CMS.4.1C). Okrem toho sa pre úroveň EAL5 v zozname konfigurácie zohľadňujú vývojové nástroje a súvisiace informácie (ALC_CMS.5.1C).

Vývojár vykonáva správu konfigurácie implementácie TOE (hardvérové schémy/rozvrhnutie), projektovej dokumentácie, testov, pokynov pre používateľov a správcov, dokumentácie správy konfigurácie a bezpečnostných chýb so stavom ich riešenia.

Riadenie konfigurácie musí byť zavedené pre návrh integrovaného obvodu (schémy, rozloženie), ako aj pre vlastný softvér integrovaného obvodu (zdrojový kód, dokumentácia). Musia byť zahrnuté všetky zdrojové súbory potrebné na generovanie TOE, ako aj identifikácia súboru masiek potrebných na výrobu TOE. V prípade masiek to zahŕňa jedinečný identifikátor masky, ako aj číslo verzie alebo číslo revízie každej vrstvy.

Keďže systém riadenia konfigurácie musí byť schopný spravovať páry hardvér-softvér ako súčasť TOE (pozri ALC_CMC), v ALC_CMS musí byť evidencia, ktorý konkrétny pár hardvér-softvér sa používa pre TOE.

Identifikácia a uvedenie modulov návrhu v konfiguračnom zozname sa zdá byť ťažké aplikovať na integrované obvody. Keďže v rámci návrhu môžu byť funkčné bloky prevzaté z knižnice HDL alebo CAD vývojára a z technologickej knižnice výrobcu IC (zoznamy technologických parametrov). Prinajmenšom musia byť jasne identifikované knižnice ako celok, ktoré sa používajú, spolu s možnými parametrami, ktoré sa používajú, ak jednotlivé komponenty knižnice nemajú vlastný identifikátor.

Informácie o testovaní, na ktoré sa vzťahuje CM, zahŕňajú všetky časti, ktoré sú potrebné na vytvorenie a testovanie TOE. To zahŕňa všetky testovacie zariadenia, knižnice a zoznam testovacích vektorov použitých počas testovania, ako aj súbor testov vrátane testovacích údajov a výsledkov.

ALC_CMS.4.3C a ALC_CMS.5.3C vyžaduje, aby sa v konfiguračnom zozname uviedol vývojár položky. Ako je definované v CC3.1 časť 1 § 138, "vývojár" sa tu vzťahuje na organizáciu zodpovednú za vývoj položky. To znamená napr. každý vývojár dodatočnej softvérovej časti (knižnice), ktorú má TOE používať (pozri CC 3 časť 3 § 352). Zámerom je poskytnúť dôkazy o pôvode častí TOE poskytnutých od externých dodávateľov alebo ak sa vývoj vykonáva v rámci rôznych organizácií.

2.8.3 Doručovanie (ALC_DEL)

Skupina záruk ALC_DEL definuje požiadavky na opatrenia, postupy a normy týkajúce sa bezpečného dodania TOE, čím sa zabezpečí, že bezpečnostná ochrana poskytovaná TOE nebude počas prenosu ohrozená.

2.8.3.1 Ciele

Cieľom týchto požiadaviek je určiť, či sú postupy doručovania zdokumentované a či sa zachováva integrita a zisťovanie modifikácie alebo zámeny TOE pri distribúcii TOE na miesto používateľa. Zahŕňa osobitné postupy alebo operácie potrebné na preukázanie autentickosti dodaného TOE. Takéto postupy
a opatrenia sú základom na zabezpečenie toho, aby počas prenosu nebola ohrozená bezpečnostná ochrana, ktorú TOE poskytuje.

2.8.3.2 Vstup

Vývojár poskytne používateľovi postupy dodania TOE alebo jeho častí. Postupy musia byť opísané a používané.

2.8.3.3 Požiadavky

Požiadavky sa týkajú doručovania používateľom. Podľa CC časť 3 § 365 sa neuvažuje o preprave od subdodávateľov k vývojárom alebo medzi rôznymi lokalitami, ale v ALC_DVS.

Preskúmanie procesu dodávky s cieľom zistiť, či sa používajú postupy dodávky, sa zvyčajne vykonáva počas inšpekcie na mieste. Overuje sa vysledovateľnosť toho, čo kto komu dodal. Osobitná pozornosť sa venuje "paralelným dodávkam", ako sú vzorky na kontrolu kvality, vyradené vzorky, preverené procesy.

V prípade potreby by sa mali dodržiavať postupy dodávky schválené národným certifikačným orgánom.

Všimnite si, že na ochranu dodávky čipu od výrobcu čipu výrobcovi karty/personalizačnému centru sa môže použiť osobitný mechanizmus autentizácie (napr. fab-key, transportný kľúč).

V prípade integrovaných obvodov je dôležitý stav zabezpečenia čipu (testovací režim, užívateľský režim) počas dodávky. Funkcionalita na deaktiváciu testovacieho hardvéru alebo na prechod
z testovacieho režimu alebo režimu inštalácie do používateľského režimu/prevádzkového režimu je dôležitá v kontexte analýzy zraniteľnosti a autentickosti dodaného TOE. Mala by sa tu uviesť s odkazom na opis v AGD_PRE.

Proces výroby a dodávky TOE musí zahŕňať výrobné testy, ktoré zabezpečia správnu funkciu každého exemplára TOE dodaného zákazníkovi. Výsledky týchto testov sa musia zdokumentovať.

2.8.4 Bezpečnosť vývoja (ALC_DVS)

2.8.4.1 Ciele

Cieľom týchto požiadaviek je určiť, či sú postupy vývojového a výrobného prostredia primerané na zabezpečenie dôvernosti a integrity návrhu, implementácie a výroby TOE, ktoré sú potrebné na zabezpečenie toho, aby nebola ohrozená bezpečná prevádzka TOE.

2.8.4.2 Vstup

Vývojár poskytne bezpečnostnú dokumentáciu vývoja.

2.8.4.3 Požiadavky

ALC_DVS.1.1C vyžaduje, aby dokumentácia opisovala všetky bezpečnostné postupy použité na ochranu TOE počas vývoja. ALC_DVS.2.2C navyše vyžaduje, aby dokumentácia zdôvodňovala, že bezpečnostné opatrenia poskytujú potrebnú úroveň ochrany.

Všimnite si, že ALC_DVS poskytuje možnosť definovať úroveň bezpečnosti Dôvernosti a Integrity. Odvolávajúc sa na CC časť 3 §14.4 374 " *Uznáva sa, že dôvernosť nemusí byť vždy problémom pre ochranu TOE v jeho rozvojovom prostredí. Použitie slova "nevyhnutné" umožňuje výber vhodných ochranných opatrení*. " Napríklad v prípade "softvéru s otvoreným zdrojovým kódom" sa nevyžaduje žiadna dôvernosť.

Počas životného cyklu hardvéru TOE sa skúmajú bezpečnostné postupy vývoja a výroby. Musia sa zohľadniť všetky príslušné miesta vývoja a výroby TOE, aby bezpečnostné požiadavky platili pre všetky fázy životného cyklu až do konečného dodania TOE v rámci hodnotenia. Je to obzvlášť dôležité, pretože požiadavky na technológiu sa nakoniec realizujú až počas výroby integrovaných obvodov vrátane testov správnej funkcie všetkých príkladov TOE dodaných odberateľovi. Skúška zahŕňa všetky kroky vývojového a výrobného procesu; ide o tieto miesta:

- vývoj špecializovaného softvéru a hardvéru (návrhové centrum),
- miesto na vytvorenie obrazu aplikačného softvéru (ak je to vhodné),
- výrobca sieťok (výrobca masky),
- výroba (fab site),
- testovanie (testovacie miesto),
- balenie (mikromontáž a testovanie) v závislosti od rozsahu TOE.

V špecifických prípadoch môže existovať samostatné návrhové centrum pre určité bunky, ktoré nie sú špecifické pre TOE (napr. štandardná bunka CPU, štandardná pamäťová bunka). Pre požiadavku ALC_DVS.1 môže existovať dostatok dôkazov o tom, že tieto preddefinované bunky (nevynucujúce bezpečnosť, ale prípadne podporujúce bezpečnosť) sú funkčne správne a celistvé, ak sú zavedené príslušné postupy dodávok, testy a dohody o dôvernosti. V tomto prípade by sa toto projektové stredisko nemuselo posudzovať v rámci ALC_DVS. S miestom výrobcu masky sa môže zaobchádzať zodpovedajúcim spôsobom.

Kontrolujú sa všetky bezpečnostné operačné postupy. Kontrola sa zvyčajne vykonáva počas inšpekcií na mieste. Kontrolujú sa aj postupy subdodávateľov. Je potrebné poznamenať, že na podporu týchto hodnotiacich činností by bol potrebný prístup hodnotiteľa do výrobného závodu, odborný personál a nástroje.

Postupy zahŕňajú tieto typy:

- fyzická (bezpečnosť pracoviska: kontrola prístupu);
- procedurálne (udelenie prístupu k vývojovým nástrojom, zrušenie prístupu, prenos chráneného materiálu, prijímanie a sprevádzanie návštevníkov, bezpečnostná politika vývoja...);
- zamestnancov (proces previerky nových zamestnancov pre rozvoj...);
- Bezpečnostné opatrenia IT (identifikácia a autentizácia, kontrola prístupu, archivácia, audit, siete, firewally...).

Ďalšie citlivé oblasti v rámci uvedených lokalít môžu byť:

- riadenie procesu (integrácia obvodov na kremík);
- produktové inžinierstvo (analýza chýb vzhľadom na proces);
- kontrola kvality bezpečnostných funkcií;
- skladovanie / dodávka.

TOE sa nachádza v rôznych štádiách vývoja a výroby v rôznych fyzických podobách. Osobitný význam má celistvosť masiek rozloženia. Tento aspekt bude podporovať bezpečné dodanie (pozri ALC_DEL).

Fyzické, procedurálne, personálne a iné opatrenia potrebné na realizáciu bezpečnostných vlastností TOE, ako sú uvedené v bezpečnostnom zámere, sa prenesú do vývoja a výroby a budú mať vplyv na bezpečnosť v prevádzkovej fáze TOE. Tieto opatrenia sa majú tiež zdokumentovať a preskúmať. Dôležité sú najmä opatrenia vo fáze testovania, prípadne aj vo fáze montáže, a opatrenia na riadenie výrobného procesu.

Na porovnanie, kompilácia softvéru TOE prebieha s pevne stanovenými možnosťami jednoznačne vo rozvojovom prostredí (prototyp a hlavná kópia). Sériová výroba softvéru je jednoducho proces kopírovania, v ktorom zohrávajú úlohu aspekty integrity kópie vzhľadom na hlavnú kópiu.

Pokiaľ ide o IC TOE, v rámci vývoja sa vytvoria výkresy a súvisiace dátové súbory. Výroba prototypu IC, ako aj série je v podstate zložitejšia ako proces kopírovania v prípade softvéru a je variabilná

prostredníctvom množstva parametrov procesu, s ktorými potenciálne manipuluje personál.

Testovacia fáza počas výroby IC má mimoriadny význam, pretože v tejto fáze je už IC fyzicky úplne k dispozícii, ale napríklad vnútorné štruktúry IC sú však nastaviteľné alebo môžu byť ohrozené prostredníctvom testovacieho režimu, ktorý je stále aktivovaný.

Dôležité môžu byť opatrenia, ktoré sa prijímajú s cieľom označiť (atramentom) chybné kocky na waferi a vytriediť chybné TOE (finálne diely), vrátane kritérií, ktoré sa majú vybrať. Potom by sa mali opísať opatrenia na zničenie chybných dielov.

2.8.5 Odstraňovanie chýb (ALC_FLR)

2.8.5.1 Ciele

Odstraňovanie chýb zabezpečuje, že chyby zistené používateľmi TOE sa budú sledovať a opravovať, kým bude TOE podporovaný vývojárom. Hoci pri hodnotení TOE nie je možné určiť budúci súlad s požiadavkami na nápravu chýb, je možné vyhodnotiť postupy a politiky, ktoré má vývojár zavedené na sledovanie a opravu chýb a na distribúciu spotrebiteľom.

2.8.5.2 Vstup

Vývojár zdokumentuje postupy odstraňovania chýb.

2.8.5.3 Požiadavky

Táto skupina CC nie je povinná pre preddefinované balíky EAL. Napriek tomu je možné vybrať jeden z komponentov záruk ALC_FLR v rámci ST rozšírením EAL.

Aspekty odstraňovania chýb by sa mohli kombinovať s používaním programu údržby hodnotenia.

2.9 Definícia životného cyklu (ALC_LCD)

2.9.1 Všeobecné poznámky

2.9.1.1 Ciele

Cieľom týchto požiadaviek je určiť, či vývojár použil zdokumentovaný model životného cyklu TOE pre vývoj a údržbu.

Definícia životného cyklu stanovuje, že inžinierske postupy používané vývojárom na vytvorenie TOE zahŕňajú úvahy a činnosti identifikované v procese vývoja a v požiadavkách na prevádzkovú podporu.

Dôvera v zhodu medzi požiadavkami a TOE je väčšia, ak sa bezpečnostná analýza a tvorba dôkazov vykonáva pravidelne ako neoddeliteľná súčasť procesu vývoja a činností operačnej podpory. Zámerom tohto komponentu nie je diktovať akýkoľvek špecifický rozvojový proces.

2.9.1.2 Vstup

Vývojár poskytne definíciu životného cyklu (z EAL4).

2.9.1.3 Požiadavky

Opis modelu by mal obsahovať informácie o postupoch, nástrojoch a technikách, ktoré vývojár používa na vývoj a údržbu TOE.

Príklad modelu životného cyklu je podrobne uvedený v ochrannom profile bezpečnostného integrovaného obvodu [BSI-CC-PP-0084-2014]. Tento model spresní vývojár.

Základný opis sa vyžaduje pri ALC_LCD.1 / EAL4 až EAL6, zatiaľ čo pri ALC_LCD.2 / EAL7 musí byť použitý model životného cyklu založený na merateľnom modeli životného cyklu, t. j. na modeli, ktorý

bol schválený akademickými odborníkmi alebo normalizačnými orgánmi.

2.9.2 Nástroje a techniky (ALC_TAT)

2.9.2.1 Ciele

Cieľom týchto požiadaviek je určiť, či vývojár použil na vývoj, analýzu a implementáciu TOE dobre definované nástroje (napr. programovacie jazyky alebo systémy počítačom podporovaného navrhovania (CAD)), ktoré poskytujú konzistentné a predvídateľné výsledky.

Zahŕňa požiadavky týkajúce sa vývojových nástrojov a možností implementácie týchto nástrojov.

2.9.2.2 Vstup

Vývojár poskytne dokumentáciu k vývojovým nástrojom používaným pre TOE (z EAL4).

2.9.2.3 Požiadavky

Aspekt hodnotenia nástrojov a techník sa vzťahuje na softvérové aj hardvérové TOE.

Pri posudzovaní nástrojov a techník pre softvérové TOE je potrebné získať dôkazy o tom, či sú použité vývojové nástroje jednoznačne a dobre definované a zdokumentované a či boli zdokumentované všetky možnosti týchto nástrojov. Z implementačných štandardov ALC_TAT.2/EAL5 sa musia uplatniť. Cieľom je tu okrem vyššej bezpečnostnej záruky o správnej implementácii TOE aj zabezpečenie opakovateľnosti konštrukcie TOE. Požadované potvrdenie hodnotiteľa, že implementačné štandardy boli uplatnené, si môže vyžadovať návštevu všetkých príslušných miest. Preto je potrebné poznamenať, že na podporu týchto hodnotiacich činností by bol potrebný prístup hodnotiteľa do výrobného závodu, odborný personál a nástroje.

V prípade špecializovaného softvéru integrovaného obvodu to zodpovedá nástrojom na vývoj softvéru.

Používanie vývojových nástrojov sa zdokumentuje. To zahŕňa najmä opis kompilačného reťazca pre zdrojový kód softvéru (ak je to vhodné) a reťazca syntézy pre HDL. Všetky možnosti musia byť zdokumentované a parametre musia byť jasne identifikované. Hodnotiteľ overí tento reťazec nástrojov, zvyčajne počas kontroly na mieste.

Na dosiahnutie cieľa ALC_TAT pre hardvérový TOE je potrebné zdokumentovať a otestovať jazyky na opis hardvéru (HDL), prvky zobrazenia (grafické logické prvky) a nástroje (napr. kompilátor HDL, simulačné nástroje a nástroje CAD) používané v hardvéri. Okrem toho je potrebné zvážiť podporné knižnice. Dôležitá je jasná a presná definícia všetkých prvkov a možností použitých pre TOE.

V prípade softvéru môžu rôzne kompilátory vytvárať rôzne objektové kódy aj pri rovnakej funkčnosti TOE (t. j. pri rovnakom logickom návrhu). Funkcionalita je definovaná príkazmi procesora a použitými možnosťami kompilátora.

V prípade, že mikročipy IC majú rôzne masky, môžu v dôsledku rôznych technológií vzniknúť rozdielne fyzické implementácie, aj keď funkčnosť môže byť rovnaká (t. j. s rovnakým logickým návrhom na úrovni schémy zapojenia). Funkcionalita je nakoniec definovaná len prostredníctvom štruktúry buniek, ktorá bola implementovaná do kremíka. V dôsledku toho je potrebné špecifikovať technológiu použitú na implementáciu čipu. Na vysokých úrovniach záruky sa musia zdokumentovať parametre použitej technológie.

Na objasnenie sú v nasledujúcej tabuľke uvedené procesy vývoja hardvérových integrovaných obvodov a softvéru:

Tabuľka 2: *Procesy vývoja hardvérových integrovaných obvodov a softvéru*

Softvér	Hardvér
Zadávanie textu programu prostredníctvom editora na	Vytvorenie logického plánu prostredníctvom grafického vstupu cez CAD nástroj alebo textového vstupu cez

vytvorenie zdrojového súboru. Syntax a sémantiku vstupného jazyka určí kompilátor.	HDL-Editor. Syntax a sémantika grafických symbolov sa určuje prostredníctvom nástroja CAD a technológie. Na modelovanie a simuláciu návrhu obvodu sa použije HDL.
Na vytvorenie funkčného softvéru TOE je potrebných niekoľko krokov: Určenie úprav kompilátora a linkera, napríklad na realizáciu určitých možností optimalizácie. Kompilácia a spájanie zdrojových súborov do programu, ktorý je spustiteľný z procesora počas jeho behu (objektové súbory ako dátové súbory programu, knižnica času behu, programový kód pre hardvérovú pamäť). Testovanie a odstraňovanie chýb v rámci kompilácie jednotlivých zdrojových súborov, ako aj celého TOE.	Na to, aby sa z návrhu skonštruoval funkčný integrovaný obvod, je potrebných niekoľko krokov: Konštrukcia netlistu z logických plánov a syntéza štruktúry hradiel, ako aj testovacej štruktúry. Simulácia tejto logiky na úrovni hradiel a na úrovni rozloženia s použitím predvoleného časovania. Konštrukcia rozloženia a masiek. Výroba mikročipu z týchto masiek po niekoľkých procesných krokoch, ktoré závisia od použitej polovodičovej technológie (napr. 0,8 mm CMOS, BiCMOS alebo bipolárna technológia).

Použitý programovací jazyk je založený na vlastnostiach kompilátora, interpretera alebo asemblera, zatiaľ čo logika, ktorá bola vytvorená pomocou HDL, je nakoniec k dispozícii až po ukončení technologického procesu.
Preto je potrebné tento aspekt bezpečnostnej záruky chápať v zmysle "nástrojov, techník a technológií".

2.10 SPRIEVODNÁ DOKUMENTÁCIA (TRIEDA AGD)

Komponenty záruk podľa Spoločných kritérií v skupinách AGD_OPE (Používateľská príručka) a AGD_PRE (Postup prípravy) "*opisujú všetky relevantné aspekty bezpečného používania TOE*".

2.10.1 Používateľská príručka (AGD_OPE)

2.10.1.1 Ciele

Dokumenty používateľskej príručky by mali poskytovať len informácie, ktoré sú potrebné na používanie TOE. V závislosti od príjemcu tejto Sprievodnje dokumentácie môžu byť v tom istom dokumente uvedené Prevádzkové a prípravné používateľské príručky.

TOE slúži ako platforma pre vstavaný softvér bezpečnostného integrovaného obvodu. Preto je úloha vývojára vstavaného softvéru bezpečnostného integrovaného obvodu hlavným cieľom tohto usmernenia.

2.10.1.2 Vstup

Vývojár poskytne sprievodnú dokumentáciu. Na podporu týchto požiadaviek by sa mohol považovať technický list integrovaného obvodu.

2.10.1.3 Požiadavky

Ak TOE poskytuje bezpečnostné funkcie, ktoré môže alebo musí spravovať vstavaný bezpečnostný softvér IC, alebo ak špecializovaný podporný softvér IC poskytuje dodatočné služby, tieto aspekty musia byť opísané v návode.

Väčšina bezpečnostných funkcionalít účinná už pred dodaním TOE. Ak je však konfigurácia možná po dodaní TOE (to znamená buď vývojárom zabudovaného softvéru bezpečnostného integrovaného obvodu, alebo výrobcom zloženého produktu), musia sa poskytnúť pokyny na určenie správania bezpečnostnej funkcie, na jej vypnutie, povolenie alebo úpravu správania bezpečnostnej funkcie. Toto usmernenie dodáva výrobca TOE.

Ak sa zložený produkt (s TOE ako hlavným prvkom) používa v termináli, kde sa komunikácia uskutočňuje prostredníctvom rozhrania, ktoré poskytuje TOE v kombinácii so vstavaným softvérom bezpečnostného integrovaného obvodu, potom sa usmernenie sa musí poskytnúť vývojárovi terminálu. Ide o informácie o fyzických vlastnostiach zariadenia, rozhraní a štandardných protokoloch,

ak ich TOE implementuje.

Usmernenia nesmú obsahovať údaje týkajúce sa bezpečnosti, ktoré nie sú potrebné na používanie alebo správu bezpečnostných funkcionalít TOE.

2.10.2 Postup prípravy pre používateľov (AGD_PRE)

2.10.2.1 Ciele

Postup prípravy pre používateľov sú určené pre osoby zodpovedné za bezpečné prijatie a inštaláciu TOE, ako aj za bezpečnú prípravu prevádzkového prostredia správnym spôsobom na dosiahnutie maximálnej bezpečnosti.

2.10.2.2 Vstup

Skupina AGD_PRE sa zaoberá činnosťami pri preberaní dodávok. V prípade hardvérovej platformy zahŕňa postupy, ktoré sa môžu použiť na identifikáciu TOE a prípadne na overenie autentickosti tejto časti TOE.

2.10.2.3 Požiadavky

TOE sa môže konfigurovať po výrobe pred dodaním zloženého produktu spotrebiteľovi. V takom prípade je potrebné zohľadniť tieto konfiguračné aspekty.

Príprava môže zahŕňať napr. stiahnutie bezpečnostného vstavaného softvéru IC. Ak TOE obsahuje softvér, ktorý sa dodáva samostatne, príprava zahŕňa integráciu vyhradeného podporného softvéru IC. Príprava zahŕňa aj konfiguráciu TOE podľa možností opísaných v bezpečnostnom zámere, ktoré sa môžu zmeniť po dodaní TOE. V riadiacej dokumentácii sa opíšu všetky príslušné postupy.

2.11 POSUDZOVANIE ZRANITEĽNOSTI (TRIEDA AVA)

Trieda AVA: Posudzovanie zraniteľnosti sa zaoberá možnosťou zneužiteľných zraniteľností, ktoré sa vyskytli pri vývoji alebo prevádzke TOE. Pozostáva len z jednej skupiny analýzy zraniteľnosti AVA_VAN, ktorá zahŕňa všetky aspekty posudzovania zraniteľnosti.

2.11.1 Analýza zraniteľnosti (AVA_VAN)

2.11.1.1 Ciele

Analýza zraniteľnosti je posúdenie s cieľom určiť, či potenciálne zraniteľnosti identifikované počas hodnotenia vývoja a predpokladanej prevádzky TOE alebo inými metódami (napr. hypotézami chýb alebo kvantitatívnou či štatistickou analýzou bezpečnostného správania základných bezpečnostných mechanizmov) by mohli útočníkom umožniť porušenie SFR.

Odstupňovanie komponentov skupiny AVA_VAN je založené na zvyšujúcej sa prísnosti analýzy zraniteľností hodnotiteľom a zvyšujúcej sa úrovni potenciálu útoku, ktorý útočník potrebuje na identifikáciu a využitie potenciálnych zraniteľností.

2.11.1.2 Vstup

Analýza zraniteľnosti je predmetom hodnotenia. Vývojár musí poskytnúť TOE na penetračné testovanie.

Hodnotitelia využívajú všetky informácie, ktoré získali, a berú do úvahy všetky potenciálne slabé miesta, ktoré sa vyskytli počas vykonávania iných hodnotiacich činností. Analýza zraniteľností vychádza
z analýzy vykonanej hodnotiteľom a je podporená testovaním hodnotiteľa.

2.11.1.3 Požiadavky

Všeobecné aspekty analýzy zraniteľnosti

V časti B.1 CEM sa uvádzajú tri hlavné faktory pri vykonávaní analýzy zraniteľnosti, a to:

a) identifikáciu potenciálnych zraniteľností;
b) posúdenie s cieľom určiť, či by identifikované potenciálne zraniteľnosti mohli umožniť útočníkovi s príslušným potenciálom útoku narušiť SFR.
c) penetračné testovanie s cieľom určiť, či sú identifikované potenciálne zraniteľnosti zneužiteľné v operačnom prostredí TOE.

Predmetom analýzy je posudzovanie odolnosti TOE proti útoku. Hodnotiteľ preto môže použiť verejne dostupnú dokumentáciu o potenciálnych zraniteľnostiach a potenciálne chybách len ako základ pre analýzu. Hodnotiteľ musí brať do úvahy aj modifikácie a vylepšenia známych útokov na overenie odolnosti TOE. Podrobné informácie o návrhu TOE môžu podporiť prispôsobenie útokov a podporiť analýzu odolnosti voči konkrétnym krokom útoku.

Táto práca si vyžaduje odborné znalosti a vybavenie uvedené v prílohe 8, MINIMÁLNE POŽIADAVKY NA ITSEF PRE HODNOTENIA BEZPEČNOSTI SMART KARIET A PODOBNÝCH ZARIADENÍ. Hodnotiteľ musí vykonať penetračné testy minimálne v takom rozsahu, aby sa celkové hodnotenie cesty útoku dalo dokázať na základe poskytnutých výsledkov testov.

Vývojové a prevádzkové zraniteľnosti

Zraniteľnosti sa môžu vyskytnúť tak pri konštrukcii samotného mechanizmu, ako aj pri výrobe technických a technologických opatrení určených na boj proti hrozbám. Efektívnosť funkčnosti závisí od technológie použitej vo fáze implementácie. Túto skutočnosť je potrebné zohľadniť pri analýze zraniteľností.

Vývoj zraniteľností využíva niektorú vlastnosť TOE, ktorá bola zavedená počas jeho vývoja, napr. prekonanie vlastnej ochrany TSF prostredníctvom manipulácie, priameho útoku alebo monitorovania TSF, prekonanie oddelenia domény TSF prostredníctvom monitorovania alebo priameho útoku na TSF alebo prekonanie neobchádzateľnosti prostredníctvom obídenia (bypassing) TSF.

Operačné zraniteľnosti využívajú slabiny netechnických protiopatrení na porušenie SFR TOE,

napr. nesprávne používanie alebo nesprávna konfigurácia. Hodnotiteľ by mal analyzovať a posúdiť všetky spôsoby, ktorými môže byť SFR deaktivovaný, obídený alebo poškodený. Táto analýza musí poskytnúť argumenty, prečo sa zraniteľnosť nedá zneužiť v prostredí TOE.

Prevádzkové zraniteľnosti sa majú posudzovať aj v kontexte používania čipu operačným systémom alebo vývojárom aplikácií. Napríklad bezpečnostné opatrenia, ktoré by sa mali prijať pri vývoji aplikácie a ktoré ovplyvňujú prevádzku čipu, by mohol útočník prípadne zneužiť (napr. požiadavky na externú kabeláž, externé technické parametre alebo opatrenia na utajenie).

Pri analýze zraniteľnosti by sa mal zohľadniť proces starnutia IC. Tak napríklad zraniteľnosť IC TOE môže spočívať v technológii polovodičov. Bunky E2PROM vydržia len obmedzený počet programovacích cyklov. Obmedzenie počtu možných cyklov vymazania a zápisu bunky je vnútornou zraniteľnosťou, ktorú by útočník mohol prípadne využiť. Tento druh technologicky založenej analýzy zraniteľnosti je na rozdiel od softvérových TOE nový a vyžaduje si analýzu zraniteľnosti týkajúcu sa technológie a jej implementácie.

Typické zraniteľnosti

V prípade smart kariet a podobných zariadení sa za základ pre vyhľadávanie potenciálnych zraniteľností považuje príloha 7, UPLATNENIE POTENCIÁLU ÚTOKU NA SMART KARTY
A PODOBNÉ ZARIADENIA. Ostatné činnosti sa vykonajú v súlade so štandardným postupom CC, ktorý je zdokumentovaný v CC, CEM a inej dokumentácii EUCC.

Hardvérové TOE môžu byť vystavené zraniteľnostiam, ktoré možno zneužiť fyzickou manipuláciou s TOE. Pokiaľ ide o útoky, ktoré fyzicky modifikujú vnútorné technické štruktúry TOE, ide o nepriamy útok, ktorý je potrebné preskúmať v kontexte analýzy zraniteľností, pretože bezpečnostné prvky môžu byť obídené, a preto môžu stratiť svoju efektívnosť. Takáto manipulácia by mohla obísť efektívnosť iných bezpečnostných mechanizmov. Okrem toho je potrebné vziať do úvahy väzbu odlišných komponentov realizovaných v mechanizmoch. Tento aspekt sa musí zohľadniť počas posudzovania zraniteľnosti a penetračného testovania.

Pri analýze zraniteľnosti by sa mali brať do úvahy aspekty väzby vzhľadom na zraniteľnosti, ktoré môžu vzniknúť v dôsledku problémov s väzbou, ak sa bezpečnostné funkcie TOE navzájom nepodporujú alebo netvoria integrovaný a účinný celok. Konkrétne sa rieši otázka nepriameho útoku na IC, napr:

- fyzické prepojenia medzi fyzickými komponentmi vo forme signálových ciest a obvodov;
- fyzické prepojenia medzi fyzickými komponentmi z dôvodu usporiadania (t. j. že informácie o technickej a technologickej realizácii musia mať určitý vplyv na analýzu);
- dynamické prelínanie v časovom chovaní jednotlivých bezpečnostných funkcií alebo mechanizmov;
- vplyv na väzbu prostredníctvom nastavenia externých signálov na mikročipe.

Niektoré hardvérové bezpečnostné mechanizmy sú účinné len v kombinácii s ďalšími softvérovými protiopatreniami v zloženom produkte. Preto je potrebná dodatočná analýza zraniteľnosti bezpečnostného mechanizmu zloženého produktu, ako je definované v prílohe 6, HODNOTENIE ZLOŽENÉHO PRODUKTU PRE SMART KARTY A PODOBNÉ ZARIADENIA. Tieto hardvérové bezpečnostné mechanizmy sa musia vyhodnotiť v takom rozsahu, aby bol hodnotiteľ zloženého produktu schopný posúdiť kombináciu hardvéru a softvéru. Súvisiaci opis musí byť zahrnutý v ETR pre zloženie. Hodnotiteľ zloženia môže použiť otvorené vzorky na nastavenie testovacieho pracoviska pre zložený produkt.

Penetračné testovanie

Penetračné testovanie pozostáva z analýzy TOE na základe potenciálnych zraniteľností a potenciálnych chýb, ktoré sú k dispozícii vo verejne dostupnej dokumentácii a dokumentácii špecifickej pre danú schému.

Potenciál útoku citácia

Jedným z kľúčových aspektov požiadaviek na analýzu zraniteľnosti je pojem odolnosti voči útokom, ktoré predstavujú útočníci s určitým potenciálom útoku (základný, zvýšený základný, stredný alebo vysoký potenciál útoku). Potenciál útoku, ktorý sa berie do úvahy pri hodnotení TOE, je vopred definovaný výberom určitého komponentu záruk AVA_VAN v ST.

Odolnosť voči útokom, ktorú má TOE zabezpečiť, závisí od:

- aktíva, ktoré sa majú chrániť, a predpokladané riziko ohrozenia týchto aktív;
- predpokladané operačné prostredie, ktoré určuje predpokladané útoky a faktory, ako sú napríklad okná príležitostí;
- vnímané požiadavky trhu s ohľadom na náklady na vývoj, výrobu a certifikáciu.

Napr. v modeloch identity účastníka (SIM) je uložený kľúč služby a účastníka, ktorý sa používa na získanie prístupu do mobilných telefónnych sietí. Hodnota tejto služby pre útočníka, ktorý klonuje kartu SIM s rizikom, že ho prevádzkovateľ siete odhalí a zablokuje, môže byť nízka. V tomto prípade môže byť vhodná základná odolnosť SIM karty proti klonovaniu. V iných prípadoch, ako je napríklad platená televízia, ktorá uchováva kryptografické kľúče používané mnohými účastníkmi v neusmernenej komunikácii, sa môže vyžadovať vysoká odolnosť proti útokom kompromitujúcim takýto kľúč.

Preto v prípade hodnotenia bezpečnostných integrovaných obvodov alebo smart kariet, ak je cieľové hodnotenie EAL nižšie ako EAL6, môže byť vhodné rozšíriť požiadavku bezpečnostných záruk o vyšší komponent AVA_VAN.

V prílohe 7, UPLATNENIE POTENCIÁLU ÚTOKU NA SMART KARTY A PODOBNÉ ZARIADENIA, sú uvedené povinné usmernenie pre hodnotenie potenciálu útoku potrebného na vykonanie konkrétnych útokov. Ide o výklad pre bezpečnostný IC založený na CEM, príloha B, zohľadňujúci špecifickú technológiu a prevádzkové prostredie, ako aj potrebu informácií o bezpečnosti počas fázy používania prevádzky, ako je samostatné hodnotenie identifikácie a prevádzky pre riadenie rizík. Rating poskytuje mieru najslabšej cesty potrebnej na zistenie tajomstiev IC alebo manipuláciu s IC. V praxi to bude pravdepodobne súčet rôznych pracovných funkcií (napr. odstránenie ochrannej bariéry, určenie usporiadania IC, dešifrovanie údajov alebo extrakcia obsahu EEPROM).

Na preukázanie hodnotenia možno použiť rôzne metódy:

- Vykonávanie penetračných testov až po konkrétny krok cesty útoku, ktorý dokazuje možnosť, ale vyžaduje značné dodatočné úsilie na zneužitie. Napríklad výkonové poruchy sa vykonávajú v takom rozsahu, aby sa výsledné poruchy dali reprodukovať a aby sa dal určiť účinok porúch, alebo

reverzné inžinierstvo sa vykonáva v takom rozsahu, aby sa dala overiť konkrétna časť obvodu bez použitia informácií o návrhu.

- Porovnanie výsledkov penetračných testov s testovacou konfiguráciou, ktorá nie je útočníkovi dostupná, s výsledkami penetračného testu s testovacou konfiguráciou, ktorá je útočníkovi dostupná. Napríklad analýza SPA/DPA sa vykonáva s vybranými hodnotami alebo špecifickými konfiguráciami a porovnáva sa s náhodnými hodnotami a hodnotenou konfiguráciou.
- Spustenie automatizovaných testov pre rovnaké časové obdobie, aké sa používa pri hodnotení. Pri takýchto testoch sa musí vopred overiť funkčnosť testovacieho nastavenia. Výsledky takýchto testov môžu byť čiastočne úspešné, nesmú však obsahovať žiadne výsledky, ktoré poukazujú na priamu zraniteľnosť. Napríklad každý polovodič je citlivý na svetelné útoky. Preto sa musí skenovať celý povrch zariadenia, aby sa skontrolovali chyby, ktoré môžu poskytnúť indície pre ďalšie úspešné útoky.

Podľa CEM sa pri výpočte potenciálu útoku už nerozlišuje medzi fázou identifikácie a fázou zneužitia, ale v rámci komunity pre smart karty a podobné zariadenia sa pri riadení rizík, ktoré vykonáva používateľ CC certifikátov, jednoznačne vyžaduje, aby sa rozlišovalo medzi nákladmi na "identifikáciu" (definícia útoku) a nákladmi na "zneužitie" (napr. po zverejnení skriptu na internete). Preto sa toto rozlíšenie zachováva v prílohe 7 pri výpočte potenciálu útoku na hodnotenie smart kariet a podobných zariadení. Hoci je pre tento typ hodnotenia produktov podstatné rozlíšenie medzi identifikáciou a zneužitím, aby bolo možné pochopiť a zdokumentovať cestu útoku, konečný súčet potenciálu útoku sa vypočíta sčítaním bodov oboch fáz, keďže obe fázy vytvárajú kompletný útok.

Pri použití hodnotiacich tabuliek z prílohy 7 alebo prílohy B CEM sa uvedie zdôvodnenie, prečo sú tvrdenia alebo predpoklady podporujúce analýzu platné (napr. prečo je pre útok použiteľná určitá úroveň odbornosti alebo určité vybavenie a nie menej).

30. PRÍLOHA 4: POŽIADAVKY NA BEZPEČNOSTNÚ ARCHITEKTÚRU (ADV_ARC) PRE SMART KARTY A PODOBNÉ ZARIADENIA

ÚČEL

Táto príloha obsahuje požiadavky na vývojára, ako uplatňovať požiadavky bezpečnostných záruk skupiny ADV_ARC na technickú doménu týkajúcu sa smart kariet a podobných zariadení. Vymedzuje, aký druh informácií musí obsahovať dokumentácia vývojára poskytovaná na splnenie požiadaviek skupiny ADV_ARC, ďalej len "dokumentácia ARC", a v akej miere podrobnosti sa tieto informácie musia poskytnúť.

Vzťahuje sa na vývojárov bezpečnostných integrovaných obvodov aj na vývojárov zložených produktov, ktoré pozostávajú z hardvérovej platformy a vstavaného softvéru (vlastný softvér, uzavreté operačné systémy s jednou alebo viacerými aplikáciami, otvorené softvérové platformy a iné).

Neurčuje povinné úlohy hodnotiteľa, ale môže slúžiť ako usmernenie pre jeho činnosť.

Môžu sa poskytnúť ďalšie usmernenia, ktoré na príkladoch ilustrujú typ informácií a úroveň podrobnosti, ktoré sa majú uviesť v dokumentácii ARC.

KONKRÉTNY STAV

Žiadne.

KRÍŽOVÝ ODKAZ NA KAPITOLU(-Y), V KTOREJ(-ÝCH) SÚ TIETO PRVKY VYHLÁSENÉ ZA UPLATNITEĽNÉ

Kapitola 8, ŠPECIFICKÉ KRITÉRIA A METÓDY HODNOTENIA.

1 ZÁKLADNÉ INFORMÁCIE

CC časť 3 zavádza bezpečnostnú architektúru skupiny ADV_ARC (Požiadavky bezpečnostných záruk - Security assurance requirements –SAR) takto:

"Cieľom tejto skupiny je, aby vývojár poskytol opis bezpečnostnej architektúry TSF. To umožní analýzu informácií, ktoré v spojení s ostatnými dôkazmi predloženými pre TSF potvrdia, že TSF dosahuje požadované vlastnosti. Popisy bezpečnostnej architektúry podporujú implicitné tvrdenie, že bezpečnostnú analýzu TOE možno dosiahnuť preskúmaním TSF; bez spoľahlivej architektúry by bolo potrebné preskúmať celú funkcionalitu TOE."

Bezpečnostná architektúra je súbor vlastností, ktoré TSF vykazuje; medzi tieto vlastnosti patrí vlastná ochrana, oddelenie domén a neobchádzateľnosť. Tieto vlastnosti sa líšia od bezpečnostných funkcionalít vyjadrených v CC časti 2 SFR, pretože zväčša nemajú priamo pozorovateľné rozhranie v TSF. Sú to skôr vlastnosti TSF, ktoré sa dosahujú prostredníctvom návrhu TOE a TSF a presadzujú sa správnou implementáciou tohto návrhu.

Bezpečnostná architektúra opisuje aj inicializáciu bezpečnostnej funkcionality TOE (TSF), t. j. spracovanie, ktoré sa uskutočňuje pri prechode zo stavu "down" do počiatočného bezpečného stavu, keď sa použije zapnutie alebo reset.

Technická doména týkajúca sa smart kariet a podobných zariadení predstavuje špecifiká, ktoré je potrebné zohľadniť pri vypracovaní dokumentácie ARC. Hlavnými charakteristikami sú:

- zariadenie patriace do tejto oblasti je kombináciou jednočipového integrovaného obvodu so zabudovaným softvérom implementujúcim kryptografické služby pomocou tajomstiev. TOE môže

pokrývať celý produkt alebo len vrstvu, ktorá zahŕňa integrovaný obvod (základnú platformu);
- TOE sa môže spustiť v režime s nízkou funkčnosťou a potom prejsť do vyhodnotenej bezpečnej konfigurácie. K prechodu z vypnutého stavu dochádza aj pri každom použití zariadenia konečným držiteľom;
- v jeho prevádzkovom prostredí môže mať útočník fyzický prístup k TOE cez fyzický port a povrchy IC;
- konkrétny životný cyklus.

2 VŠEOBECNÉ ASPEKTY OBSAHU A PREZENTÁCIE

Dokumentácia ARC podporuje analýzu zraniteľnosti hodnotiteľa, ale neposkytuje analýzu zraniteľnosti vývojára.

Dokumentácia ARC opisuje bezpečnostné domény a bezpečný proces inicializácie a preukazuje vlastnú ochranu a neobchádzateľnosť. Opis sa zameriava na použitie zavedených bezpečnostných mechanizmov a ich spoluprácu s cieľom dosiahnuť celkovú bezpečnosť. Na tento účel môže vývojár analyzovať a dospieť k záveru, ako sú bezpečnostné prvky a protiopatrenia TOE určené na odolávanie všeobecným útokom uvedeným v prílohe 7, Uplatnenie potenciálu útoku na smart karty z hľadiska manipulácie a obchádzania.

Poznámka: Na základe dokumentácie ARC hodnotiteľ vykoná nezávislú analýzu zraniteľnosti s cieľom určiť skutočnú odolnosť TOE voči útokom. Hodnotiteľ zohľadní všetky potenciálne zraniteľnosti, na ktoré narazil pri vykonávaní činností hodnotiteľa alebo ktoré našiel nezávislým metodickým vyhľadávaním. Hodnotiteľ určí, či sú zraniteľnosti zneužiteľné útočníkom, ktorý disponuje potenciálom útoku riešeným v ST. Dokumentácia ARC a analýza zraniteľností sa teda líšia zodpovednosťou, metódami a výsledkom.

Opis bezpečnostnej architektúry opisuje všetky vlastnosti TOE a TSF a všetky bezpečnostné mechanizmy TSF, ktoré prispievajú k presadzovaniu bezpečnostnej architektúry. Bezpečnostné mechanizmy špecifické pre presadzovanie vlastností bezpečnostnej architektúry môžu byť úplne opísané v dokumentácii ARC alebo v dokumentácii TDS, v takom prípade sa dokumentácia ARC na tieto opisy odvoláva.

Poznámka: niektoré bezpečnostné mechanizmy sú rozptýlené v celej implementácii a nie je možné ich vyjadriť alebo ich nie je možné jednoducho vyjadriť v rámci dokumentov TDS a mapovania na moduly. Opis bezpečnostnej architektúry by sa mal vyhnúť redundancii s inými časťami ADV.

CC vyžaduje, aby bol opis bezpečnostnej architektúry na úrovni podrobnosti zodpovedajúcej opisu abstrakcií presadzujúcich SFR opísaných v dokumente návrhu TOE. To však neznamená rovnakú prísnosť prezentácie v dokumentácii ARC; pre dokumentáciu ARC sa nevyžaduje použitie poloformálnych alebo formálnych metód. Aj keď CC vyžaduje, aby vývojár poskytol mapovanie medzi opisom návrhu TOE a vzorom zobrazenia implementácie, takéto mapovanie sa nevyžaduje pre opis bezpečnostnej architektúry.

V rámci technickej domény smart kariet a podobných zariadení sú fyzickými hranicami TOE TSFI. Povrch zariadenia je TSFI na fyzickú ochranu proti manipulácii. Povrch samotného integrovaného obvodu môže vysielať fyzické signály, ako napríklad elektromagnetické vyžarovanie, ktoré by sa mohlo použiť na analýzu bočných kanálov, alebo vstupnú energiu používanú na narušenie, napríklad laserové útoky. Porty sú fyzické vstupné alebo výstupné body napájania a fyzických signálov pre TOE, ktoré zabezpečujú prístup k TSF. Fyzický signál obsahuje viac informácií (napr. časovanie, úroveň signálu) ako údaje určené na výmenu prostredníctvom logicky definovanej TSFI. Napájací port nie je súčasťou logického rozhrania, ale môže ovplyvniť TSF (napr. poruchami).

Hodnotiteľovi pripomíname, že v centre pozornosti dokumentácie ARC je synergia, a nie rozlišovanie vlastnej ochrany, neobchádzateľnosti, oddelenia domén a bezpečnej inicializácie.

3 ÚROVEŇ POPISU V ADV_ARC

ADV_ARC.1.1C vyžaduje, aby bol opis architektúry "*na úrovni podrobnosti zodpovedajúcej opisu abstrakcií presadzujúcich SFR opísaných v dokumente návrhu TOE*".

Keďže očakávaná úroveň záruky je EAL4 rozšírená aspoň o AVA_VAN.5 alebo vyššia, úroveň opisu musí zodpovedať parametrom, činnostiam a chybovému hláseniu pre TSFI, úrovni rozhrania modulu a v niektorých prípadoch špecifickým implementačným detailom. Poloformálny alebo formálny opis sa

však nevyžaduje, pretože neprináša komplexnejšie podrobnosti.

Opis bezpečnostnej architektúry musí byť založený na bezpečnostných mechanizmoch (entity presadzujúce SFR, mechanizmy presadzujúce vlastnosti, návrh protiopatrení, konvencie kódovania). Každý bezpečnostný mechanizmus sa vysvetlí z hľadiska účelu a správania s výnimkou entít presadzujúcich SFR, ktoré sú opísané v rozkladovej dokumentácii.

V prípade bezpečnostných mechanizmov, ktoré sa rozprestierajú v celej implementácii, sa zabezpečí, aby medzi opisom v ADV_ARC a ADV_IMP nebolo veľa nejasností, a to uvedením zásad, ktoré viedli k ich implementácii do kódu. Opis bezpečnostných mechanizmov sa môže ilustrovať ukážkou kódu alebo príkladom.

4 BEZPEČNOSTNÉ DOMÉNY

Opis bezpečnostnej architektúry opisuje bezpečnostné domény, ktoré TSF udržiava v súlade s SFR (porovnaj ADV_ARC.1.2C).

Oddelenie domén je vlastnosť, ktorou TSF vytvára samostatné bezpečnostné domény pre seba a pre každú nedôveryhodnú aktívnu entitu, ktorá má pracovať s jeho prostriedkami, a potom tieto domény od seba oddeľuje tak, aby žiadna entita nemohla pracovať v doméne inej entity.

V opise bezpečnostnej architektúry sa vysvetlia rôzne druhy domén, ktoré vytvára TSF, ako sú definované z hľadiska zdrojov pridelených každej doméne a ako sú domény oddelené, aby aktívne entity v jednej doméne nemohli manipulovať so zdrojmi v inej doméne.

Ak je TSF jedinou aktívnou entitou a na správu interakcií s používateľmi sú k dispozícii iba dátové štruktúry, ktoré TSF udržiava, bezpečnostná architektúra bude opisovať, že pre aktívne entity nie je k dispozícii žiadna bezpečnostná doména.

Ak TSF poskytuje bezpečnostné domény pre iné aktívne subjekty, musí tieto domény chrániť pred nepriaznivým pôsobením týchto potenciálne škodlivých subjektov na zdroje TSF. Okrem toho bude TSF udržiavať túto doménu oddelenú od bezpečnostnej domény iných aktívnych subjektov.

Ak dokumentácia ARC opisuje bezpečnostné domény, prideľovanie a rozdeľovanie zdrojov pre aktívne subjekty by malo byť pod kontrolou SFR (napr. FDP_ACC: riadenie prístupu). Používanie zdrojov aktívnym subjektom v bezpečnostnej doméne je mimo kontroly TSF. Aktívne subjekty môžu používať tieto zdroje podľa svojich vlastných bezpečnostných politík, ale nesmú používať iné zdroje mimo svojej bezpečnostnej domény. Preto opis domény uvedený v dokumentácii ARC musí spĺňať kontrolu prístupu TSF k zdrojom bezpečnostnej domény vyjadrenú v SFR a ostatné SFR nesmú byť v rozpore s definíciou bezpečnostnej domény. Ak dokumentácia ARC opisuje bezpečnostné domény v zmysle zdrojov, ktoré nie sú kontrolované SFR, znamenalo by to, že SFR chýba.

V prípade zloženého hodnotenia by sa aplikačná vrstva mohla spoliehať na základnú platformu, aby správne inštanciovala domény, ktoré TOE definuje. Vývojár by mal uviesť zoznam použitých bezpečnostných služieb, ktoré ponúka platforma na podporu oddelenia bezpečnostných domén, a uviesť odkaz na tieto služby v opise.

5 BEZPEČNÉ SPUSTENIE

Opis bezpečnostnej architektúry musí opisovať, ako je proces inicializácie TSF bezpečný (v súlade s ADV_ARC.1.3C). Informácie uvedené v opise bezpečnostnej architektúry týkajúce sa inicializácie TSF sa zameriavajú na proces uvedenia TSF zo stavu "down" (napr. vypnutie alebo po resete) do počiatočného bezpečného stavu (t. j. keď sú všetky časti TSF funkčné, pozri odsek 530 CEM). Pre smart karty a podobné zariadenia:

- časti TSF môžu byť aktívne aj pri vypnutom napájaní, napr. fyzická ochrana proti neodhalenej manipulácii;
- časti TSF môžu byť dočasne deaktivované, napr. v režimoch úspory energie.

Cieľom procesu bezpečnej inicializácie smart kariet a podobných zariadení je presadiť bezpečnostné ciele aj v čase, keď niektoré časti TSF nie sú aktívne (t. j. počas vypnutia alebo úsporného režimu) alebo v procese aktivácie (napr. spustenie) alebo v procese deaktivácie (napr. prechod do úsporného režimu). Bezpečný proces inicializácie si vyžaduje, aby bola počas týchto prechodov zabezpečená vlastná ochrana a neobchádzateľnosť. To znamená, že v ktoromkoľvek okamihu nie je funkcia TOE dostupná, ak nie sú aktivované časti TSF chrániace túto funkciu.

Bezpečný proces inicializácie sa bude realizovať prostredníctvom špecifických bezpečnostných prvkov alebo bezpečnostných funkcií, ktoré nebudú priamo nadväzovať na SFR. Tieto špecifické bezpečnostné funkcie a ich bezpečnostné mechanizmy nemusia byť opísané v iných skupinách záruk ADV. Cieľom dokumentácie ARC pre bezpečnú inicializáciu je poskytnúť všetky informácie potrebné na to, aby sa tieto komponenty považovali za súčasť TSF.

Bezpečný proces inicializácie môže implementovať mechanizmy chrániace dôvernosť alebo kontrolujúce integritu implementácie iných TSF. Niektoré mechanizmy nemusia byť po bezpečnej inicializácii potrebné a musia byť chránené proti zneužitiu.

Ak sú externé rozhrania inicializačného procesu úplne opísané ako TSFI z hľadiska činností v ADV_FSP.4 a ďalších alebo mechanizmy ako súčasť TSF sú opísané z hľadiska účelu a interakcií modulov v ADV_TDS.3 a ďalších, nemusia sa opisovať znova.

6 SEBAOBRANA

V komponente ADV_ARC.1.4C sa vyžaduje, aby opis bezpečnostnej architektúry preukazoval, že TSF sa chráni pred neoprávnenou manipuláciou.

Vlastná ochrana sa vzťahuje na schopnosť TSF chrániť sa pred manipuláciou zo strany externých subjektov, ktorá môže viesť k zmenám TSF, takže už nebude spĺňať bezpečnostné ciele alebo SFR.

Zásah do TSF môže byť realizovaný nedôveryhodným aktívnym subjektom, ktorý beží v mene externého subjektu. Identifikovali a opísali by sa mechanizmy, ktoré zabezpečujú oddelenie domén na definovanie domény TSF, ktorá je chránená pred inými (používateľskými) doménami.

V rámci technickej domény smart kariet a podobných zariadení sú fyzickými hranicami TOE, z ktorých môže externý subjekt zasahovať, porty a povrch integrovaného obvodu. Porty sú fyzické vstupy TOE podporujúce logické rozhranie, ktoré poskytujú prístup k TSF pre fyzické parazitné signály. Povrch čipu môže byť tiež vstupným bodom pre fyzické parazitné signály. Tieto signály môžu vyvolať modifikáciu uloženého kódu a údajov alebo správneho vykonávania kódu.

Trieda funkčných požiadaviek FPT (Ochrana TSF) obsahuje skupiny požiadaviek funkcionalít, ktoré sa týkajú integrity a riadenia mechanizmov, ktoré tvoria TSF, a integrity údajov TSF.

Komponenty z triedy FPT sú potrebné na zabezpečenie požiadaviek, aby sa so SFP v TOE nedalo manipulovať.

Vlastná ochrana sa preto vo všeobecnosti nedá dosiahnuť len implementáciou SFR, ale je možné pridať ďalšie bezpečnostné mechanizmy a spolupracovať s bezpečnostnými mechanizmami implementujúcimi SFR.

Vlastná ochrana TSF sa dosiahne prostredníctvom:

- bezpečnostné mechanizmy: schopnosť každého bezpečnostného mechanizmu prispieť k ochrane proti priamym útokom;
- väzba bezpečnostných mechanizmov: schopnosť bezpečnostných mechanizmov spolupracovať spôsobom, ktorý sa navzájom podporuje a vytvára integrovaný a účinný celok;
- kombinácia hardvérových a softvérových bezpečnostných mechanizmov

Inicializačný proces zaručuje, že TSF je v počiatočnom bezpečnom stave a nebol žiadnym spôsobom podvrhnutý. Vývojár vysvetlí, ako inicializačný proces kontroluje integritu kódu TSF. Počas tohto procesu sa kontroluje aj integrita kódu inicializačného procesu.

V niektorých prípadoch sa TOE spúšťa v režime s nízkou funkčnosťou, v ktorom sa nedôveryhodní používatelia môžu prihlásiť a používať služby a prostriedky TOE. V tomto režime sa kód nespúšťa v hodnotenej konfigurácii a tieto služby už nie sú prístupné.

V tomto prípade musí opis bezpečnostnej architektúry obsahovať vysvetlenie, ako je TSF chránený proti tomuto kódu v hodnotenej konfigurácii:

- čo bráni spusteniu tohto kódu;
- čo bráni prístupu k týmto službám.

V prípade zloženého hodnotenia by platforma mohla poskytovať bezpečnostné služby, ktoré prispievajú k vlastnej ochrane v spolupráci s bezpečnostnými mechanizmami aplikačnej vrstvy. Vývojár uvedie zoznam použitých bezpečnostných služieb, ktoré platforma ponúka, a uvedie na ne

odkaz
v nasledujúcej analýze.

Vývojár opíše bezpečnostné mechanizmy a ich spoluprácu na ochranu TSF pred neoprávnenou manipuláciou. Vývojár poskytne opis toho, ako TOE reaguje v prítomnosti príslušných útokov uvedených v prílohe 7, Uplatnenie potenciálu útokov na smart karty, a poskytne záver.

7 NEPRECHODNOSŤ

V komponente ADV_ARC.1.5C sa vyžaduje, aby opis bezpečnostnej architektúry preukazoval, že TSF zabraňuje obchádzaniu funkcií vynucovania SFR

Neobchádzateľnosť je vlastnosť, že bezpečnostná funkcionalita špecifikovaná v SFR je vždy vyvolaná a nemôže byť obídená, ak je to vhodné pre daný mechanizmus (pozri prílohu A časti 3 CC).

8 VŽDY VYVOLANÝ TSF

Neobchádzateľnosť znamená predovšetkým to, že neexistuje možnosť obísť subjekt presadzujúci SFR použitím neočakávaných a nezdokumentovaných ciest v návrhu. Akákoľvek možnosť obísť SFR sa preto pripisuje chybe v návrhu alebo implementácii.

Z úrovne EAL4 musí funkčná špecifikácia opisovať všetky činnosti spojené s každou TSFI (ADV_FSP.4.4C) a návrh musí opisovať každý modul podporujúci SFR alebo modul nezasahujúci do SFR z hľadiska jeho účelu a interakcie s ostatnými modulmi (ADV_TDS.3.9C). V tomto prípade sú všetky režimy alebo operácie TSFI zdokumentované na dostatočnej úrovni, aby poskytli dôkaz
o neobchádzateľnosti využitím chyby v návrhu.

Po druhé, neobchádzateľnosť vyžaduje, aby sa žiadne funkčné rozhranie nemohlo použiť na porušenie bezpečnostných cieľov TOE, na obchádzanie SFR alebo na konflikt s SFR. Ak existujú funkčné rozhrania, vývojár ich uvedie a vysvetlí, prečo nemajú žiadnu interakciu s TSF alebo prečo neposkytujú cestu na obídenie TSF. V tomto prípade môže opis oddelenia domény (pozri príslušnú kapitolu) priniesť dôkaz o neobchádzateľnosti.

Po tretie, neobchádzateľnosť sa týka prípadov, keď má útočník iba logický prístup k TOE, na rozdiel od prípadu "manipulácie", ktorému sa má čeliť vlastnou ochranou (pozri príslušnú časť).

Vývojár opíše bezpečnostné mechanizmy a ich spoluprácu na ochranu TSF pred softvérovými útokmi využívajúcimi nedostatočný návrh alebo implementáciu na splnenie bezpečnostných cieľov TOE. Vývojár poskytne opis toho, ako TOE reaguje v prítomnosti príslušných útokov uvedených v prílohe 7, Uplatnenie potenciálu útoku na smart karty, a uvedie záver.

9 BOČNÝ KANÁL

Vedľajšie kanály sú nevynútené signalizačné kanály prenášajúce informácie o vnútorných tajomstvách, stavoch alebo procesoch, ktoré sa poskytujú monitorovaním spracovania akéhokoľvek objektu obsahujúceho tieto informácie alebo s nimi súvisiaceho (porovnaj odsek 1909 CEM). Informácie môžu byť obsiahnuté v akejkoľvek pozorovateľnej fyzikálnej hodnote ako spotreba energie zariadenia, napätie a časovanie na portoch výstupných rozhraní, elektromagnetické vyžarovanie na povrchu IC. Signály výstupných portov môžu obsahovať viac informácií ako údaje určené na výmenu prostredníctvom logického rozhrania definovaného v dokumentácii TSF. Napájacie rozhranie a elektromagnetické vyžarovanie cez povrch IC nie sú vôbec určené na výstup informácií, ale môžu niesť informácie.

Vedľajšie kanály obchádzajú TSF, pretože z nich unikajú všetky informácie, ktoré majú byť utajené. Medzi tajné informácie patria okrem iného autentizačné referenčné údaje (napr. na overenie kódu PIN), symetrické tajné alebo asymetrické súkromné kryptografické kľúče, načasovanie spracovania údajov umožňujúce ďalšie útoky.

Vývojár opíše protiopatrenia zavedené s cieľom zabrániť potenciálnym bočným kanálom TOE
v plánovanom prevádzkovom prostredí. Analýza bočných kanálov ako súčasť analýzy zraniteľnosti hodnotiteľa určí, či bočné kanály existujú a sú zneužiteľné, t. j. či sú tieto protiopatrenia účinné.

Vývojár a hodnotiteľ by mali konzultovať SFR a bezpečnostné ciele, ktoré presadzujú, aby určili, či neúmyselný tok informácií obchádza alebo neobchádza TSF. Implementácia výpočtu symetrického autentizačného kódu správy zachová dôvernosť kľúča, ale môže, ale nemusí byť potrebná na ochranu dôvernosti spracovaných údajov používateľa. Preto rozhodnutie o obídení TSF únikom informácií

o spracovaných údajoch používateľa závisí od bezpečnostného cieľa presadzovaného SFR.

31. PRÍLOHA 5: CERTIFIKÁCIA "OTVORENÝCH" SMART KARIET

ÚČEL

Cieľom tejto prílohy je určiť postup certifikácie "otvorených" produktov smart kariet, aby sa zaručilo, že ich zmenená architektúra neovplyvní efektívnosť certifikovanej bezpečnostnej funkcionality certifikátu, ktorý už bol vydaný pre inú architektúru tohto produktu.

KONKRÉTNY STAV

Žiadne.

KRÍŽOVÝ ODKAZ NA KAPITOLU(-Y), V KTOREJ(-ÝCH) SÚ TIETO PRVKY VYHLÁSENÉ ZA UPLATNITEĽNÉ

Kapitola 8, ŠPECIFICKÉ HODNOTIACE KRITÉRIA A METÓDY.

1 KONTEXT A ÚČEL DOKUMENTU

1.1 Definície

Pojem produkt sa tu vzťahuje na všeobecný pojem, ktorý zodpovedá TOE spojenej s prostredím.

Pojem "platforma" sa vzťahuje na terminológiu použitú v prílohe 6, HODNOTENIE ZLOŽENÉHO PRODUKTU PRE SMART KARTY A PODOBNÉ ZARIADENIA o zložení procesu hodnotenia výsledkov, ktorá sa uplatňuje na prípad hodnotenia zloženia "aplikácie na platforme". Produkt, ktorý sa tu označuje ako "platforma", je teda integrovaný obvod so softvérovým operačným systémom a niekedy s vlastným aplikačným kódom.

"Otvorená platforma" je platforma, ktorá môže hostiť novú aplikáciu po jej dodaní koncovému používateľovi (t. j. počas 7. fázy tradičného životného cyklu smart karty). Takéto načítanie sa nazýva "post-issuance" (načítanie aplikácií po dodaní smart karty koncovému používateľovi).

Aplikácie sa môžu inštalovať pred siedmou fázou, ktorá zodpovedá "predvýdajovému" nakladaniu.

"Uzavretá platforma" je platforma, ktorá nemôže hostiť novú aplikáciu po jej dodaní koncovému používateľovi.

"Izolovaná platforma" je platforma, ktorá zabezpečuje oddelenie prevádzkovaných domén všetkých vstavaných aplikácií na platforme, ako aj samotnej platformy.

"Izolácia" sa tu vzťahuje na oddelenie domén aplikácií, ako aj na ochranu údajov aplikácie.

"Architektúra" zodpovedá štruktúre produktu na najvyššej úrovni, konkrétne "otvorenej platforme" so všetkými aplikáciami obsiahnutými v produkte (kedykoľvek sú načítané pred alebo po vydaní).

Keďže načítanie nových aplikácií by sa mohlo zvážiť pred procesom hodnotenia alebo po ňom, na odlíšenie aplikácií, ktoré boli zohľadnené počas procesu hodnotenia, od ostatných sa používajú pojmy "známe aplikácie" a "neznáme aplikácie".

"Známe aplikácie" zodpovedajú pôvodnej architektúre certifikovaného produktu. ITSEF ich všetky zohľadňuje počas procesu hodnotenia.

"Neznáme žiadosti" sú žiadosti, ktoré v čase hodnotenia neboli známe. Zodpovedajú aktualizácii architektúry hodnoteného produktu oproti architektúre uvedenej v správe o certifikácii.

1.2 Rozsah pôsobnosti

Cieľom tejto prílohy je určiť postup certifikácie otvorených produktov, aby sa zaručilo, že ich

zmenená architektúra neovplyvní efektívnosť certifikovanej bezpečnostnej funkcionality certifikátu, ktorý už bol vydaný pre odlišnú architektúru tohto produktu. Zmenená architektúra tu znamená pridanie aplikácií do pôvodnej certifikovanej architektúry produktu (úprava prostredia TOE).

Všimnite si, že (na rozdiel od vyššie uvedenej situácie) zmena samotnej platformy si bude vyžadovať opätovnú certifikáciu/ kontinuity záruky platformy a následne celého produktu.

Aby sa v certifikáte zohľadnila zmenená architektúra týchto produktov, musí mať platforma určité vlastnosti, najmä vlastnosti izolácie pre aplikácie aktivované na produkte. Iba produkty, ktoré ponúkajú tieto izolačné vlastnosti, totiž zabezpečujú, že aktivácia novej aplikácie neovplyvní bezpečnostnú záruku funkčnosti podľa certifikátu. Platformy, ktoré boli vyhodnotené s cieľom preukázať, že ponúkajú (za určitých obmedzení) tieto garancie, sa v tomto dokumente nazývajú "otvorená a izolujúca platforma".

Keď sa na takýto otvorený produkt nahrajú nové aplikácie, vyžaduje sa overenie splnenia bezpečnostných obmedzení platformy týmito novými aplikáciami, aby sa zabezpečilo, že hodnotený produkt (TOE) dosiahne úroveň AVA_VAN, ktorá je zameraná na jeho očakávané rozšírené IT prostredie.

Otvorené platformy, ktoré nezaručujú izoláciu aplikácií, sú certifikované ako uzavreté platformy. Uzavreté platformy, ktoré nepovoľujú načítanie po vydaní, sú mimo rozsahu pôsobnosti tohto dokumentu.

1.3 Plán poznámky

Kapitola 2 definuje záruky a obmedzenia platforiem a poskytuje vstupné údaje pre hodnotenie a certifikáciu "otvorených a izolujúcich platforiem".

Kapitola 3 definuje záruky a obmedzenia pre aplikácie a poskytuje vstupné údaje pre hodnotenie aplikácií na certifikovaných "otvorených a izolovaných platformách".

2 OTVORENÁ A IZOLOVANÁ PLATFORMA

2.1 Hodnotenie

V tomto dokumente sa hovorí o otvorenej a izolovanej platforme pre platformu, ktorá bola hodnotená v súlade s prvkami uvedenými v tomto dokumente.

2.1.1 Ciele

2.1.1.1 Analyzovaná funkčnosť

"Otvorená a izolovaná platforma" poskytuje tieto funkcie, ktoré sa hodnotia:

- O1: izolácia medzi všetkými aplikáciami uloženými na danej platforme, a teda ochrana pred aplikáciami, ktoré by mohli byť nepriateľské;
- O2: ochrana načítania aplikácií po ich vydaní na príslušnú platformu prostredníctvom overenia integrity a autentickosti overenia každej aplikácie pred ich aktiváciou vďaka dôkazom definovaným v nasledujúcom OE2.

O1 a O2 sú ciele TOE v bezpečnostnom zámere platformy.

2.1.1.2 Hodnotiace prostredie

"Otvorená a izolovaná platforma" je platforma, ktorá bola podrobená hodnotiacemu procesu, v rámci ktorého sú pre všetky aplikácie, ktoré sa na ňu vkladajú, povinné tieto požiadavky:

- OE1: všetky aplikácie, ktoré sa načítajú na platformu, sa musia pred ich skutočnou inštaláciou (aktiváciou) overiť podľa obmedzení stanovených cieľovou platformou, ktoré sa týkajú jej izolačných vlastností;

- OE2: dostupnosť dôkazu o integrite pre každú aplikáciu, ktorá sa má načítať na platformu (s cieľom zabezpečiť, že načítaná aplikácia nebola zmenená od overenia OE1), a tiež dostupnosť dôkazu o autentickosti týchto overení.

OE1 a OE2 musia byť cieľmi pre prostredie v bezpečnostnom zámere platformy.

OE1 a OE2 sa vzťahujú na všetky aplikácie, či už budú alebo nebudú hodnotené ako certifikované. Ako také sú uplatniteľné na všetky známe alebo neznáme aplikácie.

V prípade známej žiadosti sa splnenie OE1 a OE2 overí prostredníctvom ITSEF. Napriek tomu je stále možné overiť len OE1 a opísať spôsob, akým sa má splniť OE2. Potom ITSEF overí splnenie OE1
a posúdi riadiacu dokumentáciu použitú na splnenie OE2. V takom prípade sa v certifikáte jednoznačne identifikujú tieto aplikácie a uviesť obmedzenie používania, pričom sa od konečného používateľa vyžaduje, aby na splnenie OE2 použil sprievodnú dokumentáciu.

V prípade neznámej aplikácie nie je možné overiť splnenie OE1 a OE2. Certifikát platformy bude pozostávať z obmedzenia používania certifikátu, ktoré vyžaduje, aby konečný používateľ použil sprievodnú dokumentáciu na splnenie OE1 a OE2.

2.1.2 Identifikácia

Všeobecne povedané, certifikácia otvorenej platformy by mala umožniť identifikáciu produktu hodnoteného ITSEF. Táto identifikácia pozostáva z:

- identifikácia produktu v stave, v akom bol predložený na hodnotenie (poskytnutá ITSEF). Zahŕňa všetky známe žiadosti načítané pred vydaním;
- identifikáciu všetkých známych aplikácií, ktoré možno načítať po vydaní.

Identifikátory vrátené na žiadosť produktu musia umožniť rozlíšiť TOE od produktu identifikáciou platformy a zoznamom všetkých uložených aplikácií.

Hodnotenie sa vzťahuje na celý produkt bez ohľadu na to, o aký TOE ide. Preto sa v identifikačných informáciách poskytnutých bezpečnostným zámerom identifikujú komponenty platformy a známe aplikácie. Tieto identifikačné informácie sa jednoznačne uvedú v správe o certifikácii platformy.

Vývojár poskytne ITSEF prostriedky na overenie, či identifikátory produktu, ktoré má ITSEF
k dispozícii, zodpovedajú súboru komponentov, ktoré ITSEF pozná (bez ohľadu na to, či tieto komponenty patria alebo nepatria do TOE).

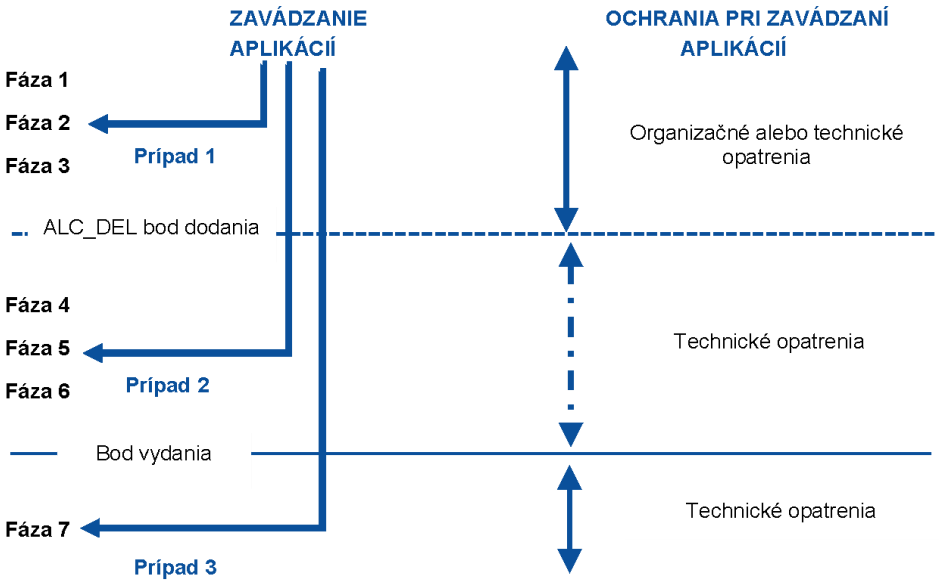
Tieto požiadavky umožňujú vyhnúť sa riziku certifikácie produktov vrátane aplikácií, ktoré nerešpektujú obmedzenia platformy, t. j. ktoré môžu byť nepriateľské pre ostatné aplikácie aktivované na produkte.

2.1.3 Životný cyklus

Nasledujúci obrázok znázorňuje fázový model životného cyklu otvorenej platformy. Je to len príklad takéhoto životného cyklu: bod dodania ALC súvisiaci s hodnotením platformy sa môže líšiť od tu identifikovaného bodu.

Upozorňujeme tiež, že posudzované miesto dodania sa môže rozšíriť oproti miestu posudzovanému v aktuálnom hodnotení, ak sa poskytnú dôkazy o certifikácii miest alebo porovnateľné výsledky auditu.

Obrázok 1: Životný cyklus otvorenej a izolovanej platformy[38]



Produkt "otvorenej a izolačnej platformy" môže obsahovať aplikácie pred vydaním a po vydaní.

Je užitočné spresniť, že opatrenia na dosiahnutie cieľa OE2 by mohli mať rôzny charakter v závislosti od momentu zaťaženia.

Môžu nastať tri rôzne prípady:

- Prípad 1: žiadosť sa načíta v predvýdajovom a preddodávkovom mieste; cieľ OE2 sa môže presadzovať organizačnými opatreniami alebo technickými opatreniami;
- Prípad 2: žiadosť je načítaná pred vydaním a po mieste dodania, organizačné opatrenia nie sú povolené a musia sa použiť technické opatrenia;
- Prípad 3: aplikácia sa načíta po vydaní (po vydaní produktu); musia sa použiť technické opatrenia súvisiace s cieľom OE2.

Podľa definície všetky uvažované platformy umožňujú zaťaženie v prípade 3 (aspoň vo fáze 7).

Na spresnenie spôsobu, akým sa realizujú OE1 a OE2, sa v bezpečnostnom zámere vysvetlia procesy, ktoré sú súčasťou vývoja, overovania a distribúcie aplikácie, a rôzne úlohy. V bezpečnostnom cieli sa opíše aj rozsah hodnotenia, pokiaľ ide o tento podrobný životný cyklus.

V prípade, že súčasťou hodnoteného produktu sú známe aplikácie, v bezpečnostnom zámere sa opíšu aj tieto podrobnosti životného cyklu:

- Identifikácia aktérov vo vzťahu k ich úlohe pri riadení procesov, ktoré sú súčasťou overovania žiadosti;
- Identifikácia účastníkov v súvislosti s ich úlohou pri riadení procesu, ktorý zahŕňa ochranu integrity a autentickosti žiadostí od ich overenia až po ich načítanie.

Okrem toho môže byť bod dodania ALC odlišný medzi certifikovanou platformou a následnou zloženou certifikáciou aplikácií nad certifikovanou platformou (pozri časť 3). Typickým prípadom použitia môže byť, že bod dodania ALC sa presunie do neskoršej fázy. Zložená certifikácia by tak zmenila klasifikáciu fáz s ohľadom na to, či patria do prípadu 1 alebo prípadu 2. Fázy certifikácie platforiem v prípade 2 by sa mohli stať fázami prípadu 1 zloženej certifikácie, keďže bod dodania je posunutý, a potom by neboli povinné technické opatrenia. Takéto preklasifikovanie sa akceptuje a nie je v rozpore s certifikáciou platformy ani na ňu nemá vplyv.

2.1.4 Usmernenie k produktu

[38] Upozorňujeme, že fázy 1 až 7 sa používajú tak, ako sú definované v ochrannom profile certifikovanom podľa [BSI-CC-PP-0084-2014]: Ochranný profil platformy bezpečnostného integrovaného obvodu s rozširujúcimi balíkmi, https://www.commoncriteriaportal.org/files/ppfiles/pp0084b_pdf.pdf

V súvislosti s hodnotiacim prostredím uvedeným v kapitole 2.1.1.2 poskytne navrhovateľ tieto konkrétne pokyny:

- Pokyny na vývoj aplikácie (v súvislosti s OE1), z ktorých sú odvodené pokyny na overovanie, ktoré opisujú obmedzenia kladené na aplikáciu s cieľom zachovať vlastnosť izolácie platformy [ISO_VERIF];
- Pokyny na ochranu pri zaťažení aplikácie (v súvislosti s OE2), ktoré zodpovedajú:
  - Organizačným opatreniam pre načítanie aplikácie [ORG_LOAD] ;
  - Technickým opatreniam na načítanie aplikácie, ktoré opisujú spôsob aktivácie súvisiacej funkcie (zodpovedajúcej O2) platformy, spojené s opatreniami potrebnými na zaručenie autentickosti overení (napríklad ochrana kľúčov) [TECH_LOAD].

Keďže "otvorené a izolované platformy" vždy umožňujú prípad 3 načítania aplikácie, [ISO_VERIF] a [TECH_LOAD] musí vždy poskytnúť vývojár.

Ak vývojár neimplementuje prípad 1 s organizačnými opatreniami, nebude potrebné poskytnúť [ORG_LOAD].

Všimnite si, že [ISO_VERIF] nezodpovedá usmerneniu, ktoré je predpísané v AGD_OPE (sprievodná dokumentácia pre kódovanie bezpečných aplikácií). V [ISO_VERIF] sú uvedené všetky pravidlá vývoja týkajúce sa zachovania izolačných vlastností platformy medzi aplikáciami. Časť usmernenia AGD_OPE venovaná vývoju aplikácií uvádza všetky pravidlá vývoja súvisiace s aplikáciami, ktoré musia poskytovať špecifické bezpečnostné vlastnosti.

Toto usmernenie sa bude musieť vyhodnotiť podľa AGD alebo ALC v závislosti od prípadov zaťaženia, ktoré zvažuje vývojár.

2.1.5 Hodnotená konfigurácia

V závislosti od skutočného životného cyklu posudzovaného produktu sa OE1 a OE2 musia v rámci ITSEF spracovať týmto spôsobom:

1) ITSEF bude musieť systematicky kontrolovať, či všetky známe aplikácie spĺňajú obmedzenie OE1. ITSEF sa môže spoliehať na dôkazy od vývojárov, aby skontroloval, či bolo vykonané overenie aplikácie. Keďže sa to nedá skontrolovať v prípade neznámych aplikácií, súlad s [ISO_VERIF] povedie k obmedzeniam certifikátu.
2) Ak sa organizačné opatrenia používajú pred miestom dodania, za načítanie aplikácie zodpovedá vývojár, súvisiaca ochrana, ktorá implementuje OE2, je pokrytá požiadavkou bezpečnostných záruk ALC. Preto sa organizačné opatrenia musia kontrolovať.
3) V rámci tohto dokumentu sa vždy používajú technické opatrenia presadzujúce OE2, prinajmenšom pre prípad 3. Súvisiace požiadavky sú uvedené v [TECH_LOAD]. Časť alebo všetky tieto požiadavky sa môžu presadzovať prostredníctvom požiadaviek bezpečnostných záruk ALC, preto sa musia kontrolovať zodpovedajúce organizačné opatrenia. Súlad s [TECH_LOAD], ktorý sa nedá skontrolovať, bude spočívať v obmedzení certifikátu.

OE1 a OE2 sa teda musia overiť pre všetky známe aplikácie.

2.2 Otvorená a izolovaná certifikácia platforiem

- Správa o certifikácii pre otvorenú a izolovanú platformu má tieto špecifiká:
- Presne sa určí, že izolácia aplikácií a tiež ochrana načítania aplikácií po vydaní boli preskúmané s cieľom určiť, či táto platforma zodpovedá koncepcii "otvorenej a izolujúcej platformy". Kapitola "Hodnotená konfigurácia" spresní, že hodnotený produkt je "otvorená a izolovaná platforma".
- V kapitolách "architektúra" a "hodnotená konfigurácia" sa uvedú všetky známe aplikácie, ktoré ITSEF skontroloval počas procesu hodnotenia. Zároveň spresní, že všetky identifikované aplikácie v správe o certifikácii boli skontrolované podľa cieľov OE1 a OE2.
- V kapitolách o "hodnotenej konfigurácii" sa tiež spresní, že certifikované sú aj produkty tvorené podmnožinou známych aplikácií.
- V kapitole "Obmedzenia používania" sa uvedú obmedzenia OE1 a OE2 a odkazy na usmernenia [ISO_VERIF], [ORG_LOAD] a [TECH_LOAD], ktoré sa vzťahujú na akúkoľvek aplikáciu nahranú do produktu, najmä na akúkoľvek novú aplikáciu, ktorá nie je známa v čase hodnotenia.

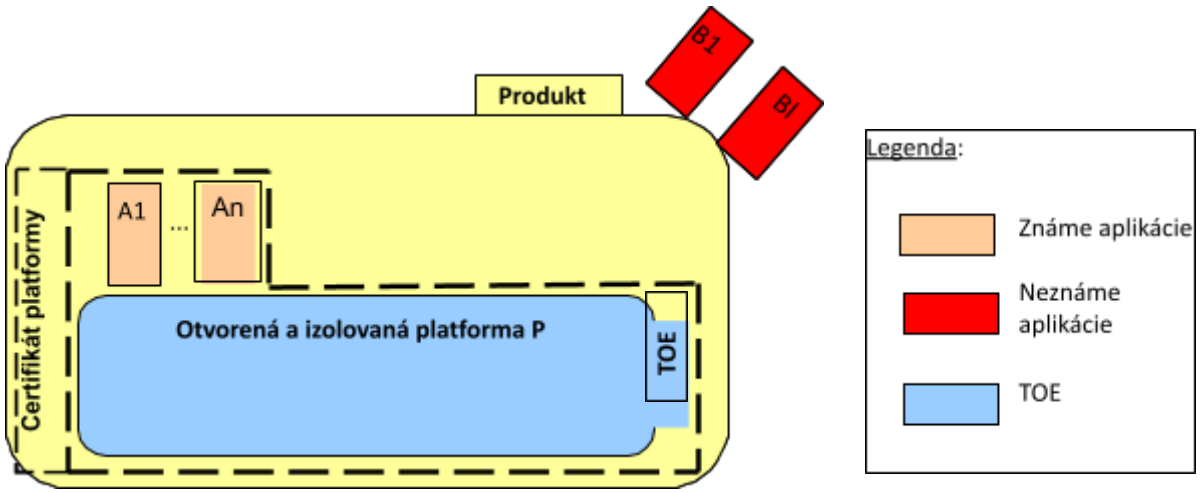
Upozorňujeme, že táto kapitola môže obsahovať aj obmedzenia používania, ktoré nesúvisia s otvorenými
a izolačnými vlastnosťami platformy.

- V kapitole "životný cyklus produktu" sa opíšu rôzne typy zaťaženia aplikácie, ktoré sa vzťahujú na produkt a ktoré vývojár zvažuje.
- Môže obsahovať aj zoznam známych aplikácií, pre ktoré bolo overené len OE1. V takýchto prípadoch sa v certifikáte jednoznačne identifikujú tieto aplikácie a uvedie sa obmedzenie používania, pričom sa vyžaduje, aby konečný používateľ použil sprievodnú dokumentáciu na splnenie OE2.

Načítanie neznámych aplikácií ako Bi (i ∈ [1,l]) znamená, že produkt už plne nevyhovuje architektúre produktu uvedenej v certifikáte otvorenej a izolovanej platformy. Výsledky hodnotenia sú platné len vtedy, ak všetky ostatné aplikácie načítané na platforme rešpektujú obmedzenia certifikátu platformy. Výslednú architektúru produktu, ktorá rešpektuje bezpečnostné obmedzenia súvisiacich certifikátov, možno teda považovať za certifikovanú. Je na manažérovi rizík, či sa spoľahne na bezpečnostnú záruku overenia OE1 a OE2, ktoré poskytuje subjekt zodpovedný za nasadenie týchto aplikácií, alebo sa spoľahne na schému. V tomto poslednom prípade (ak sa zvolí riešenie schémy CC) sa bude musieť vykonať údržba, ako je uvedené ďalej v kapitole 2.3.

Na nasledujúcom obrázku je zobrazený certifikovaný produkt. Tu TOE zodpovedá iba platforme. Aplikácie Ai (i ∈ [1,n]) zodpovedajú známym aplikáciám pred vydaním a sú potom identifikované
v správe o certifikácii platformy.

Obrázok 2: *Produkt súvisiaci s otvorenou a izolovanou platformou TOE*



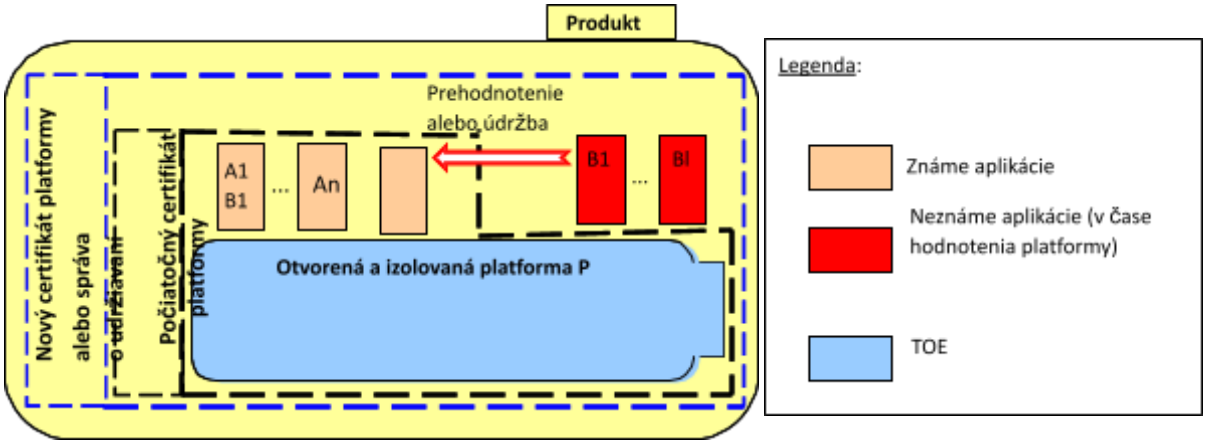
2.3 Údržba otvorenej a izolovanej platformy

Proces kontinuity záruky je možné aplikovať na certifikáty otvorenej a izolovanej platformy rovnako ako na akýkoľvek iný certifikát. Táto kapitola sa zaoberá len špecifikami tohto procesu pre otvorenú a izolovanú platformu, keď nebola vykonaná žiadna významná zmena platformy a keď vývojár chce, aby certifikovaný produkt obsahoval niektoré aplikácie, ktoré neboli známe počas počiatočného hodnotenia.

Je potrebné skontrolovať obmedzenia certifikátu týkajúce sa týchto nových aplikácií. Ak sa overenie a načítanie týchto nových aplikácií vykoná rovnakým vopred vyhodnoteným spôsobom ako v prípade známych aplikácií, čím sa reaguje na OE1 a OE2, môže sa vydať správa o udržiavaní, ak je správa o návšteve miesta stále platná.

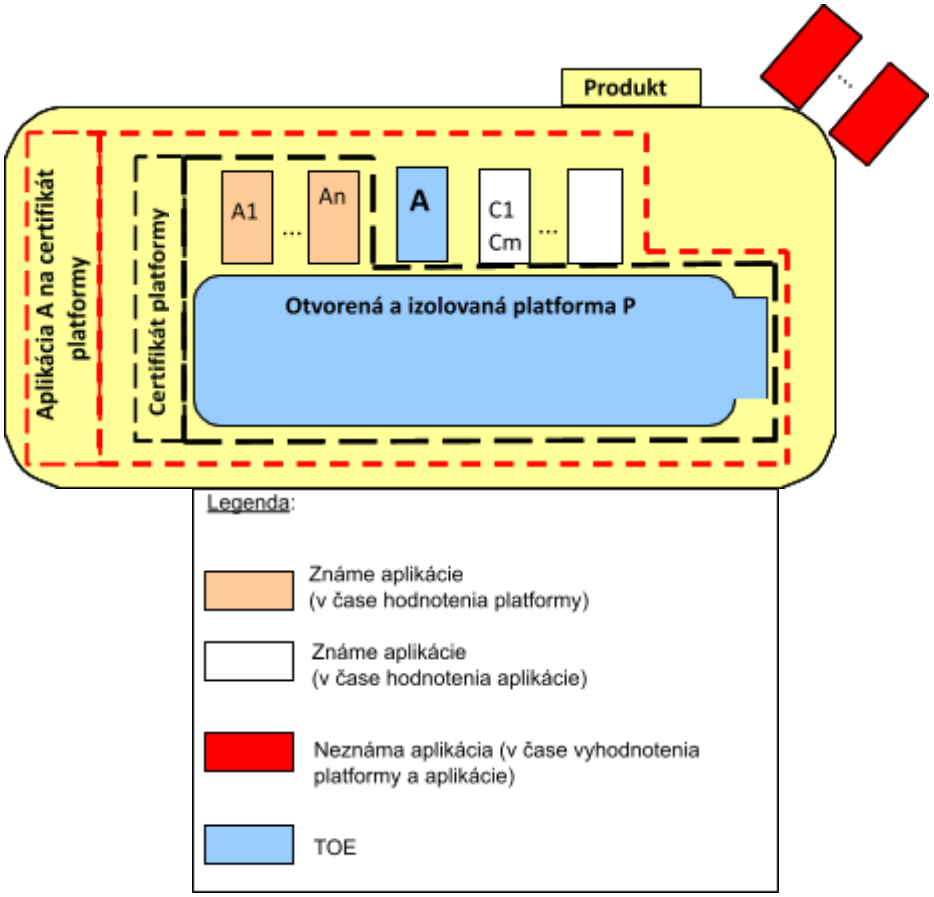
Vývojár bude musieť poskytnúť dôkazy týkajúce sa týchto nových aplikácií spolu s ich analýzou vplyvu (rovnaký typ dôkazov ako tie, ktoré boli poskytnuté počas počiatočného procesu hodnotenia aplikácií Ai (i ∈ [1,n])). V analýze vplyvu sa opíšu aj hlavné funkcie nových aplikácií (aplikácie Bi (i ∈ [1,l])).

Obrázok 3: *Udržiavaný produkt súvisiaci s otvorenou a izolovanou platformou TOE.*



3 APLIKÁCIE NA OTVORENEJ A IZOLOVANEJ PLATFORME

Obrázok 4: *Štandardný certifikát TOE a súvisiaci produkt.*



Na tomto obrázku boli vyhodnotené platforma P a aplikácie Ai (i ∈ [1,n]), ktoré viedli k otvorenému a izolovanému certifikátu platformy. V certifikáte platformy sú identifikované všetky aplikácie Ai.

Aplikácie A Cj (j ∈ [1,m]) zodpovedajú aplikácii načítanej po certifikácii platformy, ale známej v čase

hodnotenia aplikácie. Môžu zodpovedať buď aplikáciám po (prípad 3), alebo pred vydaním (prípad 1 alebo 2).

Aplikácia A je aplikácia, na ktorú sa zameriava aplikácia na hodnotenie platformy. V tomto prípade sa domnievame, že toto hodnotenie sa vykonáva v súlade s procesom skladania definovaným v prílohe 6 s odkazom na:

- obvyklé pokyny na vývoj bezpečnostných aplikácií pre aplikácie, ktoré poskytujú bezpečnostné funkcie;
- príručka [ISO_VERIF], ktorá opisuje obmedzenia kladené na aplikácie s cieľom zachovať vlastnosť izolácie;
- a prípadne usmernenie na ochranu pri načítaní aplikácie [ORG_LOAD] alebo [TECH_LOAD].
- Takže uvažovaným TOE je tu "aplikácia A na platforme P". ITSEF bude musieť samozrejme vykonávať aj ďalšie špecifické činnosti CC. Táto kapitola sa zameriava len na požiadavky kladené na hodnotenie otvorenej a izolovanej platformy.

3.1 Hodnotenie

3.1.1 Ciele z certifikátu platformy

Štandardný proces hodnotenia si vyžaduje zohľadnenie všetkých známych aplikácií. Aplikácie Ai už boli zohľadnené pri hodnotení platformy a sú uvedené v správe o certifikáte platformy (pozri 2.2). Vo výslednej správa o certifikácii A na P sa teda musia identifikovať všetky nové známe aplikácie Cj podľa pravidiel definovaných v 2.1.1.2.

Na spresnenie spôsobu realizácie OE1 a OE2 sa v bezpečnostnom zámere podrobne uvedú účastníci, ktorí sa podieľajú na vývoji, overovaní a distribúcii aplikácií, a ich úlohy. V bezpečnostnom zámere by sa mal opísať aj rozsah hodnotenia, pokiaľ ide o tento podrobný životný cyklus.

ITSEF bude musieť skontrolovať, či všetky aplikácie spĺňajú požiadavky na platformu OE1 a OE2 a či všetky aplikácie Ai a Cj spĺňajú bezpečnostné obmedzenia funkčnej kompatibility aplikácie A (pozri kapitolu 3.1.2).

V prípade aplikácií Cj sa dodržiavanie požiadaviek OE1 a OE2 hodnotí podľa rovnakých pravidiel ako v prípade známych aplikácií Ai v čase hodnotenia platformy (pozri odsek 2.1.5) s odkazom na usmernenie platformy (pozri odsek 2.1.4).

V prípade cieľovej aplikácie A sa dodržiavanie dvoch požiadaviek OE1 a OE2 realizuje počas činností zostavovania (pozri požiadavky bezpečnostných záruk ADV_COMP v prílohe 6) a môže sa riadiť pravidlami definovanými v bode 2.1.5 s odkazom na usmernenie platformy definované v bode 2.1.4 ako v prípade aplikácií Cj.

Načítanie neznámych aplikácií ako Bk ($k \in [1,m]$) znamená, že produkt už plne nevyhovuje architektúre produktu uvedenej v certifikáte otvorenej a izolovanej platformy A na P. Výsledky hodnotenia sú platné len vtedy, ak všetky ostatné aplikácie načítané na platformu rešpektujú obmedzenia certifikácie platformy. Architektúry produktu, ktoré rešpektujú bezpečnostné obmedzenia príslušných certifikátov, možno považovať za certifikované. Je na manažérovi rizík, či sa spoľahne na bezpečnostnú záruku overenia OE1 a OE2, ktoré poskytuje subjekt zodpovedný za nasadenie týchto aplikácií, alebo sa spoľahne na schému. V tomto poslednom prípade potom zadávateľ požiada o údržbu, ako je uvedené v kapitole 3.3 ďalej.

3.1.2 Kompatibilita funkcií zabezpečenia aplikácií

Cieľová aplikácia A môže vyžadovať, aby koexistujúce aplikácie rešpektovali niektoré špecifické bezpečnostné obmedzenia (napríklad aplikácia elektronického pasu nemôže koexistovať s aplikáciou, ktorá umožňuje prenos identity používateľa bez jej súhlasu), ktoré sú výslovne opísané v príručke aplikácie A AGD_OPE.

Predpoklad: Hlavná funkčnosť aplikácie načítanej pred vydaním (aplikácie Ai ($i \in [1,n]$)) musí byť opísaná v ETR a ETR-COMP súvisiacich s hodnotením platformy.

ITSEF bude musieť skontrolovať, či funkcie aplikácií Cj a Ai spĺňajú bezpečnostné obmedzenia požadované aplikáciou A.

Ak by bolo možné certifikovať len niektoré špecifické architektúry produktu, pokiaľ ide o analýzu funkčnej kompatibility, ITSEF to uvedie vývojárovi a požiada ho, aby poskytol každú z týchto architektúr.

3.2 Certifikácia

Všetky koexistujúce aplikácie s certifikovanou aplikáciou sú v takejto správe o certifikácii identifikované ako v otvorenej a izolovanej platforme (pozri bod 2.2). V kapitole "hodnotená konfigurácia" správe
o certifikácii sa však spresní, že certifikované sú aj produkty tvorené podmnožinou známych aplikácií.

3.3 Údržba certifikácie pre aplikácie na otvorenej a izolovanej platforme

V prípade, že vývojár chce, aby certifikovaný produkt obsahoval aj niektoré neznáme aplikácie, ako napríklad Bk, je potrebné stanoviť potrebné obmedzenia certifikátu týkajúce sa týchto aplikácií.

Môže sa poskytnúť správa o analýze vplyvu (IAR):

- keď sa overovanie a načítavanie týchto aplikácií vykonáva rovnakým spôsobom ako v prípade známych aplikácií Ai alebo Cj, čím sa reaguje na požiadavky OE1 a OE2;
- certifikovaná aplikácia A nevyžaduje žiadne obmedzenia funkčnej kompatibility.

Vývojár bude musieť poskytnúť dôkazy týkajúce sa týchto nových aplikácií, ktoré sa načítavajú spolu s analýzou vplyvu (rovnaký typ dôkazov ako tie, ktoré boli poskytnuté počas procesu počiatočného hodnotenia pre aplikácie Ai alebo Cj). V analýze vplyvu sa opíšu aj hlavné funkcie nových aplikácií Bk.

Ak sa toto zaťaženie vykoná v súlade s organizačnými opatreniami, certifikačný orgán bude môcť priamo udržiavať certifikát podľa podmienok definovaných v kapitole 12, PODMIENKY VYDÁVANIA, UDRŽIAVANIA, POKRAČOVANIA A OBNOVOVANIA CERTIFIKÁTOV, ak je správa z návštevy na mieste stále platná.

32. PRÍLOHA 6: HODNOTENIE ZLOŽENÉHO PRODUKTU PRE SMART KARTY A PODOBNÉ ZARIADENIA

ÚČEL

V tejto prílohe sa vymedzuje koncepcia a metodika uplatniteľná na hodnotenie zložených produktov. Produkt pozostáva z hardvérovej časti a súvisiacich knižníc (ak sú k dispozícii) a softvérovej časti, ktorá je zabudovaná do hardvéru a je vytvorená na prevádzku s týmto hardvérom. Obe časti sa môžu hodnotiť nezávisle; tým by sa mohla zvýšiť účinnosť hodnotenia, keďže hardvérová časť sa môže používať
s mnohými rôznymi softvérovými aplikáciami

KONKRÉTNY STAV

Žiadne.

KRÍŽOVÝ ODKAZ NA KAPITOLU(-Y), V KTOREJ(-ÝCH) SÚ TIETO PRVKY VYHLÁSENÉ ZA UPLATNITEĽNÉ

Kapitola 8, ŠPECIFICKÉ HODNOTIACE KRITÉRIA A METÓDY.

1 ÚVOD

1.1 Pozadie

Spoločné kritériá (Common Criteria - CC) sa vo veľkej miere používajú na hodnotenie bezpečnosti produktov smart kariet. Pri hodnotení smart kariet sa veľmi skoro ukázala potreba výkladu a podporných dokumentov.

Prvotným dôvodom bolo, že smart karta je vytvorená kombináciou dvoch častí: hardvérovej časti integrovaného obvodu (IC) a softvérovej časti, ktorú často vyvíjajú rôzne subjekty s konkrétnymi cieľmi.

Ďalším dôvodom je, že samotná softvérová časť môže byť vrstvená a pozostávať z "vrstvy operačného systému" s prípadnými integrovanými aplikačnými funkciami a "aplikačnej vrstvy", ktorá môže obsahovať rôzne aplikácie. Všetky tieto softvérové časti môžu vyvíjať rôzne subjekty so špecifickými cieľmi.

Jedným z cieľov bolo nezávisle vykonať jedno hodnotenie platformy, ktoré by sa týkalo viacerých aplikácií a zákazníkov.

Ďalším cieľom bolo vytvoriť jednu alebo viacero aplikácií, ktoré by sa načítali na jednu alebo viacero certifikovaných platforiem.

Cieľom integrácie aplikácií bolo nainštalovať jednu alebo viacero aplikácií na jednu už certifikovanú platformu, aby sa znížilo úsilie na hodnotenie pri zachovaní vysokej úrovne dôvery.

Na dosiahnutie týchto cieľov bol definovaný prenos poznatkov a opakované použitie dôkazov.

1.2 Definície

Hardvérová časť s príslušnými knižnicami (ak sú k dispozícii) sa hodnotí samostatne, pretože sa môže

používať s mnohými rôznymi softvérovými aplikáciami.

Softvér je zabudovaný do hardvéru a je vytvorený tak, aby fungoval s týmto hardvérom. Výsledný produkt je ten, ktorý sa používa v praxi (mobilné telefóny, bankové karty, zdravotné karty, identifikačné karty, digitálny podpis, e-pas, e-ticketing atď.) a ku ktorému zákazníci/užívatelia potrebujú získať dôveru.

Softvérové aplikácie môžu byť vytvorené tak, aby fungovali s podporou operačného systému. OS poskytuje mechanizmus oddelenia medzi sebou a softvérovými aplikáciami, ako aj služby softvérovým aplikáciám.

Ďalším špecifikom produktu typu smart karty je, že softvérová časť musí používať, ovládať, konfigurovať alebo aktivovať bezpečnostné mechanizmy poskytované hardvérom. A softvérové aplikácie môžu používať, ovládať, konfigurovať alebo aktivovať bezpečnostné mechanizmy poskytované operačným systémom.

1.3 Hodnotenie zložených produktov a ACO

Hoci CC zavádza špecifickú triedu záruk ACO pre zloženie, táto trieda nie je vhodná na bežné hodnotenie smart kariet a podobných zariadení.

ACO rieši TOE zloženú z dvoch certifikovaných TOE: základného TOE a závislého TOE (pozri obrázok 1). Hodnotenie zloženého TOE spočíva v hodnotení interakcie medzi oboma TOE, pričom sa opätovne použijú výsledky hodnotenia základného TOE a závislého TOE.

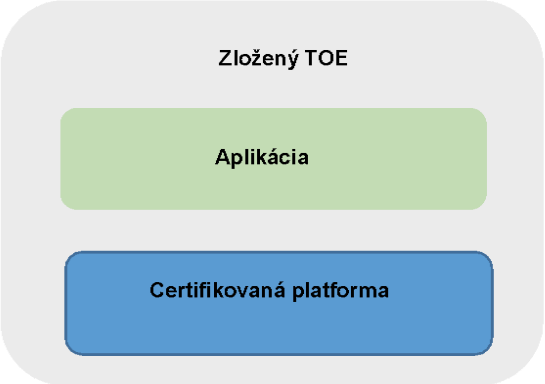
Výsledkom tohto hodnotenia nie je úroveň EAL, ale úroveň CAP, ktorá nie je porovnateľná s úrovňou EAL. Okrem toho trieda ACO je použiteľná až do rozšírenej základnej úrovne záruky, zatiaľ čo smart karty, najmä v bankovníctve alebo pri podpisových aplikáciách, vyžadujú "vysokú úroveň" záruky.

Obrázok 1: *ACO zložený z TOE (balík CAP)*

V prípade smart kariet a podobných zariadení je zložený produkt konečným produktom, pre ktorý sa vyžaduje certifikácia na úrovni EAL. To umožňuje priame porovnanie s podobnými produktmi certifikovanými po jednom hodnotení.

Vzhľadom na architektúru smart karty sa skladá z hardvérovej platformy, zvyčajne integrovaného obvodu a zabudovanej softvérovej vrstvy na hardvérovej platforme. Vstavaný softvér môže byť sám o sebe aplikáciou alebo sa skladá z "vrstvy operačného systému" s ďalšou "vrstvou aplikácie" nad "vrstvou operačného systému". Hardvér a možno aj "vrstva OS" môžu spolu tvoriť platformu s aplikáciou na jej vrchole. Pri hodnotení zloženého TOE sa certifikuje Platforma, hodnotí sa Aplikácia a výsledky certifikácie Platformy sa opätovne použijú. Pozri obrázok 2 bezpečnostnej certifikácie celého zloženého TOE.

Obrázok 2: *Hodnotenie zloženého produktu (súčasný prístup)*



Vlastnosti hardvérovej platformy týkajúce sa zabezpečenia a bezpečnostných funkcionalít sú uvedené v bezpečnostnom zámere. Platforma poskytuje mechanizmy na ochranu aktív zloženého produktu, ale správanie zloženého produktu vo veľkej miere závisí od softvérovej aplikácie, ktorá musí tieto bezpečnostné mechanizmy používať, konfigurovať a aktivovať.

Platforma OS ponúka bezpečnostné služby a poskytuje mechanizmy na ochranu aktív zloženého produktu. Správanie zloženého produktu závisí vo veľkej miere od softvérovej aplikácie, ktorá musí využívať bezpečnostné služby a používať, konfigurovať a aktivovať tieto služby. Výsledky hodnotenia platformy preto poskytujú bezpečnostné odporúčania a podmienky formulované v návode pre používateľov platformy na implementáciu softvérovej aplikácie.

Hodnotiteľ zloženého produktu okrem iného skúma, či kombinácia aplikácie a platformy nevedie k žiadnej zneužiteľnej zraniteľnosti. Metodika hodnotenia zložených smart kariet definuje presné pracovné jednotky s jasným vyhlásením o informáciách potrebných od vývojára platformy a poskytuje dohodnutý "rámec" na prenos informácií od platformy k hodnotiteľovi zloženého produktu.

Požadované informácie sú už k dispozícii z úloh hodnotenia platformy a od vývojára platformy sa nevyžaduje žiadna ďalšia práca.

- Nie je potrebné uvádzať podrobnosti o triede ADV pre vývoj platformy.
- Používateľské pokyny (AGD) platformy sa zohľadňujú na začiatku vývoja zloženého produktu a poskytujú všetky potrebné informácie o rozhraniach.
- Vývoj a hodnotenie zloženého TOE sa spoliehajú na správnu implementáciu hodnotených rozhraní platformy.
- Správne používanie všetkých relevantných rozhraní medzi platformou a aplikáciou patrí do rozsahu hodnotenia zloženého produktu.
- Skúška (ATE) a hodnotenie zraniteľnosti (AVA) sa vykonávajú na zloženom produkte s využitím výsledkov hodnotenia platformy.

Koncepcia hodnotenia zloženého TOE neobmedzuje zložené hodnotenie v EAL a odolnosti proti útokom, t. j. až na "vysoká", zatiaľ čo zložené TOE (balík CAP) je obmedzené odolnosťou proti útokom "rozšírená-základná".

1.4 Cieľ a rozsah pôsobnosti

Cieľom tejto prílohy je presne vymedziť úlohy pre rôzne strany zapojené do hodnotenia zloženého TOE.

Cieľom nie je definovať ďalšiu triedu záruk, ale definovať spresnenia existujúcich požiadaviek bezpečnostných záruk pre hodnotenie zloženého produktu.

Táto príloha sa zaoberá TOE, ktoré patria do technickej domény "smart karty a podobné zariadenia". Táto príloha sa však neobmedzuje len na smart karty a podobné zariadenia a v zásade sa môže uplatňovať (prípadne s primeranými úpravami, pokiaľ je to potrebné) na akýkoľvek iný bezpečný produkt IKT, ktorého nezávisle hodnotený komponent je súčasťou konečného zloženého produktu, ktorý sa má hodnotiť.

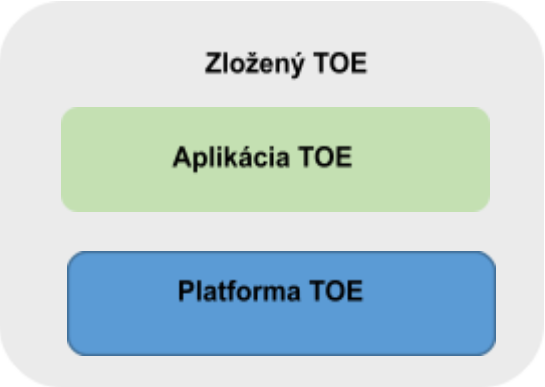
Technická doména smart kariet a podobných zariadení je definovaná ako: súvisiaca so smart kartami

a podobnými zariadeniami, kde významná časť požadovanej bezpečnostnej funkcionality závisí od hardvérových prvkov na úrovni čipu (napríklad hardvér/IC smart kariet, zložené produkty smart kariet, moduly dôveryhodnej platformy (TPM) používané v dôveryhodných počítačoch, karty digitálnych tachografov, atď.).

2 DEFINÍCIE / TERMINOLÓGIA

2.1 Definície

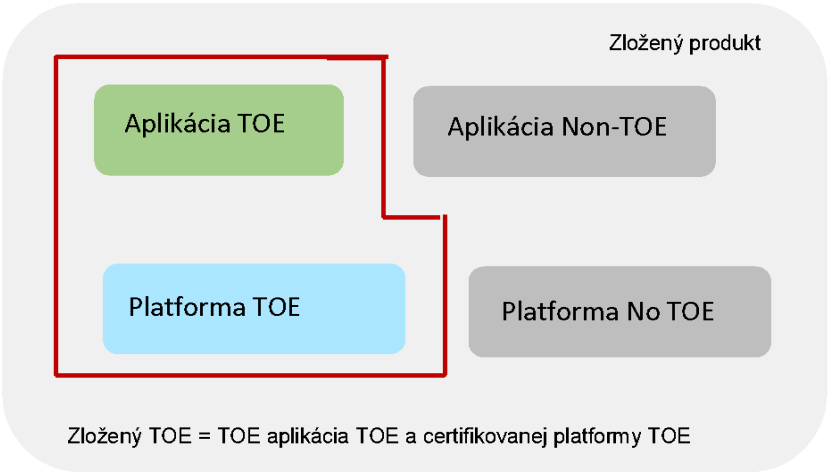
Obrázok 3: *Zložený produkt*



Zložené TOE je TOE, ktorá sa skladá zo superpozície 2 vrstiev, ako je znázornené na obrázku 3, počiatočnej vrstvy (označenej ako "platforma") a doplnkovej vrstvy ("aplikácia"):

- Počiatočná vrstva je podkladová vrstva, ktorá môže byť buď jedným produktom, alebo zloženým produktom. Máme za to, že táto vrstva už bola certifikovaná.
- Doplnková vrstva závisí od platformy. Táto vrstva podlieha zloženému hodnoteniu.

Obrázok 4: *Zložený TOE*



Zložená TOE je zložená z platformy a aplikácie a pozostáva z "platformovej TOE" a "aplikačnej TOE", ako je vyznačené v červenom rámčeku na obrázku 4, s týmito obmedzeniami:

- Aplikácia TOE sa nemôže spoliehať na funkcie platformy, ktoré sú mimo platformy TOE, v častiach mimo TOE. Na obrázku 4 je to znázornené sivou vrstvou "Non-(platform) TOE".
- Zložený TOE sa skladá z nadmnožiny celej aplikačnej TOE a nadmnožiny minimálnych funkcií TOE platformy potrebných na správne vykonanie zloženého produktu.
- Podskupina aplikácie, ktorá nie je TOE, môže využívať funkcie platformy TOE. Ako zvyčajne, zložené hodnotenie musí určiť, či táto časť aplikácie, ktorá nie je TOE, nezasahuje do aplikácie

TOE - ani priamo, ani prostredníctvom používania funkcií platformy.

Príkladom môže byť operačný systém ("aplikácia") bežiaci na hardvérovej platforme ("základná platforma") alebo Java CardTM applet ("aplikácia") bežiaci na Java Card runtime prostredí ("platforma").

Niekoľko krokov zloženia môže nasledovať za sebou, t. j. zložený produkt sa môže opierať o platformu, ktorá je sama zloženým produktom. Pre takéto zloženia s predtým zloženým produktom platia rovnaké pravidlá.

Tieto definície sú v súlade s definíciami tried ACO, kde:

- Platforma je základným komponentom,
- Aplikácia je závislým komponentom.

2.2 Úlohy

Pri činnostiach komplexného hodnotenia sa zohľadňujú tieto úlohy:

- Vývojár platformy: Môže to byť aj žiadateľ o hodnotenie platformy.
- Hodnotiteľ platformy: Subjekt, ktorý vykonáva hodnotenie platformy.
- Certifikačný orgán platformy: subjekt vykonávajúci certifikáciu platformy, v terminológii CC definovaný ako hodnotiaci orgán.
- Vývojár aplikácie: Subjekt, ktorý vyvíja aplikáciu spustenú na platforme.
- Integrátor zložených produktov: Subjekt, ktorý inštaluje aplikácie na platforme.
- Hodnotiteľ zložených produktov: Subjekt, ktorý vykonáva hodnotenie zloženého produktu.
- Certifikačný orgán pre zložené produkty: Subjekt vykonávajúci certifikáciu zložených produktov definovaný v terminológii CC ako hodnotiaci orgán.
- Hodnotenie zložených produktov Žiadateľ: Subjekt zodpovedný za zadanie hodnotenia zloženého produktu (môže to byť vývojár aplikácie).

Pri každom hodnotení sa k týmto všeobecným úlohám priradia konkrétne organizácie alebo osoby.

Na ilustráciu úlohy integrátora zložených produktov uvádzame niekoľko príkladov:

- Vlastné smart karty: Vývojár platformy je výrobca integrovaného obvodu (čipu); "aplikácia" je operačný systém karty a jeho aplikácia (aplikácie) a vývojár aplikácie je vývojár softvéru smart karty a aplikácie (aplikácií). V tomto prípade úlohu integrátora zloženého produktu zohráva i) výrobca čipu, ktorý vloží jadro operačného systému do pamäte ROM čipu, a potom ii) výrobca karty, ktorý zvyčajne nahrá niektoré časti operačného systému a aplikácie do pamätí NV (EEPROM a/alebo Flash) čipu.
- Zariadenia s podporou technológie Java Card: Základnou platformou" je prostredie Java Card Runtime Environment (Java Card RE) na čipe a vývojárom platformy je výrobca/vydavateľ karty; "aplikáciou" je Java Card applet a môže ju vyvinúť vývojár aplikácie. V tomto prípade je ďalšou rolou je Integrátor zloženého produktu (Composite Product Integrator), ktorého môže hrať poskytovateľ doménových/aplikačných služieb alebo centrum dôvery, ktoré načíta applet a často kartu elektronicky personalizuje.

3 KONCEPT ZLOŽENÉHO HODNOTENIA

3.1 Aké sú problémy?

Aktíva, ktoré sa majú chrániť, sú konečné aktíva zloženého produktu definované v bezpečnostnom zámere zloženého produktu.

Bezpečnostné mechanizmy, ktoré sa podieľajú na ochrane týchto aktív, sú tie, ktoré poskytuje platforma a samotná aplikácia.

Niektoré bezpečnostné mechanizmy a bezpečnostné služby poskytované platformou si môžu vyžadovať konfiguráciu, programovanie alebo aktiváciu aplikáciou.

Vývojár aplikácie preto potrebuje všetky informácie (vo forme návodu alebo používateľskej príručky) týkajúce sa bezpečnostných mechanizmov platformy a bezpečnostných služieb, ktoré má aplikácia spravovať.

Okrem toho potrebuje bezpečnostný zámer platformy, aby mohol vytvoriť zložený bezpečnostný zámer produktu a zabezpečiť konzistentnosť definície bezpečnosti medzi vývojom platformy a aplikácie. Vyhodnotenie sa vykonáva a overuje na konečnom zloženom produkte.

Ak sú časti platformy a aplikácie spojené do zloženého produktu, hodnotiteľ zloženého produktu musí preskúmať, či je dosiahnutá úroveň bezpečnosti požadovaná bezpečnostným cieľom. Hodnotiteľ zloženého produktu preto musí vykonať úlohy hodnotenia potrebné vzhľadom na bezpečnostný zámer konečného zloženého produktu a poskytnúť súvisiaci ETR. Z tohto hľadiska by mal hodnotiteľ zloženého produktu opätovne použiť výsledky hodnotenia a certifikácie platformy, čím sa ušetria náklady a čas.

3.2 Aké informácie sú potrebné?

Hodnotiteľ zložených produktov nepotrebuje všetky výsledky hodnotenia platforiem. Bezpečnostný certifikát a správa o certifikácii zaručujú, že platforma bola hodnotená podľa Spoločných kritérií. Hodnotiteľ zloženého produktu bude potrebovať doplňujúce informácie o opatreniach bezpečnostných záruk, ak sa vývoj platformy a aplikácie prelínajú. Na kontrolu, či aplikácia spĺňa bezpečnostné požiadavky na používanie platformy, bude hodnotiteľ zloženého produktu potrebovať rovnakú úroveň znalostí o platforme ako vývojár aplikácie. Okrem štandardného množstva hodnotiacich príspevkov podľa balíka záruky zvoleného pre hodnotenie zloženého produktu (napr. úroveň EAL) je potrebné hodnotenie (ďalšie podrobnosti sú uvedené v časti 4.7 "Doručovanie"):

- Všetky informácie dodané od vývojára platformy integrátorovi zloženého produktu,
- Všetky informácie dodané od vývojára platformy vývojárovi aplikácie,
- ETR pre zložené hodnotenie, ktoré pripravil hodnotiteľ platformy, pozri kapitolu 5 "ETR pre zložené hodnotenie" (vrátane informácií o analýze zraniteľnosti a testovaní prienikov),
- Informácie o súlade bezpečnostných zámerov a návrhov platformy a aplikácie, ktoré pripravil vývojár aplikácie,
- Informácie o súlade postupov dodávok zo strany vývojárov platforiem a aplikácií s postupom akceptácie zo strany integrátora zložených produktov,
- Informácie o integrácii oboch častí s použitím ich správnych certifikovaných verzií a správnych konfiguračných parametrov. Tieto informácie pripraví integrátor zloženého produktu; znamená to aj bezpečnostnú záruku, že aplikáciu správne spravuje vývojár platformy (napr. v prípade smart karty, kde sa dodáva kód ROM na maskovanie na platforme).

Certifikačný orgán pre zložené produkty bude potrebovať rovnaké množstvo informácií ako hodnotiteľ zložených produktov.

3.3 Prípad zmeny zloženého produktu

V prípade zmien zloženého produktu v dôsledku menšej zmeny platformy alebo aplikácie, prípadne oboch, si pozrite prílohu 11, KONTINUITA ZÁRUKY.

Ak zmena pochádza z platformy, posúdenie zmeny pre platformu vykoná certifikačný orgán platformy. Na základe toho posudzovanie zmeny pre zložený produkt vykonáva certifikačný orgán pre zložený produkt.

Ak zmena vyplynie zo žiadosti, posúdenie zmeny zloženého produktu vykoná certifikačný orgán pre zložené produkty.

3.4 Špecifický prípad, keď je žiadosť už certifikovaná

V prípade, že platforma aj aplikácia už boli certifikované, môže sa vykonať čiastočné hodnotenie na základe výsledkov získaných z predchádzajúceho hodnotenia aplikácie. Napriek tomu sa stále vyžadujú zložené úlohy hodnotenia definované v tomto dokumente.

4 OPIS ČINNOSTÍ ZLOŽENÉHO HODNOTENIA

Súčasný prístup možno uplatniť nezávisle od hodnotenie úrovne záruky (EAL) pre zameraný zložený produkt. Ak niektoré hodnotiace činnosti nie sú uplatniteľné vzhľadom na zvolenú úroveň EAL, nepredpokladá sa ani ich uplatnenie.

V nasledujúcich odsekoch možno predpokladať, že úroveň záruky platformy je rovnaká alebo vyššia v porovnaní s úrovňou hodnotenia zloženého produktu.

Ostatné prípady sa musia prerokovať v rámci systémov.

Prvky činností vývojára a hodnotiteľa špecifické pre zloženie, ako aj činnosti hodnotiteľa (pracovné jednotky) patriace k činnostiam zloženia sú definované ako spresnenia pre hodnotenie zloženia, pozri prílohu 1: Špecifické požiadavky pre zloženie.

4.1 Hodnotenie bezpečnostného zámeru zloženého produktu

Je potrebné napísať a vyhodnotiť bezpečnostný zámer pre zložený produkt.

Hodnotiteľ zloženého produktu musí preskúmať, či bezpečnostný zámer zloženého produktu[39] nie je v rozpore s bezpečnostným zámerom základnej platformy[40]. Konkrétne to znamená, že hodnotiteľ zloženého produktu musí preskúmať bezpečnostný zámer zloženého produktu a platformy z hľadiska akýchkoľvek protichodných predpokladov, kompatibility bezpečnostných cieľov, bezpečnostných požiadaviek a bezpečnostných funkcionalít potrebných pre aplikáciu.

[R1] Táto úloha sa dá obmedziť, ak sa skontroluje zhoda ochranných profilov, ktoré si nárokujú jednotlivé bezpečnostné zámery.

[R2] Žiadateľ o hodnotenie zloženého produktu musí zabezpečiť, aby bol bezpečnostný zámer platformy k dispozícii vývojárovi aplikácie, hodnotiteľovi zloženého produktu a certifikačnému orgánu zloženého produktu. Informácie dostupné vo verejnej verzii bezpečnostného zámeru nemusia byť dostatočné.

4.2 Integrácia aplikácie do systému správy konfigurácie

[R3] Hodnotiteľ zloženého produktu overí, či bola hodnotená verzia aplikácie nainštalovaná na hodnotenú verziu základnej platformy alebo do nej vložená.

[R4] Žiadateľ o hodnotenie zloženého produktu musí zabezpečiť, aby mal hodnotiteľ zloženého produktu k dispozícii príslušné dôkazy vytvorené integrátorom zloženého produktu. Tieto dôkazy môžu okrem iného zahŕňať zoznam konfigurácie vývojára platformy, ktorý poskytol v rámci svojho vyhlásenia o uznaní

4.3 Kontrola zlučiteľnosti pre dodacie a preberacie postupy

[R5] Hodnotiteľ zloženého produktu overí, či sú postupy dodávok vývojárov aplikácií a platforiem kompatibilné s postupom akceptácie, ktorý používa integrátor zloženého produktu.

[R6] Hodnotiteľ zloženého produktu overí, či integrátor zloženého produktu používa všetky konfiguračné parametre predpísané vývojármi aplikácií a platforiem (napr. predpersonalizačné údaje, predpersonalizačné skripty).

[R7] Žiadateľ o hodnotenie zloženého produktu musí zabezpečiť, aby mal hodnotiteľ zloženého produktu k dispozícii príslušné dôkazy vytvorené integrátorom zloženého produktu. Tieto dôkazy môžu okrem iného zahŕňať: prvok dôkazu o prijatí, akceptácii a parametrizácii aplikácie zo strany vývojára platformy (vo forme vyhlásenia o potvrdení).

4.4 Súlad návrhov

[R8] Hodnotiteľ zloženého produktu overí, či sú ustanovenia pre vývojára aplikácie, ktoré stanovil vývojár platformy vo svojich certifikovaných pokynoch pre používateľov a na ktoré sa odkazuje v správe o certifikácii platformy, splnené zloženým produktom, t. j. či ich vývojár aplikácie zohľadnil.

[R9] Žiadateľ o hodnotenie zloženého produktu musí zabezpečiť, aby boli hodnotiteľovi zloženého produktu k dispozícii tieto informácie:

- Pokyny pre používateľov súvisiace s platformou,

[39] Ďalej len "Zložený ST".

[40] Ďalej len "Platforma-ST".

- ETR pre zložené hodnotenie, ktoré pripravil hodnotiteľ platformy, pozri kapitolu 5 "ETR pre zložené hodnotenie",
- Správa o certifikácii pre platformu vypracovaná certifikačným orgánom platformy,
- Odôvodnenie bezpečnej implementácie zloženého produktu vrátane dôkazov pripravených vývojárom aplikácie.

4.5 Skúšanie funkčnosti zložených produktov

[R10] Skúšanie funkčnosti niektorých aplikácií sa môže vykonávať len na emulátoroch pred ich vložením/integráciou do platformy, pretože efektívnosť tohto testovania (vyhovuje/nevyhovuje) nemusí byť viditeľná pomocou rozhraní zloženého produktu. Napriek tomu sa skúšanie funkčnosti zloženého produktu vykonáva aj na vzorkách zloženého produktu podľa opisu bezpečnostných funkcionalít zloženého TOE a s použitím štandardného prístupu, ako to vyžaduje príslušná trieda záruk. Tu sa nevyžaduje žiadna ďalšia činnosť vývojára.

[R11] Keďže množstvo, pokrytie a hĺbka funkčných skúšok platformy už boli overené certifikátom platformy, nie je potrebné tieto úlohy v rámci komplexného hodnotenia vykonávať znova. Upozorňujeme, že ETR pre zložené hodnotenie (pozri kapitolu 5 "ETR pre zložené hodnotenie") neposkytuje žiadne informácie o funkčnom skúšaní platformy.

[R12] Žiadateľ o hodnotenie zloženého produktu musí zabezpečiť, aby mal hodnotiteľ zloženého produktu k dispozícii tieto informácie:

- Vzorky zložených produktov vhodné na skúšanie.

4.6 Analýza zraniteľnosti zloženého produktu

[R13] Hodnotiteľ zloženého produktu vykoná analýzu zraniteľnosti zloženého produktu, pričom okrem iného použije výsledky hodnotenia a certifikácie platformy. Táto analýza zraniteľnosti sa potvrdí penetračným testovaním.

[R14] Hodnotiteľ zloženého produktu musí skontrolovať, či je ochrana dôvernosti zabudovaného softvéru v pamäti platformy v súlade s úrovňou dôvernosti deklarovanou vývojárom aplikácie pre ALC_DVS.

[R15] V osobitných prípadoch môže byť analýza zraniteľnosti a definovanie útokov náročné, vyžaduje si značný čas a rozsiahle predbežné testovanie, ak je k dispozícii len dokumentácia. Platforma sa môže používať aj spôsobom, ktorý vývojár platformy a hodnotiteľ platformy nepredpokladali, alebo vývojár aplikácie nemusel dodržať ustanovenia uvedené pri certifikácii platformy. V takýchto prípadoch existujú rôzne možnosti skrátenia zloženej analýzy zraniteľnosti:

- Hodnotiteľ zloženého produktu sa môže poradiť s hodnotiteľom platformy a využiť jeho skúsenosti získané počas hodnotenia platformy.
- Oddelenie zraniteľností aplikácie a platformy pomocou "otvorených vzoriek" ("otvorené vzorky" sú vzorky platformy, na ktoré môže hodnotiteľ zloženého produktu nahrať softvér podľa vlastného uváženia). Zámerom je používať testovací softvér bez aplikačných protiopatrení bez deaktivácie akéhokoľvek protiopatrenia vlastného platforme. Cieľom je jednoznačne neopakovať hodnotenie platformy. (Ďalšie podrobnosti sú uvedené v prílohe 7, UPLATNENIE POTENCIÁLU ÚTOKU NA SMART KARTY A PODOBNÉ ZARIADENIA).

[R16] Žiadateľ o hodnotenie zloženého produktu musí zabezpečiť, aby mal hodnotiteľ zloženého produktu k dispozícii tieto informácie:

- ETR pre zložené hodnotenie (ETR_COMP), ktorý pripravil hodnotiteľ platformy, pozri kapitolu 5 "ETR pre zložené hodnotenie" nižšie,
- Správa o certifikácii pre platformu vypracovaná certifikačným orgánom platformy.

4.7 Dodávky

V nasledujúcich tabuľkách sú zhrnuté dodávky dokumentácie, ktoré si strany vymieňajú, aby umožnili činnosti zloženého hodnotenia, ako sú definované v predchádzajúcich odsekoch.

Žiadateľ o hodnotenie zloženého produktu je zodpovedný za začatie procesu.

Žiadateľ o hodnotenie zloženého produktu je zodpovedný za zachovanie alebo vytvorenie akejkoľvek dohody o zachovaní mlčanlivosti (NDA), ktorá by bola potrebná medzi všetkými stranami zapojenými

do činností spojených so zložením.

Dohoda o zachovaní mlčanlivosti by mala byť uzavretá v závislosti od citlivosti a vlastníctva informácií, ktoré sa majú vymieňať.

Tabuľka 1: *Definícia dokumentov o zložení*

Číslo	Dokument/Príspevok	Popis
1	Bezpečnostný zámer platformy	Bezpečnostný zámer platformy uvedený v správe o certifikácii platformy.
2	Otvorené vzorky platformy na skúšanie	Vzorky platforiem, ako sú definované v prílohe 7.
3	Pokyny pre používateľov platformy	Zahŕňa všetky pokyny pre používateľov platformy a príručky potrebné pre vývojára aplikácií a integrátora zložených produktov, na ktoré sa odkazuje v správe o certifikácii platformy.
4	Platforma ETR_COMP	ETR pre zloženie, ako je definované v kapitole 5 a uvedené v správe o certifikácii platformy.
5	Správa o certifikácii platformy	Správa o certifikácii platformy vydaná autorizovaným certifikačným orgánom platformy.
6	Dôkazy o súlade návrhu	Obsahuje prvky dôkazov o tom, ako sú v zloženom produkte splnené požiadavky na návrh aplikácie, ktoré sú stanovené v usmernení platformy a správe o certifikácii.
7	Dôkazy o zloženej konfigurácii	Zahŕňa: (i.) Identifikačné prvky zloženého produktu ● preukázanie, že v zloženom produkte sa používa správna certifikovaná verzia platformy, ● preukázanie, že bola integrovaná správna, vyhodnotená verzia aplikácie; (ii.) a Dôkazné prvky, že integrátor zloženého produktu skutočne uplatňuje bezpečnostné opatrenia predpísané vývojármi platformy a aplikácie
8	Dôkazy o postupoch dodávania a preberania	Prvky dôkazov o tom, ako sú postupy dodávania vývojárov platforiem a aplikácií kompatibilné s postupom prijímania integrátora zloženého produktu.

V nasledujúcej tabuľke je uvedené, ktoré dokumenty/príspevky z tabuľky 1 sa poskytnú ktorému účastníkovi v rámci procesu komplexného hodnotenia.

Tabuľka 2: *Hlavné dodávky medzi aktérmi*

##	Dokument / Príspevok	Hodnotenie zložených produktov Žiadateľ	Integrátor zložených produktov	Vývojár aplikácií	Hodnotiteľ zložených produktov	Zložený produkt CB
1	**Bezpečnostný zámer platformy**	Nie	Nie	Áno	Áno	Áno
2	**Otvorené vzorky platformy na testovanie**	Nie	Nie	Nie	Áno	Áno
3	**Pokyny pre používateľov platformy**	Nie	Áno	Áno	Áno	Áno
4	**Platforma ETR_COMP**	Nie	Nie	Nie	Áno	Áno
5	**Správa o certifikácii platformy**	Áno	Áno	Áno	Áno	Áno
6	**Dôkazy o súlade návrhu**	Nie	Nie	Nie	Áno	Áno
7	**Dôkazy o zloženej konfigurácii**	Nie	Nie	Nie	Áno	Áno
8	**Dôkazy o postupoch dodávania a preberania**	Nie	Nie	Nie	Áno	Áno

V nasledujúcej tabuľke sú uvedené niektoré príklady prípadov použitia zloženého TOE s definíciou komponentov a rolí.

Tabuľka 3: Príklad zložených prípadov použitia TOE

Definície komponentov a rolí	**Smart karta – I** **Zložený TOE je postavený z:** - **bezpečnostný integrovaný obvod s aplikačným kódom nahraným v pamäti ROM (operácia maskovania) a aplikačnými údajmi nahranými v pamäti EEPROM**	**Smart karta – II** **Zložený TOE je postavený z** - **bezpečnostný integrovaný obvod bez pamäte ROM, ale s technológiou Flash a zavádzačom Flash** - **aplikačný kód a údaje nahrané do pamäte flash výrobcom smart karty.**	**Karta Java** **Zložený TOE je postavený z** - **platforma Java Card** - **aplikácia Java card: applet**
Platforma je	Bezpečnostný IC	Bezpečnostný integrovaný obvod s pamäťou Flash a zavádzačom Flash	Platforma Java Card vrátane správcu kariet so zariadením Applet loader
Aplikácia je	Kód operačného systému a ďalšie dátové súbory	Kód operačného systému, inicializačné údaje pamäte Flash a údaje aplikácie	Applet
Vývojár platformy je	Výrobca bezpečnostných integrovaných obvodov:	Vývojár platformy je	Výrobca bezpečnostných integrovaných obvodov:
Vývojár aplikácie je	Vývojár softvéru Smartcard: - Vyvíja aplikáciu; - Poskytuje aplikáciu integrátorovi zložených produktov	Vývojár softvéru Smartcard: - Vyvíja aplikáciu; - Dodanie aplikácie integrátorovi zložených produktov	Vývojár Appletu: - Vyvíja applet; - Dodanie appletu integrátorovi zložených produktov
Integrátor zložených produktov je	Výrobca bezpečnostných integrovaných obvodov: - má na starosti maskovanie operačného systému v pamäti ROM a načítanie údajov aplikácie do pamäte EEPROM; - Dodáva zložený TOE, ktorý sa má hodnotiť	Výrobca karty: - má na starosti načítanie aplikácie do pamäte flash pomocou Security IC flash loader; - Dodáva zložený TOE, ktorý sa má hodnotiť	Vydavateľ karty: - Načíta applet na platforme Java Card pomocou mechanizmu načítania appletu; - Dodáva zložený TOE, ktorý sa má hodnotiť

5 ETR PRE ZLOŽENÉ HODNOTENIE

5.1 Cieľ dokumentu

Štandardná technická správa hodnotenia (ETR) obsahuje informácie, ktoré sú predmetom vlastníctva a ktoré nemožno zverejniť. Dokument ETR pre zložené hodnotenie (ETR_COMP) je zostavený z ETR s cieľom poskytnúť dostatočné informácie pre zložené hodnotenie produktu s certifikovanou platformou. Informácie, ktoré sú uvedené v dokumente ETR_COMP, sú podmnožinou informácií uvedených
v úplnom ETR. Mal by umožniť hodnotiteľovi zloženého produktu a príslušnému certifikačnému orgánu pochopiť posudzované cesty útoku, vykonané testy a efektívnosť protiopatrení implementovaných platformou.

Vzor dokumentu ETR_COMP je uvedený v dodatku 2: Vzor ETR pre zložené hodnotenie.

5.2 Všeobecné pravidlá:

[R17] ETR pre zložené hodnotenie by mal vypracovať hodnotiteľ platformy na základe výsledkov hodnotenia platformy. Táto úloha by sa mala zohľadniť pri určovaní pracovného programu hodnotenia, aby sa znížili dodatočné náklady a úsilie.

[R18] Obsah ETR_COMP musí nájsť správnu rovnováhu medzi ochranou vlastníckych informácií vývojára platformy a/alebo hodnotiteľa platformy a poskytnutím dostatočných informácií pre hodnotiteľa zloženého produktu a príslušný certifikačný orgán, pozri tabuľku 2 vyššie.

[R19] ETR_COMP neobsahuje informácie ovplyvňujúce národnú bezpečnosť.

[R20] Poskytnuté informácie musia schváliť všetky strany zapojené do hodnotenia platformy (t. j. hodnotiteľ, certifikačný orgán, vývojár a žiadateľ o hodnotenie). Certifikačný orgán platformy musí potvrdiť jej súlad s pôvodným ETR. Správa o certifikácii platformy musí odkazovať na ETR pre zložené hodnotenie.

[R21] Ak sa aktuálny ETR_COMP sám spolieha na zložené hodnotenie a ak existuje priame rozhranie s predchádzajúcou platformou, musí sa uviesť odkaz na toto predchádzajúce zložené hodnotenie ETR_COMP.

[R22] ETR_COMP nemá obsahovať kópie informácií z iných dostupných dôkazov platformy, ako je bezpečnostný zámer a usmernenie. Súhrnné hodnotenie je však značne podporené odkazmi na príslušné časti.

5.3 Výmena ETR za zloženie

ETR_COMP obsahuje duševné vlastníctvo vývojára platformy, ako aj hodnotiteľa platformy a na jeho obsahu sa podieľa aj certifikačný orgán platformy. Dokument by sa mal považovať minimálne za dokument s obmedzeným prístupom. Dokument ETR_COMP vytvára a udržiava Hodnotiteľ platformy. Pri danej certifikácii je však vývojár platformy kontaktným bodom pre Vývojára aplikácie.

Vývojár aplikácie sa obráti na vývojára platformy, aby doručil ETR_COMP kontaktnému bodu hodnotiteľa zloženého produktu. Vývojár platformy skontroluje svoje pravidlá riadenia dôvernosti (existencia príslušného NDA s laboratóriom a CB atď.), či je doručenie možné. V prípade potreby sa vývojár platformy obráti na certifikačný orgán platformy o zámere doručenia ETR_COMP.

Následne sa vývojár platformy spojí s hodnotiteľom platformy a požiada o doručenie (bezpečnou metódou a budú distribuované len označené verzie) ETR_COMP na dané kontaktné miesto hodnotiteľa zloženého produktu. Ak je súhlas udelený, buď hodnotiteľ platformy, alebo vývojár platformy pošle ETR_COMP hodnotiteľovi zloženého produktu v závislosti od dohôd medzi týmito dvoma stranami.

V závislosti od (zmluvnej) dohody medzi Vývojárom platformy a Hodnotiteľom platformy môžu existovať odchýlky od opísaného postupu dodania ETR_COMP Hodnotiteľovi zloženého produktu.

V prípade potreby si hodnotiteľ platformy a hodnotiteľ zloženého produktu vymenia podrobnejšie informácie. Toto je vždy pod kontrolou Vývojára platformy. V prípade objasnenia budú hlavnými stranami Hodnotiteľ platformy a Hodnotiteľ zloženého produktu. Ak sa vyžaduje dodatočné vyhlásenie o bezpečnostnej záruke, potom sa do výmeny zapojí aj certifikačný orgán platformy.

5.4 Obsah ETR pre zložené hodnotenie

[R23] Požadované informácie sú zamerané na:

1) Formálne informácie o platforme, ako je jej presná identifikácia, odkaz na správu o certifikácii atď.
2) Informácie o dizajne platformy.
3) Informácie o hodnotenej konfigurácii platformy.
4) Informácie o postupoch doručovania, zúčastnených miestach a výmene údajov.
5) Informácie o penetračnom testovaní platformy vrátane zvažovaných ciest útoku a zhrnutia výsledkov testov.
6) Informácie o penetračnom testovaní podporných funkcií platformy
7) Postrehy a odporúčania pre používateľov.

5.4.1 Formálne informácie

[R24] Táto časť ETR_COMP poskytuje formálne informácie o hodnotení platformy ako:

- identifikácia produktu,
- identitu žiadateľa a vývojára,
- totožnosť hodnotiaceho zariadenia a certifikačného orgánu,
- úroveň záruky z hodnotenia,
- formálne hodnotenie a výsledky certifikácie, ako napríklad vyhovel/nevyhovel,
- odkazy na ETR.

5.4.2 Návrh platformy

[R25] Táto časť ETR_COMP obsahuje opis IT produktu a jeho hlavných komponentov na vysokej úrovni na základe výsledkov požadovaných triedou záruk ADV Spoločných kritérií. Zámerom tejto časti je charakterizovať stupeň architektonického oddelenia hlavných komponentov a uviesť možné technické závislosti medzi platformou a aplikáciou, ktorá platformu používa (napr. závislosti medzi HW platformy a SW aplikácie). Táto časť musí obsahovať náčrt bezpečnostných mechanizmov platformy, na ktoré sa vzťahuje hodnotenie platformy.

5.4.3 Hodnotená konfigurácia

[R26] Táto časť ETR_COMP poskytuje informácie o hodnotenej konfigurácii platformy na základe zoznamu konfigurácie vývojára alebo príslušných častí podľa potreby alebo na základe jednotlivých prípadov. Platforma musí byť jednoznačne identifikovateľná a táto identifikácia musí zodpovedať hodnotenej konfigurácii, ako je uvedené v správe o certifikácii platformy.

[R27] V prípade potreby by sa mali vysvetliť nastavenia parametrov generovania a inštalácie, ktoré sú pre platformu bezpečnostne relevantné, a uviesť ich vplyv na obranu proti útokom (napr. dĺžka kľúča, limity počítadiel). Zahŕňa to metódy na overenie hodnôt týchto nastavení pre vývojára aplikácie a hodnotiteľa s cieľom overiť, či sa používa očakávaná hodnotená konfigurácia.

[R28] Tento dôkaz môže zahŕňať postupy inštalácie, generovania a spustenia TOE, ako je uvedené v AGD_PRE, aby sa zabezpečilo, že platforma je nakonfigurovaná bezpečným spôsobom.

5.4.4 Dodacie postupy, miesta a výmena údajov

[R29] Na podporu zloženého hodnotenia môžu byť potrebné dôkazy o hodnotení na dodanie platformy a postupy prijímania aplikácie a súvisiacich údajov, ktoré sa majú integrovať počas vývoja a výroby.

Preto môžu byť relevantné dôkazy o hodnotení AGD_PRE a ALC_DEL + AGD_PRE.

[R30] ETR_COMP poskytne prehľad pracovísk zapojených do vývoja a výroby platformy vrátane úlohy každého pracoviska a dátumu poslednej návštevy pracoviska.

[R31] Pre zložené hodnotenie OS na IC je potrebný opis fázy 1 a 4, ktoré budú podrobne opísané v tomto dokumente. Malo by sa zvážiť aj dodanie špecializovaného softvéru IC a usmernenie pre vývojára aplikácie. Okrem toho by sa mali určiť podrobnosti o ochrannom mechanizme fab-key.

V prípade integrovaného obvodu podľa prílohy 3, APLIKÁCIA CC NA INTEGROVANÉ OBVODY, sa uvažuje o týchto dodávkach:

1) dodanie kódu vstavanej aplikácie výrobcovi mikrokontroléra (v prípade produktov Flash môže byť nahradené dodaním kľúča od výrobcu mikrokontroléra vývojárovi vstavaného softvéru bezpečnostného integrovaného obvodu)
2) Dodanie mikrokontroléra subjektu zodpovednému za ďalší krok (testovanie, zabudovanie do mikromodulu, výroba karty).

V prípade operačného systému sa uvažuje o týchto dodávkach:

1) Dodanie vloženého aplikačného kódu výrobcovi (ak bude kód vložený v pamäti ROM) alebo

integrátorovi produktu (ak bude kód vložený v pamäti EEPROM alebo Flash).
2) Dodanie smart karty/platformy (IC so zabudovaným OS) zodpovednému subjektu v ďalšom kroku (integrátor produktu, personalizátor atď.)
3) Poskytovanie bezpečnostného poradenstva
4) Výmena kľúčového materiálu pre prístup k smart karte/platforme (IC s integrovaným OS).

5.4.5 Penetračné testovanie

[R32] V tejto časti ETR_COMP sa uvádzajú informácie o nezávislej analýze zraniteľnosti, ktorú vykonal hodnotiteľ platformy, pričom sa zohľadnili scenáre útoku, vykonalo sa testovanie prieniku a uviedol sa odkaz na príslušné hodnotenie (citáciu) potenciálu útoku (podľa prílohy 7] platného v čase certifikácie platformy).

[R33] Informácie o výsledkoch penetračného testovania by mali obsahovať:

- podrobnosti potrebné na pochopenie scenárov/ciest útoku
- hodnotenia výsledkov prieniku, ako aj zhrnutie preukazujúce, že počas analýzy zraniteľnosti boli zohľadnené všetky metódy útoku uvedené v prílohe 11.

Ak sa potenciálna zraniteľnosť musí riešiť dodržiavaním usmernení, musí to byť jasné zo zhrnutia vrátane odkazu na konkrétnu časť usmernení alebo, ak je to možné, na prvok usmernení.

[R34] Popisy scenárov útokov by mali poskytovať dostatočné podrobnosti, aby mohli hodnotitelia zložených produktov reprodukovať útoky, ktoré si vyžadujú dodatočné protiopatrenia v zloženom TOE.

[R35] V súlade s požiadavkami CEM sú tieto informácie k dispozícii v ETR. Môže sa teda zostaviť pre ETR_COMP.

[R36] V tejto časti sa uvádza aj hodnotenie prístupu k "otvoreným vzorkám" (t. j. verejné/obmedzené/citlivé/kritické). Použitie "otvorených vzoriek" sa musí zohľadniť pri hodnotení cesty útoku. Upozorňujeme, že "otvorené vzorky" sú hodnotiacimi nástrojmi, ale nepredstavujú TOE.

5.4.6 Pripomienky a odporúčania

[R37] Hodnotená dokumentácia s pokynmi pre používateľa musí obsahovať všetky informácie potrebné na bezpečné používanie TOE, ako je definované v bezpečnostnom zámere platformy, vrátane odporúčaní, ako sa vyhnúť zvyškovým zraniteľnostiam a neočakávanému správaniu. Odporúčania a dokumentácia s pokynmi pre používateľa musia byť konzistentné. Hodnotiteľ platformy overí, či ETR pre zloženie obsahuje len odporúčania týkajúce sa bezpečného používania, ktoré sú riešené aj ako požiadavky v pokynoch pre používateľov. Požiadavky na používateľské pokyny musia byť špecifické, čo umožní vývojárovi aplikácie vykonať analýzu zhody návrhu

[R38] V špecifických prípadoch však môžu byť okrem sprievodnej dokumentácie potrebné aj podrobné informácie, ako napríklad:

- Pripomienky k výsledkom hodnotenia (napr. špecifická konfigurácia TOE pre hodnotenie),
- Odporúčania/postupy pre hodnotiteľa zloženého produktu: špecifické informácie o použití výsledkov hodnotenia (napr. o špecifickom testovaní potrebnom počas hodnotenia zloženia).

Každá takáto pripomienka alebo odporúčanie/odporúčanie môže pochádzať od hodnotiteľa platformy a certifikačného orgánu platformy.

6 SPRÁVY Z HODNOTENIA/O CERTIFIKÁCII A PLATNOSŤ CERTIFIKÁTU PLATFORMY

[R39] Výsledky hodnotenia zloženia sa poskytnú certifikačnému orgánu pre zložené produkty vo forme technickej správy hodnotenia zloženého produktu. Táto ETR zloženého produktu musí okrem iného obsahovať konečný celkový verdikt zloženého hodnotenia na základe čiastkových verdiktov pre každý komponent záruk, ktorý je v rozsahu aktuálneho zloženého hodnotenia. V ETR zloženého produktu a v správe o certifikácii zloženého produktu musí byť odkaz na tento podporný dokument CC.

[R40] Keďže zložený certifikát produktu sa vzťahuje aj na platformu, platnosť zloženého certifikátu produktu je spojená s platnosťou certifikátu platformy.

[R41] Certifikačný orgán pre zložené produkty potrebuje aktuálny certifikát alebo posúdenie od certifikačného orgánu pre platformy o stave príslušného certifikátu platformy.

[R42] Certifikačný orgán pre zložené produkty spravidla požiada o opätovné posúdenie platformy, ak dátum ETR platformy pre zloženie je viac ako jeden a pol roka pred predložením správy obsahujúcej úplné výsledky skúšok prieniku zloženia. Toto opätovné posúdenie pozostáva buď z opätovného posúdenia platformy so zameraním na obnovenie analýzy zraniteľnosti (úloha dohľadu), alebo sa môže alternatívne vyžiadať potvrdzujúce vyhlásenie certifikačného orgánu platformy.

[R43] Upozorňujeme, že v prípade, že celý zložený produkt je vytvorený ako reťazec zložených produktov postavených nad sebou (napr. samotná platforma je už zloženým produktom), maximálna doba platnosti 18 mesiacov sa vzťahuje na najstarší ETR pre zloženie použité v tomto reťazci zložených produktov. Okrem toho je pri opätovnom použití výsledkov v zloženom hodnotení na vrchole potrebné zohľadniť závislosti z ETR pre zloženie nižšej úrovne na ETR pre zloženie vyššej úrovne.

[R44] Upozorňujeme tiež, že ak bol ETR pre zloženie platformy vydaný pred menej ako rokom a pol pred predložením príslušných úloh zloženého hodnotenia, ale došlo k významnej zmene v „state of the art“ pri vykonávaní príslušných útokov na platformu (napr. významná zmena v prílohe 7 – Uplatnenie potenciálu útoku na smart karty " alebo významná zmena v metódach útoku alebo hodnotení útoku), potom má orgán pre certifikáciu zložených produktov právo požadovať opätovné posúdenie so zameraním na novú metódu útoku.

[R45] Platnosť a relevantnosť certifikátu platformy pre aktuálnu zloženú certifikáciu produktu musí uznať orgán pre certifikáciu zložených produktov a zahŕňa určenie rovnocennosti jednotlivých komponentov záruk (a teda úrovní záruky) patriacich do rôznych verzií CC, ak certifikácia platformy bola podľa inej verzie CC, ako je aktuálna zložená certifikácia. Takúto rovnocennosť stanoví/uzná orgán pre certifikáciu zložených produktov.

[R46]Certifikačný orgán pre zložené produkty môže vydať bezpečnostný certifikát pre zložený produkt, ak:

- verdikty pre zložený produkt ETR sú PASS a
- Certifikačný orgán pre zložené produkty uznáva platnosť a aktuálnosť certifikátu platformy pre aktuálny zložený produkt.

[R47] Upozorňujeme, že ak hodnotiteľ zloženého produktu zistí niektoré chyby vyplývajúce z testovania platformy (napr. zraniteľnosti v dôsledku zlepšených metód alebo techník útoku), výsledky sa oznámia certifikačnému orgánu zloženého produktu. Orgán pre certifikáciu zloženého produktu potom spolu s orgánom pre certifikáciu platformy podnikne príslušné kroky, napr. vyvolá opätovné posúdenie alebo opätovnú certifikáciu TOE platformy.

[R48] Certifikačný orgán platformy pred vydaním správy o certifikácii overí, či sú odporúčania v ETR týkajúce sa zloženia platformy v súlade s požiadavkami uvedenými v príručke pre používateľa platformy. Ak sa zistia nezrovnalosti, certifikačný orgán platformy má možnosť doplniť do správy o certifikácii chýbajúce informácie pre vývojára aplikácie.

1DODATOK 1 ŠPECIFICKÉ POŽIADAVKY NA ZLOŽENIE

V nasledujúcom texte sú definované prvky činností vývojára a hodnotiteľa špecifické pre zloženie, ako aj činnosti hodnotiteľa (pracovné jednotky) patriace k činnostiam zloženia (pozri kapitolu 4 vyššie). Vyžadujú si prvky dôkazov uvedené v kapitole 4.7.

Cieľom týchto spresnení požiadaviek bezpečnostných záruk je poskytnúť hodnotiteľovi zloženého produktu a tvorcovi aplikácie presné usmernenie, ktoré relevantné aspekty sa musia opísať a posúdiť v kontexte hodnotenia zloženého produktu a úloh, ktoré sa majú vykonať.

Umožňuje certifikačnému orgánu pre zložené produkty skontrolovať pomocou ETR zloženého produktu, či boli požadované (povinné) úlohy riadne vykonané.

Všetky činnosti hodnotiteľa špecifické pre zloženie musia byť zdokumentované podľa pravidiel schémy a ukončené jedným z verdiktov PASS, FAIL alebo INCONCLUSIVE. Keďže tieto činnosti sú spresneniami tradičných činností zameraných na činnosti zloženia, tieto verdikty musia byť začlenené do celkového verdiktu.

Tento prístup možno uplatniť nezávisle od cieľového hodnotenia úrovne záruky (EAL) pre zložený produkt. Ak niektoré hodnotiace činnosti nie sú uplatniteľné vzhľadom na zvolenú EAL, nepredpokladá

sa ani uplatnenie súvisiacich úloh špecifických pre zloženie.

Kvôli pohodlnej identifikácii činností špecifických pre zloženie a súvisiacich pracovných jednotiek je každé spresnenie pomenované ako

*_COMP, kde * je názov triedy záruk, ku ktorej sa vzťahuje.

DODATOK 1.1 Zložené špecifické úlohy pre zložené hodnotenie v CC

Konzistentnosť bezpečnostného zámeru zloženého produktu (ASE_COMP)

Pracovné jednotky špecifické pre zloženie definované v tejto kapitole sú určené na začlenenie ako zdokonalenie hodnotiacich činností triedy ASE uvedených v nasledujúcej tabuľke. Ostatné činnosti triedy ASE si nevyžadujú pracovné jednotky špecifické pre zloženie.

CC skupina zabezpečenia	Hodnotiaca činnosť	Hodnotiaca pracovná jednotka	Pracovná jednotka špecifická pre zloženie
ASE_OBJ	ASE_OBJ.2.1C ASE_OBJ.2.1C ASE_OBJ.2.3C	ASE_OBJ.2-1 ASE_OBJ.2-3	ASE_COMP.1-5 ASE_COMP.1-6
ASE_REQ	ASE_REQ.1.6C ASE_REQ.2.9C ASE_REQ.1.6C ASE_REQ.2.9C ASE_REQ.2.8C ASE_REQ.2.3C	ASE_REQ.1-10 ASE_REQ.2-13 ASE_REQ.1-10 ASE_REQ.2-13 ASE_REQ.2-12 ASE_REQ.2-4	ASE_COMP.1-1 ASE_COMP.1-2 ASE_COMP.1-3 ASE_COMP.1-4

ASE_COMP.1 Konzistentnosť bezpečnostného zámeru

Cieľom tejto činnosti je určiť, či bezpečnostný zámer zloženého produktu[41] nie je v rozpore s bezpečnostným zámerom základnej platformy[42].

Aplikačné poznámky

Tieto aplikačné poznámky pomáhajú vývojárovi pri vytváraní, ako aj hodnotiteľovi pri analýze zloženého bezpečnostného zámeru a opisujú všeobecnú metodiku. Podrobné informácie/pokyny nájdete
v jednotlivých pracovných jednotkách uvedených nižšie.

Na vytvorenie zloženého bezpečnostného zámeru by mal vývojár vykonať nasledujúce kroky:

Krok 1: Vývojár sformuluje predbežný bezpečnostný zámer pre zložený produkt (Composite-ST) pomocou štandardného kódexu postupov. Composite-ST sa môže formulovať nezávisle od bezpečnostného cieľa základnej platformy (Platforma-ST) - prinajmenšom pokiaľ neexistujú formálne nároky na zhodu s PP.

Krok 2: Vývojár určí prekrývanie medzi Platforma-ST a Composite-ST prostredníctvom analýzy a porovnania ich bezpečnostných funkcionalít TOE (TSF)[43][44] 44:

[41] Ďalej len "Composite-ST".

[42] Ďalej len "Platforma-ST". Vo všeobecnosti bezpečnostný zámer vyjadruje bezpečnostnú politiku pre definovanú TOE.

[43] Pretože TSF presadzujú bezpečnostný zámer (spolu s organizačnými opatreniami presadzujúcimi bezpečnostné ciele pre prevádzkové prostredie TOE).

[44] Porovnanie sa vykonáva na úrovni abstrakcie SFR. Ak vývojár definoval skupiny bezpečnostných funkcionalít (TSF-groups) v časti TSS svojho bezpečnostného zámeru, hodnotiteľ by ich mal tiež zohľadniť, aby lepšie pochopil kontext bezpečnostných služieb ponúkaných TOE.

Krok 3: Vývojár určí, za akých podmienok môže dôverovať a spoliehať sa na platformu TSF, ktorú používa Composite-ST, bez nového skúmania.

Po vykonaní týchto krokov vývojár dokončí predbežný bezpečnostný zámer pre zložený produkt.

Nie je povinné, aby platforma a zložená TOE boli certifikované podľa rovnakej verzie CC. Dôvodom je skutočnosť, že aplikácia sa môže spoliehať na niektoré bezpečnostné služby platformy, ak (i) úroveň záruky platformy pokrýva zamýšľanú úroveň záruky zloženého TOE a (ii) bezpečnostný certifikát platformy je platný a aktuálny. Rovnocennosť jednotlivých komponentov záruk (a teda aj úrovní záruky), ktoré patria do rôznych verzií CC, stanoví/uzná certifikačný orgán pre zložený produkt, pozri kapitolu 6.

Ak sa deklaruje zhoda s PP (napr. zložený ST deklaruje zhodu s PP, ktorý deklaruje zhodu s hardvérovým PP), kontrola konzistentnosti sa môže obmedziť na prvky bezpečnostného zámeru, ktoré ešte neboli pokryté týmito ochrannými profilmi. Skutočnosť zhody s PP nie je dostatočná na to, aby sa zabránilo nekonzistentnosti. Predpokladajme, že

nasledujúca situácia, kde → znamená "vyhovuje"

Composite-ST → SW PP → HW PP → platforma-ST

SW PP môže vyžadovať akýkoľvek druh zhody[45] 45, ale to nemení "dodatočné prvky", ktoré

platforma-ST môže zaviesť do HW PP. Záverom možno konštatovať, že tieto doplnky nemusia byť v súlade s doplnkami Composite-ST/SW PP: Neexistuje žiadny scenár, ktorý by zabezpečil konzistenciu "by construction".

Všimnite si, že konzistentnosť nemusí byť priamou zhodou: napr. ciele pre prostredie platformy sa môžu stať cieľmi pre zloženú TOE.

Závislosti:

Žiadne závislosti.

Akčné prvky pre vývojárov:

ASE_COMP.1.1D

Vývojár poskytne vyhlásenie o kompatibilite medzi zloženým bezpečnostným zámerom a bezpečnostným zámerom platformy. Toto vyhlásenie sa môže poskytnúť v rámci zloženého bezpečnostného zámeru produktu.

Obsah a prezentácia prvkov dôkazov:

ASE_COMP.1.1C

Vo vyhlásení o kompatibilite sa opisuje rozdelenie platformy-TSF na príslušnú platformu-TSF, ktorú používa Composite-ST a iné.

ASE_COMP.1.2C

Vyhlásenie o kompatibilite medzi zloženým bezpečnostným zámerom a bezpečnostným zámerom platformy musí preukazovať (napr. vo forme mapovania), že bezpečnostné zámery zloženého produktu a základnej platformy sa zhodujú, t. j. že neexistuje konflikt medzi bezpečnostnými prostrediami, bezpečnostnými cieľmi a bezpečnostnými požiadavkami zloženého bezpečnostného zámeru a bezpečnostného zámeru platformy. Možno to zabezpečiť uvedením príslušných prvkov priamo v bezpečnostnom zámere pre zložený produkt, za ktorým v prípade potreby nasleduje vysvetľujúci text.

Akčné prvky hodnotiteľa:

ASE_COMP.1.1E

[45] napr. "prísne" alebo "preukázateľné" podľa CC.

Hodnotiteľ potvrdí, že poskytnuté informácie spĺňajú všetky požiadavky na obsah a prezentáciu dôkazov.

Činnosti hodnotiteľa:

Akcia ASE_COMP.1.1E

ASE_COMP.1.1C

ASE_COMP.1-1 Hodnotiteľ musí skontrolovať, či vyhlásenie o kompatibilite opisuje rozdelenie Platformy-TSF na príslušné Platformy-TSF, ktoré používa Composite-ST, a ostatné.

Všimnite si, že TSF znamená v CC V3 "TOE Bezpečnostná funkcionalita", pričom obsah TSF je zobrazovaný v SFR. V príslušnej súhrnnej špecifikácii TOE (TSS) sa pre každý SFR uvedie opis spôsobu, akým je každý SFR splnený[46]. Hodnotiteľ použije tento opis, aby pochopil kontextový rámec SFR.

Ak vývojár definoval skupiny bezpečnostných funkcionalít (TSF-groups) v časti TSS svojho bezpečnostného zámeru ako takýto kontextový rámec SFR, hodnotiteľ by ich mal tiež zohľadniť, aby lepšie pochopil kontext bezpečnostných služieb ponúkaných TOE.

Táto pracovná jednotka sa vzťahuje na krok 2 vyššie uvedených poznámok k aplikácii. Na určenie oblasti priesečníka hodnotiteľ považuje zoznam Platforma-SFR (uvedený v ST základnej platformy) za jednotlivé vlastnosti bezpečnostných služieb platformy.

Ako príklad uveďme, že existujú tieto platformy-SFR: Kryptografické operácie FCS_COP.1/RSA, FCS_COP.1/AES, FCS_COP.1/EC, ako aj odolnosť voči neoprávnenej manipulácii FPT_PHP.3 a obmedzené možnosti a dostupnosť FMT_LIM.1 a FMT_LIM.2[47].

Tieto platformy-SFR sú rozdelené do troch skupín:

- IP_SFR: irelevantné Platforma-SFR, ktoré sa nepoužívajú v Composite-ST.
- RP_SFR-SERV: Príslušné platformy-SFR, ktoré používa Composite-ST na implementáciu bezpečnostnej služby s pridruženou TSFI.
- RP_SFR-MECH: Relevantné Platforma-SFR, ktoré používa Composite-ST kvôli svojim bezpečnostným vlastnostiam poskytujúcim ochranu pred útokmi na TOE ako celok a sú riešené v ADV_ARC. Tieto požadované bezpečnostné vlastnosti sú výsledkom bezpečnostných mechanizmov a služieb, ktoré sú implementované v Platforma TOE.

Druhá a tretia skupina RP_SFR-SERV a RP_SFR-MECH presne zobrazujú danú oblasť križovatky. Napríklad IP_SFR = {FCS_COP.1/AES}, RP_SFR-SERV= {FCS_COP.1/RSA, FCS_COP.1/EC} a RP_SFR-

MECH = { FPT_PHP.3, FMT_LIM.1, FMT_LIM.2}, t. j. AES sa v zloženom TOE nepoužíva, ale používajú sa všetky ostatné SFR platformy. RP_SFR-MECH však nemôže byť priamo pripojený k SFR v zloženom TOE.

Veľkosť prekrývajúcej sa oblasti (t. j. obsah skupiny RP_SFR-SERV a RP_SFR-MECH) vyplýva z konkrétnych vlastností Platforma-ST a Composite-ST. Ak Composite-ST nevyužíva žiadnu vlastnosť Platforma-ST, a teda oblasť prieniku je prázdna množina (RP_SFR-MECH ∪ RP_SFR-SERV) = {∅}), nie sú vôbec potrebné ďalšie činnosti zloženého hodnotenia: V takom prípade existuje technické, ale nie bezpečnostné zloženie.

Výsledok tejto pracovnej jednotky sa integruje do výsledku ASE_REQ.1.6C/ ASE_REQ.1-10 (alebo ekvivalentných vyšších komponentov, ak je zvolená vyššia úroveň záruky) a ASE_REQ.2.9C/ ASE_REQ.2-13.

ASE_COMP.1-2 Hodnotiteľ preskúma vyhlásenie o kompatibilite, aby určil, či je platforma-TSF, ktorú používa Composite-ST, úplná a konzistentná pre aktuálnu zložený TOE.

S cieľom určiť úplnosť zoznamu platformy-TSF, ktorú používa zložený systém-ST, hodnotiteľ overí, či:

- Platforma-SFR = IP_SFR ∪ RP_SFR-SERV ∪ RP-SFR-MECH
- Prvky, ktoré patria do RP_SFR-SERV a RP-SFR-MECH, sa zohľadňujú počas hodnotenia

[46] Porovnaj CC časť 3, ASE_TSS.1.1C.

[47] FMT_LIM.1 a FMT_LIM.2 sa nachádzajú v dokumente BSI-CC-PP-0084-2014, Security IC Platform Protection Profile with Augmentation Packages.

zloženého TOE. IP-SFR sú samozrejme súčasťou Platformy-TOE, ale počas hodnotenia zloženej TOE sa neberú do úvahy.

S cieľom určiť konzistentnosť zoznamu Platforma-TSF, ktorý používa Composite-ST, hodnotiteľ overí, či v ňom nie sú nejednoznačné a protichodné vyhlásenia.

Podrobnejšie informácie o analýze konzistentnosti nájdete v spoločných dokumentoch CC.

Výsledok tejto pracovnej jednotky sa integruje do výsledku ASE_REQ.1.6C/ ASE_REQ.1-10 (alebo ekvivalentných vyšších komponentov, ak je zvolená vyššia úroveň záruky) a ASE_REQ.2.9C/ ASE_REQ.2-13.

ASE_COMP.1.2C

ASE_COMP.1-3 Hodnotiteľ musí skontrolovať, či požiadavky bezpečnostných záruk zloženého hodnotenia predstavujú podmnožinu požiadaviek bezpečnostných záruk základnej platformy.

Táto pracovná jednotka sa vzťahuje na krok 2 vyššie uvedených poznámok k aplikácii. S cieľom zabezpečiť dostatočný stupeň dôveryhodnosti platformy-TSF hodnotiteľ porovnáva požiadavky bezpečnostných záruk TOE (SAR) zloženého hodnotenia s požiadavkami základnej platformy. Hodnotiteľ rozhodne, že stupeň dôveryhodnosti Platformy-TSF je dostatočný, ak zložené-SAR predstavujú podmnožinu Platformy-SAR:

Platforma-SAR ⊇ Composite-SAR,

napr. EAL zvolené pre zložené hodnotenie nepresahuje EAL použité na hodnotenie platformy. Výsledok tejto pracovnej jednotky sa integruje do výsledku ASE_REQ.2.8C/ ASE_REQ.2-12.

ASE_COMP.1-4 Hodnotiteľ preskúma vyhlásenie o kompatibilite s cieľom určiť, či sú všetky vykonávané operácie na príslušných požiadavkách bezpečnostných funkcionalít TOE platformy vhodné pre Composite-ST.

Táto pracovná jednotka sa vzťahuje na krok 3 vyššie uvedených poznámok k aplikácii. Príslušné požiadavky bezpečnostných funkcionalít TOE platformy zahŕňajú aspoň prvky skupiny RP_SFR-SERV (pozri pracovnú jednotku ASE_COMP.1-1), ale ako príslušné požiadavky bezpečnostných funkcionalít TOE sa môže uviesť aj RP-SFR-MECH. Nerelevantné požiadavky bezpečnostných funkcionalít TOE patria do skupiny IP_SFR.

Na vykonanie tejto pracovnej jednotky hodnotiteľ porovnáva jednotlivé parametre príslušných SFR platformy s parametrami zloženého hodnotenia. Napríklad vyhodnocovateľ porovnáva vlastnosti príslušných komponentov FCS_COP.1/RSA a určuje, že Composite-ST vyžaduje dĺžku kľúča 2048 bitov a platforma-ST presadzuje funkciu RSA s dĺžkou kľúča 1024 a 2048 bitov, t. j. tento parameter platformy je vhodný pre Composite-ST. Upozorňujeme, že Composite-SFR nemusia byť nevyhnutne rovnaké ako Platforma-SFR, napr. dôveryhodný kanál (FTP_ITC.1) v zloženom produkte môže byť vytvorený pomocou implementácie RSA (FCS_COP.1/RSA) platformy.

Výsledok tejto pracovnej jednotky sa integruje do výsledku ASE_REQ.2.3C/ ASE_REQ.2-4.

ASE_COMP.1-5 Hodnotiteľ preskúma vyhlásenie o kompatibilite s cieľom určiť, či príslušné bezpečnostné ciele TOE platformy-ST nie sú v rozpore s cieľmi Composite-ST.

Táto pracovná jednotka sa vzťahuje na krok 3 vyššie uvedených poznámok k aplikácii. Príslušné bezpečnostné ciele TOE platformy-ST sú tie, ktoré sú priradené k príslušným SFR platformy-ST (pozri pracovnú jednotku ASE_COMP.1-1).

Na vykonanie tejto pracovnej jednotky hodnotiteľ porovná príslušné bezpečnostné ciele TOE platformy-ST s cieľmi Composite-ST a určí, či nie sú v rozpore.

Výsledok tejto pracovnej jednotky sa integruje do výsledku ASE_OBJ.2.1C/ ASE_OBJ.2-1.

ASE_COMP.1-6 Hodnotiteľ preskúma vyhlásenie o kompatibilite, aby určil, či významné bezpečnostné ciele pre operačné prostredia platformy-ST nie sú v rozpore s cieľmi Composite-ST.

Táto pracovná jednotka sa vzťahuje na krok 3 vyššie uvedených poznámok k aplikácii. S cieľom určiť, ktoré predpoklady Platformy-ST sú významné pre Composite-ST, hodnotiteľ analyzuje ciele pre prostredie Platformy-ST a ich rozdelenie do nasledujúcich skupín:

- IrOE: Ciele pre prostredie, ktoré nie sú relevantné pre Composite-ST, napr. ciele pre prostredie týkajúce sa vývojovej a výrobnej fázy platformy.

- CfPOE: Ciele pre prostredie, ktoré sa plnia automaticky pomocou Composite-ST. Takéto ciele prostredia Platformy-ST možno vždy priradiť k bezpečnostným cieľom TOE Composite-ST. Vďaka tejto skutočnosti ich bude plniť buď Composite-SFR, alebo Composite- SAR automaticky. Ako príklad uveďme cieľ pre prostredie OE.Resp-Appl Platformy-ST: "Všetky údaje používateľa sú vo vlastníctve vstavaného softvéru smart karty. Preto sa musí predpokladať, že s bezpečnostne relevantnými údajmi používateľa (najmä kryptografickými kľúčmi) zaobchádza Smartcard Embedded Software tak, ako je to definované pre špecifický kontext aplikácie." a bezpečnostný cieľ TOE OT. Key_Secrecy Composite-ST: "Tajomstvo súkromného kľúča podpisu používaného na generovanie podpisu je primerane zabezpečené proti útokom s vysokým potenciálom útoku. Ak je súkromný kľúč jediným citlivým dátovým prvkom, potom je cieľ pre prostredie OE.Resp-Appl automaticky pokrytý bezpečnostným cieľom TOE OT.Key_Secrecy.
- SgOE: Zostávajúce ciele pre životné prostredie platformy-ST, ktoré nepatria ani do skupiny IrOE, ani do skupiny CfOE Presne táto skupina tvorí významné ciele pre životné prostredie pre zloženú platformu-ST, ktoré sa budú riešiť v zloženej platforme-ST.

Na vykonanie tejto pracovnej jednotky hodnotiteľ porovnáva významné bezpečnostné ciele pre operačné prostredie platformy-ST s cieľmi Composite-ST a určuje, či nie sú v rozpore. V prípade potreby sa významné bezpečnostné ciele pre operačné prostredie platformy-ST zahrnú do Composite-ST vrátane súvisiacich predpokladov, z ktorých sa ciele pre prostredie odvodzujú. Zahrnutie nie je potrebné, ak Composite-ST už obsahuje rovnocenné (alebo podobné) bezpečnostné ciele (pokrývajúce všetky relevantné aspekty) a predpoklady.

Keďže bezpečnostná záruka rozvojového a výrobného prostredia platformy sa potvrdzuje certifikátom platformy, príslušné ciele platformy, ak existujú, patria do skupiny IrOE

Bezpečnostná záruka rozvojového a výrobného prostredia je zvyčajne úplne riešená triedou záruk ALC, a preto si nevyžaduje žiadny explicitný bezpečnostný cieľ.

Výsledok tejto pracovnej jednotky sa integruje do výsledku ASE_OBJ.2.1C/ ASE_OBJ.2-1 a ASE_OBJ.2.3C/ ASE_OBJ.2-3.

Integrácia častí zloženia a kontrola konzistentnosti postupov dodania (ALC_COMP)

Pracovné jednotky špecifické pre zloženie definované v tejto kapitole sú určené na integráciu ako zdokonalenie hodnotiacich činností triedy ALC uvedených v nasledujúcej tabuľke. Ostatné činnosti triedy ALC si nevyžadujú pracovné jednotky špecifické pre zloženie.

CC skupina záruk	Hodnotiaca činnosť	Hodnotiaca pracovná jednotka	Pracovná jednotka špecifická pre zloženie
ALC_CMS	ALC_CMS.1.2C	ALC_CMS.1-2	ALC_COMP.1-1
AGD_PRE	AGD_PRE.1.1C	AGD_PRE.1-1	ALC_COMP.1-2
ALC_CMC	ALC_CMC.4.8C	ALC_CMC.4-10	ALC_CMC.4-10

Poznámka: Ak je úroveň zvolenej požiadavky bezpečnostnej záruky vyššia ako tie, ktoré sú uvedené v tejto tabuľke, platí aj pracovná jednotka špecifická pre zloženie.

ALC_COMP.1 Integrácia aplikácie do základnej platformy a kontrola konzistentnosti postupov dodania a prijatia

Ciele

Cieľom tejto činnosti je zistiť, či

- správna verzia aplikácie je nainštalovaná na správnu verziu základnej platformy a
- postupy prípravného vedenia vývojárov platforiem a aplikácií sú kompatibilné s postupom prijímania integrátora zložených produktov.

Závislosti:

Žiadne závislosti.

Akčné prvky pre vývojárov:

ALC_COMP.1.1D

Vývojár poskytne dôkaz o konfigurácii komponentov; pozri bod č. 7, bod č. 8 a bod č. 3 v tabuľke 1, oddiel 4.7.

Obsah a prezentácia prvkov dôkazov:

ALC_COMP.1.1C

Dôkazy o konfigurácii komponentov musia preukazovať, že hodnotená verzia aplikácie bola nainštalovaná na certifikovanú verziu základnej platformy alebo do nej bola vložená.

ALC_COMP.1.2C

Dôkazy o konfigurácii komponentov preukazujú, že:

i. Dôkazy o kompatibilite dodávok a akceptácie musia preukazovať, že postupy dodávok vývojárov platforiem a aplikácií sú kompatibilné s postupom akceptácie integrátora zloženého produktu.
ii. dôkazy preukazujú, že postupy prípravného vedenia predpísané vývojármi platformy a aplikácií sú buď skutočne používané integrátorom zloženého produktu, alebo sú kompatibilné s vedením integrátora zloženého produktu a nie sú vo vzájomnom rozpore

Akčné prvky hodnotiteľa:

ALC_COMP.1.1E

Hodnotiteľ potvrdí, že poskytnuté informácie spĺňajú všetky požiadavky na obsah a prezentáciu dôkazov.

ALC_COMP.1.2E

Hodnotiteľ potvrdí, že dôkazy o zlučiteľnosti dodávok sú úplné, koherentné a vnútorne konzistentné.

Činnosti hodnotiteľa:

Akcia ALC_COMP.1.1E

ALC_COMP.1-1 Hodnotiteľ preskúma dôkaz, že hodnotená verzia aplikácie bola nainštalovaná na správnu certifikovanú verziu základnej platformy.

Dokumentácia AGD_PRE platformy, ktorú poskytuje vývojár platformy, obsahuje požiadavky na bezpečné prijatie platformy a bezpečnostné opatrenia, ktoré musí vývojár aplikácie alebo zložený integrátor produktu dodržiavať. Vývojár aplikácie musí poskytnúť dôkazy o tom, že (ak je to uplatniteľné), tieto požiadavky sú dodržané a požadované bezpečnostné opatrenia sú implementované.

Osobitnou činnosťou hodnotiteľa zloženého produktu je kontrola dôkazov o správnosti verzie pre obe časti zloženého produktu a o tom, že bola vykonaná bezpečná akceptácia a inštalácia platformy.

V prípade základnej platformy hodnotiteľ určí, či skutočná identifikácia platformy zodpovedá príslušným údajom v certifikáte platformy v rámci sledovania postupov uvedených v AGD_PRE platformy.

Pre aplikáciu je príslušná úloha triviálna vzhľadom na skutočnosť, že hodnotiteľ zloženého produktu musí túto úlohu vykonať v kontexte skupiny záruk ALC_CMS.

Dôkazy o identifikácii komponentov možno poskytnúť dvoma rôznymi spôsobmi: technickým a organizačným. Technický dôkaz správnosti verzie vytvára samotný zložený produkt: platforma a aplikácia vracajú - v každom prípade - reťazce obsahujúce jednoznačné čísla verzií ako odpovede na príslušné príkazy.

Môže to byť napr. návratový reťazec príkazu alebo kópia informácií systému Windows (napr. "About"); v prípade smart kariet to môže byť príslušný ATR.

Technický dôkaz správnosti verzie hardvéru možno v prípade potreby poskytnúť aj odčítaním jednoznačného nápisu na jeho povrchu. Všimnite si, že na väčšine mikrokontrolérov smart kariet

neexistuje žiadna fyzická indikácia.

Odporúča sa predložiť technické dôkazy.

Organizačný dôkaz o správnosti verzie vytvára integrátor zloženého produktu na základe svojich konfiguračných zoznamov obsahujúcich jednoznačné informácie o verzii platformy a aplikácie, ktoré boli zložené do konečného zloženého produktu.

Napríklad v prípade smart kariet to môže byť potvrdenie (napr. konfiguračný zoznam) výrobcu integrovaného obvodu[48] výrobcovi vstavaného softvéru[49], ktoré obsahuje dôkazy o verziách čipu, vstavaného softvéru a jeho parametroch pred personalizáciou[50].

Organizačné dôkazy sú vždy možné, a preto sa poskytnú.

Výsledok tejto pracovnej jednotky sa integruje do výsledku ALC_CMS1.1C/ ALC_CMS.1-2 (alebo ekvivalentných vyšších komponentov, ak je zvolená vyššia úroveň záruky).

ALC_COMP.1-2 Hodnotiteľ preskúma postup prijímania Integrátora zloženého produktu, postupy dodávania Vývojára aplikácie a Vývojára platformy, aby sa presvedčil, či sú kompatibilné a či ich v prípade potreby buď uplatňuje Integrátor zloženého produktu, alebo sú predpísané v prípravnom usmernení. .

Všeobecné informácie o požiadavkách na prípravné vedenie, ktoré okrem iného zahŕňajú konfiguračné parametre, sú zastúpené a musia sa preskúmať v kontexte skupiny záruk AGD_PRE [1.2C]. Osobitnou činnosťou hodnotiteľa je preskúmať dôkazy vývojára a rozhodnúť, či integrátor zloženého produktu vhodne zaobchádza s touto osobitnou podmnožinou požiadaviek na prípravné usmernenie.

Hodnotiteľ musí preskúmať tieto poskytnuté dôkazy, ktoré zahŕňajú kontrolu, či sú postupy dodávok vývojárov platforiem a aplikácií v súlade s postupom prijímania integrátora zloženého produktu.

V prípadoch, keď integrátor zloženého produktu ponechá požiadavky na prípravné pokyny predpísané vývojárom platformy a vývojárom aplikácie na používateľa, hodnotiteľ zloženého produktu overí, či sú tieto požiadavky uvedené v prípravných pokynoch zloženého hodnotenia.

Napríklad v prípade karty Java Card ako zloženého TOE musí vydavateľ karty pri inštalácii appletu na platformu karty Java Card nastaviť všetky parametre, ktoré predpísala platforma Java Card a vývojári appletu; pozri tabuľku 3, časť

4.7. A tiež overte, či je balík overený bajtovým kódom a má platný digitálny podpis.

Výsledok tejto pracovnej jednotky sa integruje do výsledku AGD_PRE.1.2C/AGD_PRE.1-4 a ALC_CMC.4.8C/ ALC_CMC.4-10.

Zhoda zloženého návrhu (ADV_COMP)

Pracovné jednotky špecifické pre zloženie definované v tejto kapitole sú určené na začlenenie ako zdokonalenie hodnotiacich činností triedy ADV uvedených v nasledujúcej tabuľke. Ostatné činnosti triedy ADV si nevyžadujú pracovné jednotky špecifické pre zloženie.

CC skupina záruk	Hodnotiaca činnosť	Hodnotiaca pracovná jednotka	Pracovná jednotka špecifická pre zloženie
ADV_ARC	ADV_ARC.1.1E	ADV_ARC.1.1C/ ADV_ARC.1-1	ADV_COMP.1-1
ADV_IMP	ADV_IMP.1.1E	ADV_IMP.1.1C/ ADV_IMP.1-1	ADV_COMP.1-1
ADV_TDS	ADV_TDS.1.2E	ADV_TDS.1-7	ADV_COMP.1-1

[48] -> základná platforma

[49] -> aplikácia

[50] Akékoľvek údaje dodané výrobcom vstavaného softvéru, ktoré výrobca integrovaných obvodov vloží do nevolatilnej pamäte. Tieto údaje sa používajú napríklad na sledovateľnosť a/alebo na zabezpečenie prepravy medzi jednotlivými fázami (pozri [Smartcard IC Platform Protection Profile with augmentation packages (Ochranný profil platformy smart kariet s rozširujúcimi balíkmi), verzia 1.0, január 2014, registračné číslo BSI PP 084-2014], odd. 7.7).

Poznámka: Ak je úroveň zvolenej požiadavky bezpečnostnej záruky vyššia ako tie, ktoré sú uvedené v tejto tabuľke, platí aj pracovná jednotka špecifická pre zloženie.

ADV_COMP.1 Súlad návrhu so správou o certifikácii platformy, usmerneniami a cieľmi ETR_COMP

Cieľom tejto činnosti je určiť, či sú požiadavky na aplikáciu, ktoré kladie základná platforma, splnené v zloženom produkte.

Aplikačné poznámky

Požiadavky na aplikáciu, ktoré kladie základná platforma, môžu byť formulované v príslušnej správe o certifikácii (napr. vo forme obmedzení a odporúčaní), návode pre používateľa a ETR_COMP (vo forme pripomienok a odporúčaní) pre platformu. Vývojár zloženého produktu musí zohľadniť každý z týchto zdrojov, ak je k dispozícii (pozri tabuľku 2, oddiel 4.7), a implementovať zložený produkt tak, aby boli splnené príslušné požiadavky.

TSF zloženého produktu je zobrazovaný na rôznych úrovniach abstrakcie v skupinách vývojovej triedy ADV. Skúsenostne sú vhodnými úrovňami zobrazenia návrhu na skúmanie, či sú požiadavky platformy splnené zloženým produktom, návrh TOE (ADV_TDS), bezpečnostná architektúra (ADV_ARC) a implementácia (ADV_IMP). V prípade, že tieto úrovne zobrazenia návrhu nie sú k dispozícii (napr. z dôvodu, že zvolený balík záruky je EAL1), táto činnosť sa neuplatňuje (dôvod pozri v nasledujúcom odseku).

Vzhľadom na definíciu zloženého TOE (pozri oddiel 2.1 "Definície") je rozhranie medzi základnou platformou a aplikáciou interné, preto funkčná špecifikácia (ADV_FSP) ako úroveň zobrazenia nie je vhodná na analýzu zhody návrhu.

Bezpečnostná architektúra ADV_ARC ako skupina záruk je určená na zabezpečenie správneho fungovania integračných bezpečnostných služieb, ako je oddelenie domén, vlastná ochrana a nepriechodnosť. Nie je možné a ani nie je zmyslom zloženého hodnotenia nahliadnuť do architektonických vnútorností základnej platformy (je to záležitosť hodnotenia platformy). Zložený hodnotiteľ musí v kontexte ADV_ARC urobiť nasledovné

(i) určiť, či aplikácia využíva služby základnej platformy v rámci vlastného Composite-ST na zabezpečenie oddelenia domény, vlastnej ochrany, neobchádzateľnosti a chráneného spustenia; ak nie, pre ADV_ARC sa nevykonávajú žiadne ďalšie zložené činnosti; ak áno, potom

(ii) hodnotiteľ musí určiť, či aplikácia využíva tieto služby platformy vhodným/bezpečným spôsobom (pozri pokyny pre používateľov platformy, pozri bod č. 3 v tabuľke 1, časť 4.7).

Keďže konzistentnosť bezpečnostnej politiky zloženého produktu sa už zvažovala v kontexte bezpečnostného cieľa v skupine záruk ASE_COMP (pozri stranu 31 vyššie), nie je potrebné zvažovať nekontradiktórnosť modelu bezpečnostnej politiky (ADV_SPM) zloženého TOE a modelu bezpečnostnej politiky základnej platformy.

Závislosti:

Žiadne závislosti.

Akčné prvky pre vývojárov:

ADV_COMP.1.1D

Investor poskytne odôvodnenie súladu návrhu; pozri bod č. 6, ako aj body č. 3, 4 a 5 v tabuľke 1, oddiel 4.7.

Obsah a prezentácia prvkov dôkazov:

ADV_COMP.1.1C

Odôvodnenie zhody návrhu musí obsahovať zdôvodnenie zhody návrhu - na primeranej úrovni znázornenia - toho, ako sú požiadavky na aplikáciu uložené základnou platformou splnené v zloženom produkte.

Akčné prvky hodnotiteľa:

ADV_COMP.1.1E

Hodnotiteľ potvrdí, že odôvodnenie súladu návrhu je úplné, koherentné a vnútorne konzistentné.

Činnosti hodnotiteľa:

Opatrenie ADV_COMP.1.1E

ADV_COMP.1-1 Hodnotiteľ preskúma zdôvodnenie zhody návrhu s cieľom určiť, či zložený produkt spĺňa všetky uplatniteľné požiadavky na aplikáciu, ktoré kladie základná platforma.

Na vykonanie tejto pracovnej jednotky hodnotiteľ použije zdôvodnenie zhody návrhu, ako aj zastúpenie TSF na úrovniach ADV_TDS, ADV_ARC a ADV_IMP na jednej strane a vstupy vývojára platformy vo forme správe o certifikácii, usmernenia a ETR_COMP na strane druhej. Hodnotiteľ analyzuje, ktoré požiadavky platformy sú uplatniteľné na súčasný zložený produkt na základe identifikovaných RP-SFR-MECH a RP-SFR-SERV. Hodnotiteľ porovná každú z uplatniteľných požiadaviek so skutočnou špecifikáciou a/alebo implementáciou zloženého produktu a pre každú požiadavku určí, či je splnená. Výsledkom je, že hodnotiteľ potvrdí alebo vyvráti odôvodnenie zhody návrhu.

Napríklad navádzanie platformy môže vyžadovať, aby aplikácia vykonala špeciálnu spúšťaciu sekvenciu, ktorá testuje aktuálny stav platformy a inicializuje jej mechanizmy vlastnej ochrany. Takéto informácie sa môžu nachádzať v opise bezpečnej architektúry ADV_ARC zloženého TOE; pozri aj vyššie uvedenú aplikačnú poznámku.

Druhý príklad, usmernenie platformy môže vyžadovať, aby aplikácia vykonala kontrolu DFA operácie DES, zatiaľ čo aplikácia implementuje BAC v MRTD elektronického pasu [PP-0055[51]]. V ADV_ARC sa vysvetlí, či sa usmernenie platformy dodržiava alebo nie, a v prípade, že sa požiadavky v usmernení platformy nedodržiavajú, uvedie sa príslušné odôvodnenie. Argumenty vývojára vysvetľujú, prečo nedodržanie požiadaviek nezavedie zraniteľnosti.

Príslušnú úroveň zobrazenia (ADV_TDS, ADV_ARC a/alebo ADV_IMP), na ktorej sa analýza vykonáva, možno vybrať a kombinovať flexibilne v závislosti od konkrétneho zloženého TOE a danej požiadavky.

V prípade, že nie je samoúčelné, hodnotiteľ zdôvodní, prečo je zvolená úroveň zastúpenia vhodná.

Činnosti hodnotiteľa v rámci tejto pracovnej jednotky môžu byť rozložené na rôzne jednotlivé aspekty hodnotenia (napr. na ADV_TDS a ADV_IMP). V takom prípade hodnotiteľ vykonáva čiastkovú činnosť v kontexte príslušného jednotného hodnotiaceho aspektu. Potom je zápis tejto pracovnej jednotky ADV_COMP.1-1-TDS, ADV_COMP.1-1-ARC a ADV_COMP.1-1-IMP, resp.

Ak zvolený balík záruky neobsahuje skupiny ADV_TDS, ADV_ARC alebo ADV_IMP (napr. EAL1), táto pracovná jednotka sa nepoužije (pozri poznámku k aplikácii vyššie).

Výsledok tejto pracovnej jednotky sa integruje do výsledku ADV_TDS.1-2E/ ADV_TDS.1-7, ADV_ARC.1.1E/ ADV_ARC.1.1C/ ADV_ARC.1-1, ADV_IMP.1.1E/ ADV_IMP.1.1C/ ADV_IMP.1-1 (alebo ekvivalentných vyšších komponentov, ak je zvolená vyššia úroveň záruky).

Zložené funkčné skúšanie (ATE_COMP)

Pracovné jednotky špecifické pre zloženie definované v tejto kapitole sú určené na začlenenie ako zdokonalenie hodnotiacich činností triedy ATE uvedených v nasledujúcej tabuľke. Ostatné činnosti triedy ATE si nevyžadujú pracovné jednotky špecifické pre zloženie.

CC skupina záruk	Hodnotiaca činnosť	Hodnotiaca pracovná jednotka	Pracovná jednotka špecifická pre zloženie
ATE_COV	ATE_COV.1.1C	ATE_COV.1-1	ATE_COMP.1-1
ATE_FUN	ATE_FUN.1.2C	ATE_FUN.1-3	ATE_COMP.1-1

[51] Strojovo čitateľný cestovný doklad s aplikáciou ICAO, základná kontrola prístupu.

Poznámka: Ak je úroveň zvolenej požiadavky bezpečnostnej záruky vyššia ako tie, ktoré sú uvedené v tejto tabuľke, platí aj pracovná jednotka špecifická pre zloženie.

ATE_COMP.1 Skúšanie funkcionality zloženého produktu

Ciele

Cieľom tejto činnosti je určiť, či zložený produkt ako celok vykazuje vlastnosti potrebné na splnenie požiadaviek funkcionalít jeho bezpečnostného zámeru.

Aplikačné poznámky

Zložený produkt sa môže testovať samostatne a integračne. Samostatné testovanie znamená, že platforma a aplikácia sa testujú nezávisle od seba. V rámci dosiahnutého hodnotenia sa mohlo vykonať veľa testov platformy. Aplikácia sa môže testovať na simulátore alebo emulátore, ktoré predstavujú virtuálny stroj.

Integračné testovanie znamená, že sa testuje zložený produkt v jeho súčasnej podobe: aplikácia beží na platforme.

Správanie implementácie niektorých SFR môže závisieť od vlastností základnej platformy, ako aj aplikácie (napr. správnosť opatrení zloženého produktu na odolanie útoku bočným kanálom alebo správnosť implementácie odolnosti proti manipulácii proti fyzickým útokom). V takom prípade sa implementácia SFR testuje na konečnom zloženom produkte, ale nie na simulátore alebo emulátore.

Táto činnosť sa zameriava výlučne na testovanie zloženého produktu ako celku a predstavuje len čiastkové úsilie v rámci všeobecného prístupu k testovaniu, na ktorý sa vzťahuje bezpečnostná záruka ATE. Tieto integračné skúšky sa špecifikujú a vykonávajú, pričom sa uplatňuje prístup štandardných skupín záruk triedy ATE.

- Správne správanie Platforma-TSF, ktoré je relevantné pre Composite-ST (zodpovedá skupine RP_SFR- SERV a RP-SFR-MECH v pracovnej jednotke ADV_COMP.1-1 vyššie), a - neprítomnosť zneužiteľných zraniteľností (dostatočná efektívnosť) v kontexte Platforma-ST sú potvrdené platným certifikátom platformy, pozri kapitolu 6 vyššie.

Závislosti:

Žiadne závislosti.

Akčné prvky pre vývojárov:

ATE_COMP.1.1D

Vývojár poskytne súbor testov podľa požiadaviek vybraného balíka záruky. ATE_COMP.1.2D

Vývojár poskytne zložený TOE na skúšanie.

Obsah a prezentácia prvkov dôkazov:

ATE_COMP.1.1C

Obsah a prezentácia špecifikácie a dokumentácie integračných testov musia zodpovedať štandardným požiadavkám skupín záruk ATE_FUN a ATE_COV.

ATE_COMP.1.2C

Dodaný zložený TOE musí byť vhodný na skúšanie.

Akčné prvky hodnotiteľa:

ATE_COMP.1.1E

Hodnotiteľ potvrdí, že poskytnuté informácie spĺňajú všetky požiadavky na obsah a prezentáciu dôkazov.

Činnosti hodnotiteľa:

Akcia ATE_COMP.1.1E

ATE_COMP.1-1 Hodnotiteľ preskúma, či vývojár vykonal integračné skúšky pre všetky SFR, ktoré sa majú skúšať na zloženom produkte ako celku.

Na vykonanie tejto pracovnej jednotky hodnotiteľ pre každý SFR analyzuje, či priamo závisí od bezpečnostných vlastností platformy a aplikácie. Potom hodnotiteľ overí, či integračné testy vykonané vývojárom pokrývajú aspoň všetky takéto SFR.

Ak zvolený balík záruky neobsahuje skupinu ATE_FUN a ATE_COV (napr. EAL1), táto pracovná jednotka sa nepoužije.

Výsledok tejto pracovnej jednotky sa integruje do výsledku ATE_COV.1-1C/ ATE_COV.1-1 a ATE_FUN.1.2C/ ATE_FUN.1-3 (alebo ekvivalentných vyšších komponentov, ak je zvolená vyššia úroveň záruky).

Zložené hodnotenie zraniteľnosti (AVA_COMP)

Pracovné jednotky špecifické pre jednotlivé zloženia definované v tejto kapitole sú určené na začlenenie do hodnotiacich činností triedy AVA uvedených v nasledujúcej tabuľke. Ostatné činnosti triedy AVA si nevyžadujú pracovné jednotky špecifické pre zloženie.

CC Skupina záruk	Hodnotiaca činnosť	Hodnotiaca pracovná jednotka	Pracovná jednotka špecifická pre zloženie
AVA_VAN	AVA_VAN.1.3E	AVA_VAN.1-5 AVA_VAN.1-6 AVA_VAN.1-7 AVA_VAN.1-8	AVA_COMP.1-1 AVA_COMP.1-2

Poznámka: Ak je úroveň zvolenej požiadavky bezpečnostnej záruky vyššia ako tie, ktoré sú uvedené v tejto tabuľke, uplatňuje sa aj pracovná jednotka špecifická pre zloženie.

AVA_COMP.1 Posúdenie zraniteľnosti zloženého produktu

Ciele

Cieľom tejto činnosti je určiť možnosť zneužitia chýb alebo slabých miest v zloženom TOE ako celku v plánovanom prostredí.

Aplikačné poznámky

Táto činnosť sa zameriava výlučne na posúdenie zraniteľnosti zloženého produktu ako celku a predstavuje len čiastkové úsilie v rámci všeobecného prístupu, na ktorý sa vzťahuje štandardná skupina záruk triedy AVA: AVA_VAN.

Výsledky posúdenia zraniteľnosti pre základnú platformu zastúpenú v ETR_COMP sa môžu opätovne použiť za týchto podmienok: sú aktuálne a všetky zložené činnosti pre správnosť - ASE_COMP.1, ALC_COMP.1, ADV_COMP.1 a ATE_COMP.1 - sú ukončené verdiktom PASS.

Zložením platformy a aplikácie vzniká nová kvalita, ktorá môže spôsobiť ďalšie zraniteľnosti platformy, ktoré nemusia byť uvedené v ETR_COMP. Za týchto okolností platí [R44].

Závislosti:

Žiadne závislosti.

Akčné prvky pre vývojárov:

AVA_COMP.1.1D

Vývojár poskytne zloženú TOE na penetračné testovanie.

Obsah a prezentácia prvkov dôkazov:

AVA_COMP.1.1C

Poskytnutý zložený TOE musí byť vhodný na skúšanie ako celok. Prvky činnosti hodnotiteľa:

AVA_COMP.1.1E

Hodnotiteľ vykoná penetračné testovanie zloženého produktu ako celku na základe vlastnej analýzy zraniteľností hodnotiteľa, aby sa uistil, že zraniteľnosti relevantné pre zložený produkt nie sú zneužiteľné.

Činnosti hodnotiteľa:

Akcia AVA_COMP.1.1E

AVA_COMP.1-1 Hodnotiteľ preskúma výsledky hodnotenia zraniteľnosti základnej platformy, aby zistil, či sa dajú opätovne použiť na zložené hodnotenie.

Výsledky hodnotenia zraniteľnosti základnej platformy sú zvyčajne uvedené v ETR_COMP. Môžu sa opätovne použiť, ak sú splnené tieto podmienky: sú aktuálne a všetky zložené činnosti pre správnosť - ASE_COMP.1, ALC_COMP.1, ADV_COMP.1 a ATE_COMP.1 - sú ukončené verdiktom PASS. Hodnotiteľ zohľadní aj príslušné zistenia v správe o certifikácii platformy. Platnosť certifikátu bezpečnosti platformy je uvedená v kapitole 6 vyššie. Je potrebné poznamenať, že samotná platforma by mohla byť zloženou TOE. To znamená, že sa musí skontrolovať aj platnosť každého ETR pre zloženie TOE, ktoré tvoria TOE platformy.

Keď sa kontroluje platnosť ETR pre zloženie, nutnosť kontroly obsahu závisí od aplikácie a používateľa, ktorý má k dispozícii TSFI. Ak sú TSFI dostupné používateľovi alebo používané aplikáciou, obsah ETR sa musí kontrolovať. Ak nie a formálne platformové TSFI už nie sú k dispozícii ako TSFI, stačí dátum platnosti ETR_COMP.

Výsledok tejto pracovnej jednotky sa integruje do výsledku AVA_VAN.1.3E/ AVA_VAN.1-5 (alebo ekvivalentných vyšších komponentov, ak je zvolená vyššia úroveň záruky).

AVA_COMP.1-2 Hodnotiteľ špecifikuje, vykoná a zdokumentuje penetračné testovanie zloženého produktu ako celku s použitím štandardného prístupu skupiny záruk AVA_VAN.

Ak sú činnosti súvisiace so správnosťou - ASE_COMP.1, ALC_COMP.1, ADV_COMP.1 a ATE_COMP.1 - ukončené verdiktom PASS a certifikát pre platformu pokrýva všetky bezpečnostné vlastnosti potrebné pre zložený produkt, zloženie platformy a aplikácie nesmie vytvoriť ďalšie zraniteľnosti platformy.

Ak hodnotiteľ zistil, že zloženie platformy a aplikácie vytvára dodatočné zraniteľnosti platformy[52], musí sa predpokladať rozpor s verdiktom PASS pre činnosti správnosti alebo certifikát pre platformu nepokrýva všetky bezpečnostné vlastnosti potrebné pre súčasný zložený produkt.

Výsledok tejto pracovnej jednotky sa integruje do výsledku AVA_VAN.1.3E/ AVA_VAN.1-6, AVA_VAN.1-7, AVA_VAN.1-8 (alebo ekvivalentných vyšších komponentov, ak je zvolená vyššia úroveň záruky).

DODATOK 2: ETR PRE ZLOŽENÉ HODNOTENIE

Agentúra ENISA vypracuje šablónu ETR pre zloženie, ktorú použije vývojár platformy na vydanie ETR_COMP.
https://www.sogis.eu/documents/cc/domains/sc/JIL-ETR-template-for-composition-v1-1.pdf je súčasná platná šablóna pre zložené hodnotenia súvisiace s MRA SOG-IS, ktorá môže slúžiť ako technický základ pre šablónu ETR pre zloženie schémy EUCC.

DODATOK 3: PRÍKLADY POKYNOV PRE POUŽÍVATEĽOV PLATFORMY

Upozornenie: Táto časť nemá byť prílohou skutočného ETR pre hodnotenie zloženia, ale je zahrnutá na podporu vývojára platformy pri vytváraní požiadaviek na usmernenie používateľov. Tieto požiadavky na usmernenie používateľa musí vývojár vstavaného softvéru implementovať do aplikácie na ochranu TOE proti určitým útokom.

[52] t. j. nie sú uvedené v ETR_COMP.

Požiadavky na usmernenie používateľa, ktoré sa poskytujú vývojárovi aplikácie, musia mať tieto vlastnosti:

1) Musí byť jasné, čo má používateľ urobiť na ochranu TOE
2) Musí byť jasné, pred akým útokom (cesta alebo čiastočný útok) požiadavka chráni. Podrobnosť musí byť taká, aby vývojár vstavaného softvéru bol schopný vykonať analýzu zhody návrhu. Inými slovami, ak určitý útok nie je pre aplikáciu relevantný, formulácia musí byť taká, aby to vývojár aplikácie rozpoznal.

33. PRÍLOHA 7: UPLATNENIE POTENCIÁLU ÚTOKU NA SMART KARTY A PODOBNÉ ZARIADENIA

ÚČEL

Táto príloha obsahuje opisy metód útoku, ktoré sú špecifické pre smart karty alebo podobné zariadenia, a poskytuje orientačné metriky na výpočet potenciálu útoku, ktorý útočník potrebuje na uskutočnenie útoku. Základným cieľom je pomôcť vyjadriť celkové úsilie potrebné na uskutočnenie úspešného útoku. Toto by sa malo uplatňovať na prevádzkové správanie smart karty alebo podobného zariadenia, a nie na aplikácie špecifické len pre hardvér alebo softvér.

KONKRÉTNY STAV

Žiadne.

KRÍŽOVÝ ODKAZ NA KAPITOLU(-Y), V KTOREJ(-ÝCH) SÚ TIETO PRVKY VYHLÁSENÉ ZA UPLATNITEĽNÉ

Kapitola 8, ŠPECIFICKÉ HODNOTIACE KRITÉRIA A METÓDY.

1 ÚVOD

Táto príloha interpretuje aktuálnu verziu metodiky spoločných kritérií (CEM) (príloha B.4) a poskytuje orientačné metriky na výpočet potenciálu útoku, ktorý útočník potrebuje na uskutočnenie útoku na smart kartu alebo podobné zariadenie. Základným cieľom je pomôcť vyjadriť celkové úsilie potrebné na uskutočnenie úspešného útoku. Toto by sa malo uplatňovať na prevádzkové správanie smart karty alebo podobného zariadenia, a nie na aplikácie špecifické len pre hardvér alebo softvér.

2 OBSAH

Tento dokument zavádza pojem cesta útoku pozostávajúca z jedného až viacerých krokov útoku. Aby sa zraniteľnosť realizovala, je potrebné vykonať analýzu a testy pre každý krok útoku na ceste útoku. Ak ide o kryptografiu, treba sa poradiť s certifikačným orgánom.

3 PREDSLOV: PRACOVNÉ ZAŤAŽENIE PRE HODNOTENIE AVA_VAN.5

Nemožno stanoviť žiadne pevné pravidlá, koľko času by malo kompetentné laboratórium venovať typickému hodnoteniu smart karty alebo podobného zariadenia VAN.5, ale v snahe o harmonizáciu hodnotení a rôznych národných systémov sa predsa len uvádzajú tieto usmernenia: za predpokladu, že analýza zraniteľnosti CC už bola vykonaná, by malo testovanie hodnotenia od začiatku pre nový integrovaný obvod trvať približne 3 mesiace v závislosti od zložitosti integrovaného obvodu, ako je počet kryptografických služieb, rozhraní atď. Celkový čas hodnotenia zložených hodnotení s použitím certifikovaného IC pre testovacie činnosti VAN.5 je rádovo 1 - 3 mesiace v závislosti od zložitosti platformy, ako je otvorená platforma, natívna platforma, počet API atď. Od tohto usmernenia je možné sa odchýliť, ale certifikačnému orgánu bude potrebné poskytnúť určité odôvodnenie.

Predpokladom tohto výkladu je, že certifikačné orgány zabezpečia harmonizáciu nielen na národnej úrovni, ale aj medzi národnými systémami. Je to potrebné napríklad v prípadoch, keď sa uplatňujú nové typy útokov a je potrebné rozhodnúť, kedy sa útok považuje za "vyspelý" a kedy už nezíska body za čas alebo odborné znalosti potrebné na vývoj útoku (ako sa uvádza ďalej).

4 IDENTIFIKÁCIA FAKTOROV

V spoločných kritériách sa nerozlišuje medzi fázou identifikácie a fázou zneužitia útoku. V rámci komunity smart kariet si však riadenie rizík vykonávané používateľom certifikátov CC jednoznačne vyžaduje rozlišovanie medzi nákladmi na "identifikáciu" (preukázanie útoku) a nákladmi na "zneužitie" (napr. po zverejnení skriptu na internete). Preto sa toto rozlíšenie musí vykonať pri výpočte potenciálu útoku pri hodnotení smart kariet alebo podobných zariadení. Hoci je rozlišovanie medzi identifikáciou a zneužitím nevyhnutné na to, aby sa pri hodnotení pochopil a zdokumentoval priebeh útoku, konečný súčet potenciálu útoku sa vypočíta spočítaním bodov týchto dvoch fáz, keďže obe fázy spolu tvoria úplný útok.

4.1 Ako vypočítať útok

Identifikácia cesty útoku, ako aj analýza a testy zneužitia sú mapované na príslušné faktory: uplynulý čas, odborné znalosti, znalosť TOE, prístup k TOE, vybavenie potrebné na vykonanie útoku, ako aj to, či boli použité otvorené vzorky alebo vzorky so známymi tajomstvami. Aj keď útok pozostáva z viacerých krokov, identifikáciu a využitie stačí vypočítať pre celú cestu útoku.

Identifikačná časť útoku zodpovedá úsiliu potrebnému na vytvorenie útoku a preukázanie, že ho možno úspešne aplikovať na TOE (vrátane nastavenia alebo vytvorenia potrebného testovacieho zariadenia). Pri demonštrácii, že útok sa dá úspešne aplikovať, je potrebné zvážiť všetky ťažkosti pri rozširovaní výsledku preukázaného v laboratóriu na vytvorenie užitočného útoku. Napríklad, ak experiment odhalí niektoré bity alebo bajty dôvernej dátovej položky (napríklad kľúč alebo PIN), je potrebné zvážiť, ako by sa získal zvyšok dátovej položky (v tomto príklade by sa niektoré bity mohli merať priamo ďalšími experimentmi, zatiaľ čo iné by sa mohli nájsť inou technikou, napríklad vyčerpávajúcim vyhľadávaním). Na identifikáciu úplného útoku nemusí byť potrebné vykonať všetky experimenty za predpokladu, že je jasné, že útok skutočne dokazuje, že bol získaný prístup k prostriedku TOE a že by sa celý útok mohol reálne vykonať. Predpokladá sa, že jedným z výstupov z identifikácie je skript, ktorý poskytuje opis vykonania útoku krok za krokom - predpokladá sa, že tento skript sa použije v časti zneužitia.

Niekedy fáza identifikácie zahŕňa vývoj nového typu útoku (prípadne vytvorenie nového zariadenia), ktorý sa môže následne použiť na iné TOE. V takom prípade vzniká otázka, ako zaobchádzať s uplynulým časom a ďalšími parametrami pri opätovnom použití útoku. Výklad prijatý v tejto prílohe je taký, že čas vývoja (a prípadne odbornosť) na identifikáciu bude zahŕňať čas vývoja na počiatočné vytvorenie útoku až do momentu, ktorý určí príslušný certifikačný orgán a ktorý sa potom harmonizuje podľa schémy EUCC. Po určení tohto časového bodu sa pri výpočte potenciálu útoku už nebudú používať žiadne ďalšie body za vývoj útoku (z hľadiska času alebo odborných znalostí).

Využitie útoku zodpovedá dosiahnutiu útoku na inú inštanciu TOE pomocou analýzy a techník definovaných v identifikačnej časti útoku. Predpokladá sa, že zneužitie vykoná iný útočník, ale technika (a príslušné základné informácie) je pre zneužitie k dispozícii vo forme skriptu alebo súboru inštrukcií definovaných počas identifikačnej časti útoku. Predpokladá sa, že skript identifikuje potrebné vybavenie a napríklad matematické techniky použité pri analýze[53]. To znamená, že uplynulý čas, odborné znalosti a hodnotenia znalostí TOE pre využitie budú niekedy nižšie pre využitie ako pre identifikáciu. Predpokladá sa napríklad, že skript identifikuje také veci, ako je čas a fyzické umiestnenie potrebné na útok rušivým vplyvom, a preto vo fáze zneužitia nemusí útočník stráviť značný čas hľadaním správneho bodu, v ktorom použije rušivý vplyv. Okrem toho tie isté informácie môžu znížiť aj požiadavku na zneužitie na obyčajné meranie času, zatiaľ čo fáza identifikácie si mohla vyžadovať spätné inžinierstvo hardvérových alebo softvérových informácií z údajov o napájaní - preto sa môže znížiť požiadavka na odborné znalosti. Podobne aj poznatky o aplikácii, ktorá bola použitá na dosiahnutie časového priebehu útoku, môžu byť zahrnuté buď priamo v skripte, alebo nepriamo (prostredníctvom údajov o požadovanom časovom priebehu). Vo všeobecnosti platí, že za fázu zneužitia nemožno vôbec udeliť body, ak bol napr. vo fáze identifikácie kompromitovaný tajný hlavný kľúč spoločný pre všetky skúmané TOE. Je to dôsledok toho, že skript definujúci podrobnosti, ktoré sa majú odovzdať medzi fázou identifikácie a fázou zneužitia, už bude obsahovať informácie o tomto hlavnom kľúči.

Príkladom môže byť uloženie hlavného kľúča v pamäti ROM a obsah pamäte ROM bol počas

[53] Tento predpoklad predstavuje najhorší možný scenár: Informácie získané pri prvom útoku (vo fáze identifikácie) sú plne zdieľané s ostatnými útočníkmi, ktorí chcú tento útok využiť (fáza využitia). Tento predpoklad nie je vždy správny, najmä ak sa útok uskutočňuje s cieľom komerčného zisku a zdieľanie by muselo prebiehať medzi súperiacimi zločineckými organizáciami.

identifikačnej fázy prečítaný, dešifrovaný alebo odkódovaný.
V mnohých prípadoch hodnotitelia skôr odhadnú parametre pre fázu využívania, než aby vykonali úplné využívanie. Odhady a ich zdôvodnenie budú zdokumentované v ETR.

Na dokončenie výpočtu potenciálu útoku je potrebné sčítať body za identifikáciu a zneužitie, pretože obe fázy spolu tvoria úplný útok. Pri prezentácii výpočtu potenciálu útoku v ETR hodnotitelia argumentujú vhodnosť použitých hodnôt parametrov, a preto dajú vývojárovi možnosť spochybniť výpočet pred certifikáciou. Konečný výsledok potenciálu útoku bude preto vychádzať z diskusií medzi vývojárom, ITSEF a CB, pričom CB prijme konečné rozhodnutie, ak sa nedosiahne dohoda.

4.2 Uplynulý čas

V porovnaní s faktorom "uplynulý čas", ktorý je uvedený v CEM, sa pre smart karty a podobné zariadenia zavádza ďalšia granularita. Rozlišuje sa najmä medzi jedným týždňom a niekoľkými týždňami. Uplynulý čas sa teraz delí na tieto intervaly:

Tabuľka 1: *Hodnotenie uplynulého času*

	Identifikácia	Využívanie
< jedna hodina	0	0
< jeden deň	1	3
< jeden týždeň	2	4
< jeden mesiac	3	6
> jeden mesiac	5	8
Nepraktické (pozri nižšie)	*	*

Ak bola identifikovaná cesta útoku a existujú dobre pochopené výsledky analýzy, ktoré umožňujú extrapolovať uplynulý čas pre skutočnú bezpečnostnú konfiguráciu TOE, potom **Error! Reference source not found.** sa rozšíri o tabuľku 1a:

Tabuľka 1a: *Dodatočný hodnotiaci krok pre uplynulý čas*

	Identifikácia	Využívanie
> štyri mesiace	6	10

Nie je rozumné očakávať, že hodnotiace laboratórium bude venovať útokom viac času. Preto sa tabuľka 1a uplatňuje len ako primeraná výnimka. A táto výnimka musí byť odôvodnená výsledkami analýzy/merania, ktoré umožnia definovať zdôvodnenie škálovateľného časového faktora pri útoku. To znamená, že napr. intuícia a náhodný úspech nie sú dostatočným kritériom.

CEM definuje pojem *Nepraktické* ako "cesta útoku nie je zneužiteľná v časovom horizonte, ktorý by bol pre útočníka užitočný".

V praxi je nepravdepodobné, že by hodnotiteľ strávil prácou na TOE viac ako 3 mesiace. Na konci hodnotenia musí hodnotiteľ posúdiť čas, ktorý by potreboval na vykonanie minimálnej cesty útoku. Tým sa vypočíta odhadovaný čas na uskutočnenie útoku, ktorý nemusí byť nevyhnutne časom, ktorý hodnotiteľ strávi vykonaním útoku.

Extrapolácia výsledkov má za cieľ ušetriť náklady a čas, avšak ak je zdôvodnenie spoľahlivé, ale vývojár výsledky spochybní, je potrebné vykonať dodatočné testovanie. Certifikačný orgán musí byť o takomto dodatočnom testovaní informovaný. Upozorňujeme, že sa musí započítať oddelene od pôvodne plánovanej pracovnej záťaže a nesmie nahradiť iné útoky.

Ak útok vychádza zo zistení predchádzajúceho hodnotenia, je potrebné zohľadniť uplynulý čas, ako aj odbornosť, napr. konkrétny útok mohol byť vyvinutý na smart kartu alebo podobné zariadenie s porovnateľnými vlastnosťami ako TOE. Tu nie je možné poskytnúť všeobecné usmernenie.

Otázka "Nepraktické" môže závisieť od konkrétneho scenára útoku, ako ukazujú nasledujúce dva príklady:

a) Uvažujte o smart karte alebo podobnom zariadení ako o TOE používanom v online systéme, kde TOE obsahuje len jednotlivé kľúče, a ďalej predpokladajte, že tieto kľúče sú v systéme deaktivované do niekoľkých dní po nahlásení straty karty. V tomto prípade útok nie je praktický ani vtedy, ak útočník dokáže kľúče extrahovať v priebehu jedného týždňa.
b) Za TOE považujeme smart kartu alebo podobné zariadenie, ktoré obsahuje systémové kľúče, ktoré by sa mohli použiť na podvod, aj keď je použitie jednotlivých kariet po strate zablokované. V tomto prípade môže byť útok úspešný, aj keď trvá rok.

Ak je teda potrebný všeobecný predpoklad o čase "Nepraktické", niečo okolo 3-5 rokov je lepší časový rámec orientovaný na najhorší prípad. (To je čas, po ktorom sa bežne vymieňa generácia kariet a v porovnateľnom časovom rámci sa môžu meniť kľúče celého systému). Najlepším pravidlom sa však zdá byť rozhodovanie o význame "Nepraktické" len v konkrétnom scenári útoku.

4.3 Odbornosť

Na účely smart kariet a podobných zariadení sú úrovne odbornosti definované na základe schopnosti útočníka realizovať útoky, navrhovať spôsoby útoku, vyvíjať nastavenia a postupy útoku, ako aj schopnosti porozumieť konceptom útoku, ak sa uplatňujú aspoň na jednu z nasledujúcich oblastí (neúplný zoznam): Manipulácia s HW, softvérové útoky, kryptografia, zavádzanie chýb, analýza bočných kanálov, reverzné inžinierstvo. Ďalším faktorom určujúcim úroveň odborných znalostí je schopnosť útočníka pracovať s potrebnými nástrojmi a zariadeniami (zoznam príkladov nástrojov a zariadení je uvedený v tabuľke 9).

Tabuľka 2 obsahuje podrobné definície a rozlišovacie faktory pre úrovne odbornosti. Útočník Expert má najmä schopnosť nielen pochopiť zložité koncepty, ale aj využiť toto pochopenie na inováciu a prispôsobenie sa. To zahŕňa vytváranie nových útočných techník, nových spôsobov útoku, neštandardných nastavení alebo postupov, ako aj prepracovanie alebo prispôsobenie existujúcich komplexných útočných techník, spôsobov útoku alebo postupov s cieľom aplikovať ich na TOE. Od zdatného útočníka sa neočakávajú inovačné a adaptačné schopnosti. Schopnosti zdatného útočníka sú obmedzené na úpravy parametrov, ako sú tie, ktoré sú opísané v používateľských príručkách pre zariadenia a nástroje.

Tabuľka 2: *Definícia odbornosti*

	Definícia podľa CEM	**Podrobná definícia, ktorá sa má použiť pri hodnotení smart kariet alebo podobných zariadení[54]**
a) Odborníci	Oboznámený s - Implementované algoritmy, protokoly, hardvérové štruktúry, bezpečnostné správanie, princípy a koncepty bezpečnosti a - Techniky a nástroje na definovanie nových útokov, kryptografia, klasické útoky pre daný typ produktu, metódy útokov atď.	• Schopnosť implementovať novo publikované útoky (zvyčajne na základe dokumentu alebo súvisiaceho patentu) alebo schopnosť navrhnúť nové techniky útoku alebo cesty útoku, ktoré nie sú riešiteľné pomocou hotových zariadení a nástrojov a dobre predpísaných a dostupných súborov postupov. Patrí sem aj prepracovanie alebo implementácia útočných techník, spôsobov útoku, nastavení alebo postupov pre zavedené komplexné útoky, ak novosť alebo potreba prispôsobenia súvisí napríklad s konkrétnym cieľom alebo implementovanými protiopatreniami. a • Hlboké znalosti alebo rozsiahle školenie či skúsenosti v oblasti implementovaných algoritmov, protokolov, hardvérových štruktúr, bezpečnostného správania, princípov a koncepcií bezpečnosti, ktoré umožňujú pochopiť koncepcie „state of the art“ útokov a postupov útokov. ALEBO Schopnosť obsluhovať zložité nástroje a zariadenia, ktoré si vyžadujú odborné znalosti presahujúce rámec toho, čo

[54] Logické operátory v tomto stĺpci by sa mali interpretovať ako: (klauzula 1 a klauzula 2) ALEBO klauzula 3.

	Definícia podľa CEM	Podrobná definícia, ktorá sa má použiť pri hodnotení smart kariet alebo podobných zariadení[54]
		možno ľahko získať z používateľskej príručky. To môže zahŕňať napríklad odborné znalosti v oblasti materiálových vied alebo pokročilého zobrazovania, ktoré sú potrebné na interpretáciu priebežných výsledkov.
b) Znalec	Známe bezpečnostné správanie typu produktu	• Možnosť vykonávať útoky podľa vopred vypracovaných a dostupných postupov, pričom prípadné úpravy parametrov musia byť podrobne opísané, ako napríklad tie, ktoré sú opísané v používateľských príručkách pre zariadenia a nástroje. a • Základné znalosti, školenia alebo skúsenosti s implementovanými algoritmami, protokolmi, hardvérovými štruktúrami, bezpečnostným správaním, princípmi a koncepciami bezpečnosti. ALEBO • Dostatok praxe a znalostí na obsluhu hotových zariadení a nástrojov, pričom sa spoliehajú na dostupné súvisiace používateľské príručky.
c) Laici	Žiadne osobitné odborné znalosti	Žiadne osobitné odborné znalosti

V prípade nejasností by mal ITSEF rozhodovať o vyrovnávaní odbornosti v jednotlivých prípadoch. Najmä v určitých prípadoch, ako napríklad pri manipulácii s HW, ak je súbor postupov na vykonanie útoku dobre predpísaný a dostupný, ale je veľmi zložitý na vykonanie, je možné zvážiť úroveň Útočník Expert (Expert útočník). Naopak, ak presný súbor nekomplikovaných postupov na vykonanie sofistikovaného útoku nie je predpísaný a dostupný, ale od takéhoto dostupného súboru sa líši len nepatrne, úroveň útočníka sa môže považovať za Znalca.

Okrem toho by ITSEF mal rozlišovať medzi internou dostupnosťou vypracovaných postupov útoku a ich dostupnosťou mimo ITSEF. Je to dôležité najmä v prípade po sebe nasledujúcich hodnotení podobných produktov. Najmä hodnotenie by malo vždy odrážať náročnosť celej cesty útoku, ako keby ju vykonávali subjekty mimo ITSEF.

Úrovne Znalec a Expert možno dosiahnuť výlučne na základe schopnosti pracovať s nástrojmi a zariadeniami. Príkladom nástrojov a zariadení, ktoré vedú k hodnoteniu Expert, sú pokročilé nástroje na analýzu porúch, ako je napr. stanica Focus Ion Beam, ktorých obsluha si vyžaduje rozsiahle odborné znalosti, a to aj v prípade, že sa používajú na útoky, ktoré sú dobre zavedené, dobre opísané a nie sú zložité.

Môže sa stať, že na sofistikované útoky je potrebných niekoľko typov odborných znalostí. V takýchto prípadoch sa vyberie najvyšší z rôznych odborných faktorov, ako je uvedené v CEM. Vo veľmi špecifických prípadoch by sa mohla použiť úroveň "Viacnásobný expert", ale treba poznamenať, že expertízy sa musia týkať oblastí, ktoré sú striktne odlišné. Napríklad experti, ako je definované v tabuľke 2, v dvoch alebo viacerých z nasledujúcich oblastí (neúplný zoznam): Manipulácia s HW, softvérové útoky, kryptografia, zavádzanie chýb, analýza bočných kanálov, reverzné inžinierstvo.

Tabuľka 3: *Hodnotenie odbornosti*

	Identifikácia	Využívanie
Laik	0	0
Znalec	2	2
Odborník	5	4
Viacnásobný expert	7	6

4.4 Znalosť TOE

Znalosť TOE sa vzťahuje len na úrovne utajenia súvisiace s identifikáciou a zneužitím zraniteľností v TOE.

Je potrebné dbať na rozlišovanie informácií potrebných na identifikáciu zraniteľnosti od informácií potrebných na jej zneužitie, najmä v oblasti citlivých alebo kritických informácií. Je potrebné jasne si uvedomiť, že akékoľvek informácie potrebné na identifikáciu sa nepovažujú za dodatočný faktor na zneužitie. Vo všeobecnosti sa očakáva, že všetky poznatky potrebné vo fáze zneužitia budú odovzdané z fázy identifikácie prostredníctvom vhodných skriptov opisujúcich útok. Vyžadovať citlivé alebo kritické informácie na zneužitie by bolo neobvyklé.

Ochrana informácií určí stupeň utajenia informácií.

Znalosť TOE môže byť odstupňovaná podľa abstrakcie návrhu, hoci to možno urobiť len na základe TOE. Niektoré návrhy TOE môžu mať verejný zdroj (alebo môžu byť do veľkej miery založené na verejnom zdroji), a preto by sa aj zobrazenie návrhu klasifikovalo ako verejné alebo nanajvýš obmedzené, zatiaľ čo zobrazenie implementácie iných TOE je veľmi prísne kontrolovaná, a preto sa považuje za citlivú alebo dokonca kritickú.

Pri šírení informácií mimo organizácie, ktorá je riešiteľom, možno rozlišovať medzi šírením informácií a poskytovaním prístupu k informáciám. Distribúcia informácií znamená odovzdanie informácií, čím ich použitie už nemôže (prístup) kontrolovať vývojár. Poskytovanie prístupu znamená, že informácie zostanú pod kontrolou vývojára a prístup k nim bude kontrolovaný a chránený. Pre distribúciu a prístup môžu existovať rôzne stupne, ako je definované ďalej.

Čím vyššia je klasifikácia, tým ťažšie je pre útočníka získať informácie potrebné na útok. Toto sa konkrétne vzťahuje na všetky citlivé a kritické informácie, pri ktorých sa vyžaduje audit pracoviska, aby sa poskytlo potrebnú bezpečnostnú záruku o dostatočnosti bezpečnostných opatrení (pozri aj CC ALC_DVS.2, ak sa uplatňuje).

Upozorňujeme, že vývojárska organizácia je definovaná ako všetky organizácie, ktoré sa podieľajú na vývojových a výrobných fázach životného cyklu produktu, ktorý je predmetom hodnotenia (pozri tiež triedu CC ALC). To znamená, že napr. výrobca masky, ktorého subdodávateľom je vývojár smart karty, sa považuje za súčasť vývojárskej organizácie a jeho opatrenia na ochranu a kontrolu prístupu sú súčasťou hodnotenia.

Poznámka: Keďže táto príloha definuje hodnotenie útokov, zdieľanie informácií počas hodnotenia s dôveryhodným systémom certifikačných orgánov a ITSEF neovplyvňuje nižšie uvedenú klasifikáciu. Dôveryhodný systém znamená, že všetky certifikačné orgány v rámci tohto systému si navzájom dôverujú.

Poznámka: ETR pre zloženie (ETR_COMP) je dokument kontrolovaný prostredníctvom systému CC, ktorý vydal príslušný certifikát. Je určený na to, aby ho používal ITSEF, ktorý hodnotí zložený produkt, a nevstupuje do hodnotenia útokov.

Použije sa táto klasifikácia:

- **Verejné informácie** o TOE (alebo žiadne informácie): Informácie sa považujú za verejné, ak ich môže ktokoľvek ľahko získať (napr. z internetu) alebo ak ich vývojár poskytne ktorémukoľvek zákazníkovi bez ďalších prostriedkov.
- **Obmedzené informácie** týkajúce sa TOE: Informácie sa považujú za obmedzené, ak sú kontrolované v rámci vývojárskej organizácie a distribuované iným organizáciám na základe dohody o nezverejňovaní informácií.
- **Citlivé informácie** o TOE sú poznatky, ktoré sú k dispozícii len oddeleným tímom[55] v rámci vývojárskej organizácie. Citlivé informácie sú chránené vyhodnotenými bezpečnými IT systémami (napr. prostredníctvom požiadaviek súvisiacich s prílohou 2, MINIMÁLNE BEZPEČNOSTNÉ POŽIADAVKY LOKALITU) a vhodnými environmentálnymi a organizačnými prostriedkami. Ak je potrebné, aby sa takéto informácie distribuovali iným organizáciám mimo vývojára alebo aby k nim mali prístup iné organizácie, musí to byť obmedzené na prísnu potrebu poznať informácie chránené osobitnou zmluvou.
- **Kritické informácie** o TOE sú poznatky, ktoré sú v rámci vývojárskej organizácie dostupné len tímom na základe zásady "need-to-know". Kritické informácie sú fyzicky a environmentálne chránené vysoko bezpečnou IT infraštruktúrou, ako aj bezpečným fyzickým prostredím vrátane vrstiev na detekciu a prevenciu útokov. Ak je potrebné, aby k takýmto informáciám mali prístup aj

[55] Pri činnostiach ALC sa musia zohľadniť všetky osoby, ktoré sa podieľajú na získavaní prístupu k takýmto informáciám.

iné organizácie ako vývojárska, musí to byť obmedzené na prísnu zásadu need-to-know chránenú osobitnou zmluvou.

- **Veľmi dôležité informácie** o TOE sú poznatky, ktoré sú známe len niekoľkým jednotlivcom a prístup k nim je veľmi prísne kontrolovaný na základe prísnej potreby vedieť a individuálneho záväzku. Návrh moderných integrovaných obvodov zahŕňa nielen obrovské databázy, ale aj sofistikované nástroje na mieru. Prístup k užitočným údajom si preto vyžaduje obrovské a časovo náročné úsilie, ktoré by spôsobilo, že odhalenie by bolo pravdepodobné aj s podporou zasvätenej osoby z vývojárskej organizácie. Ak je útok založený na takýchto znalostiach, zavádza sa nová úroveň "veľmi kritických informácií".

  Veľmi dôležité informácie sa nikdy nesmú poskytovať organizáciám mimo vývojára bez konzultácie
  s príslušným certifikačným orgánom, ktorý vydáva certifikát.

  Mohlo by sa stať, že veľmi dôležité informácie nebude možné exportovať z technických dôvodov, pretože sofistikované na interpretáciu informácií sú potrebné špeciálne nástroje vývojára, alebo jednoducho neexistuje rozhranie na export, alebo existuje len špecializovaná skupina ľudí - ktorá sa môže líšiť od ostatných skupín s nižším stupňom utajenia -, ktorým je špecificky umožnený prístup k týmto veľmi dôležitým informáciám.

  Preskúmanie takýchto informácií je preto zvyčajne možné len v priestoroch vývojára. Spoločnou dohodou všetkých strán hodnotenia by malo byť, že vývoz takýchto informácií mimo priestorov vývojára predstavuje výnimočné riziko, ktorému by sa malo predchádzať.

  - Informácie sa *nepovažujú za praktické,* ak sa uchovávajú len vo vysoko zabezpečených IT systémoch (v rámci chránených lokalít ako v prípade veľmi dôležitých a kritických informácií.

Môže sa stať, že pre sofistikované útoky je potrebných niekoľko typov znalostí. V takýchto prípadoch sa vyberie najvyšší z rôznych faktorov znalostí.

Tabuľka 4: *Hodnotenie znalostí TOE*

	Identifikácia	Využívanie
Verejnosť	0	0
Obmedzené	2	2
Citlivé	4	3
Kritické	6	5
Veľmi kritické	9	*
Nepraktické	*	*

4.5 Prístup k TOE

Dôležitým faktorom je aj prístup k TOE. Vo všeobecnosti hodnotí náročnosť a úsilie pri prístupe a získavaní vzoriek TOE a je opísaný v nasledujúcom texte. V niektorých prípadoch môže balík TOE vytvoriť ďalšiu prekážku prístupu k citlivým častiam TOE. Preto sa hodnotenie "Prístup k TOE" môže rozšíriť o posúdenie balíka ako súčasti TOE. Metodika je opísaná v časti 4.5.1.

Predpokladá sa tu, že vzorky TOE by útočník zakúpil alebo inak získal a že okrem iných faktorov neexistuje žiadne časové obmedzenie pri analýze alebo modifikácii TOE. Je potrebné zohľadniť dostupnosť vzoriek (z hľadiska času a nákladov), ako aj počet vzoriek potrebných na uskutočnenie cesty útoku (toto nahradí faktor CEM "Window of Opportunity").

Scenár útoku si môže vyžadovať prístup k viac ako jednej vzorke TOE, pretože:

- útok je úspešný len s určitou pravdepodobnosťou na danom zariadení, takže je potrebné vyskúšať viacero zariadení,
- útok je úspešný až po zničení určitého počtu zariadení (v priemere),
- útočník musí zhromažďovať informácie z viacerých kópií TOE. V tomto prípade sa prístup k TOE zohľadňuje pomocou nasledujúceho hodnotenia:

Tabuľka 5: Hodnotenie prístupu k TOE

	Identifikácia	Využívanie
< 10 vzoriek	0	0
< 30 vzoriek	1	2
< 100 vzoriek	2	4
> 100 vzoriek	3	6
Nepraktické	*	*

"Nepraktické" sa vysvetľuje takto:

- Pre identifikáciu: nepraktické sa začína s najnižším číslom medzi 2 000 vzorkami a najväčším celým číslom menším alebo rovným $n/(1+(log\ n)^2)$, pričom n je odhadovaný počet produktov, ktoré sa majú vytvoriť.
- Pre využitie: nepraktické začína s najnižším číslom medzi 500 vzorkami a najväčším celým číslom menším alebo rovným $n/(1+(log\ n)^3)$, pričom n je odhadovaný počet produktov, ktoré sa majú vytvoriť.

Napríklad, ak sa *n* rovná 20 000 (vyrobených vzoriek), limity "Nepraktické" by boli 1 025 a 248 vzoriek pre identifikáciu a využitie.

Mala by sa zohľadniť aj bezpečnostná politika vyjadrená v bezpečnostnom zámere.

4.5.1 Hodnotenie úsilia pri príprave balíka TOE

V prípadoch, keď dodávateľ definoval balík ako súčasť TOE, môže byť balík následne súčasťou cesty útoku a musí sa zohľadniť vo fáze identifikácie a zneužitia.

V nasledujúcom texte sa uvádzajú skôr usmernenia než absolútne pevné hodnoty hodnotenia, pretože na jednej strane existuje nespočetné množstvo typov a materiálov obalov a na druhej strane vznikajú nové metódy a techniky, ktoré ešte nemusia byť verejne známe pre odstraňovanie obalov v tejto oblasti.

Môžu sa vyskytnúť balíky, v ktorých je odstránenie problematické, pokiaľ ide o metódy a techniky, a v takýchto prípadoch musí predajca poskytnúť hodnotiteľovi požadované informácie. Ak stále pretrváva neistota, hodnotiteľ by sa mal spojiť s externými odborníkmi, napríklad univerzitami, inštitútmi atď. s cieľom získať jasnú predstavu o tom, ako hodnotiť odstránenie takéhoto balíka.

Hodnotenie útokov (napr. zavádzanie chýb, reverzné inžinierstvo, útoky bočným kanálom atď.) sa hodnotí nezávisle od úsilia o prípravu balíka. Ak sa tvrdí, že balík je súčasťou TOE, čiastočný útok na prípravu balíka sa hodnotí extra bodmi za "prístup k TOE", ako je opísané ďalej. Toto hodnotenie úsilia o prípravu balíka pokrýva všetky ostatné faktory, a preto sa inde neprideľujú žiadne ďalšie body.

Usmernenie pre hodnotenie odstránenia balíka zohľadňuje odchýlku na nízku, strednú a vysokú náročnosť prípravy balíka. Definícia týchto pojmov a príklady hodnotenia sú uvedené v časti A.1.

Tabuľka 6: Hodnotenie odstránenia balíka TOE (dodatočné body vo faktore "Prístup k TOE")

	Identifikácia	Využívanie
Nízke nároky na prípravu	0	0
Stredné úsilie pri príprave	1	2
Vysoké úsilie pri príprave	2	4

Nízka náročnosť prípravy: Jednoduché obaly, ktoré možno odstrániť štandardným chemickým leptaním, mechanickým pôsobením, opätovným zapojením alebo podobne.

Stredne náročná príprava: Balíky, ktoré majú relatívne vysoké riziko fatálneho poškodenia TOE (strata funkčnosti, ktorá je cieľom alebo je potrebná na hodnotenie) z dôvodu špeciálnej konštrukcie.

Vysoké úsilie pri príprave: Balíky, ktoré si vyžadujú viacero expertov, vysoké úsilie a zriedkavé nástroje na mieru, ktoré nie sú deklarované ako bezpečnostné funkcie.

Všimnite si, že ak reverzné inžinierstvo nie je potrebné pri zneužití opakovať, body za zneužitie sa následne pridelia len vtedy, ak si zostávajúca cesta útoku stále vyžaduje špecializované vybavenie alebo vyššie.

4.6 Zariadenie

Zariadením sa rozumie hardvér/softvér alebo cloudové/on-line služby, ktoré sú potrebné na identifikáciu alebo zneužitie zraniteľnosti.

Pri určovaní kategórie zariadenia je potrebné zohľadniť cenu a dostupnosť.

- Žiadne
- **Štandardné vybavenie** je vybavenie, ktoré je útočníkovi ľahko dostupné buď na identifikáciu zraniteľnosti, alebo na útok. Toto vybavenie sa dá ľahko získať napr. v blízkom obchode alebo stiahnuť z internetu. Zariadenie môže pozostávať z jednoduchých útočných skriptov, osobných počítačov, čítačiek kariet, generátorov vzorov, jednoduchých optických mikroskopov, napájacích zdrojov alebo jednoduchých mechanických nástrojov.
- **Špecializované vybavenie** nie je pre útočníka ľahko dostupné, ale so zvýšeným úsilím by ho mohol získať. Mohlo by to zahŕňať nákup stredne veľkého množstva zariadení (napr. nástroje na analýzu výkonu, použitie stoviek počítačov prepojených cez internet, analyzátory protokolov, osciloskopy, pracovisko s mikrosondou, chemický pracovný stôl, presné frézy atď. alebo vývoj rozsiahlejších útočných skriptov alebo programov.
- **Zariadenia na mieru** nie sú ľahko dostupné pre verejnosť, pretože môžu vyžadovať špeciálnu výrobu (napr. veľmi sofistikovaný softvér) alebo sú natoľko špecializované, že ich distribúcia je kontrolovaná, prípadne dokonca obmedzená. Prípadne môže byť zariadenie veľmi drahé (napr. fokusovaný iónový lúč, skenovací elektrónový mikroskop a abrazívne laserové zariadenie).
  V závislosti od možností prenájmu zariadenia a typu manipulácie, ktorá sa má vykonať, sa môže prehodnotiť klasifikácia zariadenia ako zariadenia na mieru. Komplexný a špecializovaný softvér (napr. pokročilé analytické nástroje, ktoré nie sú k dispozícii na zakúpenie), ktorý bol vyvinutý počas fázy identifikácie, možno považovať za vybavenie na mieru alebo alternatívne hodnotiť podľa kritérií Elapsed time (Uplynulý čas) a Expertise (Odbornosť); vo fáze využívania sa nesmie dodatočne posudzovať. Ak hodnotiteľ musí prispôsobiť svoj špecializovaný analytický softvér, napr. nástroje/skripty na zarovnávanie alebo filtre špeciálne pre TOE alebo deriváty TOE, potom sa to musí hodnotiť dodatočne (Elapsed time (uplynulý čas), Expertise (odbornosť), Knowledge of the TOE (znalosť TOE), samples (vzorky) ...) vo fáze identifikácie.

  Komplexný a špecializovaný softvér, ako je uvedené vyššie, možno charakterizovať ako softvér vyvinutý počas identifikačnej fázy pre hodnotené TOE alebo aplikovaný na iné TOE, pričom ITSEF ho stále považuje za softvér, ktorý je mimo súčasného „state of the art“. V prípade, že existuje neistota o „state of the art“, môže byť potrebná diskusia na úrovni príslušnej podskupiny ECCG.

Môže sa stať, že na sofistikované útoky je potrebných niekoľko typov zariadení. V takýchto prípadoch sa štandardne vyberie najvyšší z rôznych faktorov vybavenia.

Všimnite si, že používanie zariadení na mieru by malo viesť minimálne k miernemu potenciálu.

Úroveň "Multiple Bespoke" sa zavádza s cieľom umožniť situáciu, keď sú pre jednotlivé kroky útoku potrebné rôzne typy na mieru vyrobeného vybavenia.

Tabuľka 7: *Hodnotenie zariadení*

	Identifikácia	Využívanie
Žiadne	0	0
Štandard	1	2
Špecializované [1]	3	4
Na mieru	5	6

	Identifikácia	Využívanie
Viaceré na mieru	7	8

(1) Ak sú pre jednotlivé kroky útoku potrebné jasne odlišné testovacie pracoviská pozostávajúce zo špecializovaného vybavenia, hodnotí sa to ako na mieru. Testovacie pracoviská pre útoky bočnými kanálmi a útoky na poruchy sa zvyčajne považujú za príliš podobné a nedostatočne odlišné. V takýchto prípadoch, keď sa vyžaduje viacero podobných špecializovaných zariadení, sa to potom bude považovať za viacnásobne špecializované a k hodnoteniu sa pripočíta ďalší 1 bod.

V ideálnom svete je potrebné uviesť definície, aby sme vedeli, aké sú pravidlá a charakteristiky pre priradenie kategórie k zariadeniu alebo súboru zariadení. Do úvahy sa berie najmä cena, dostupnosť zariadenia (verejne dostupné, predaj kontrolovaný výrobcom s potenciálne niekoľkými úrovňami kontroly, môže byť prenajaté) a dostupnosť príslušných prevádzkových zdrojov. Dostupnosť príslušných prevádzkových zdrojov sa musí zohľadniť najmä vtedy, ak sa má klasifikovať vybavenie na mieru, ako sú nástroje na overovanie návrhu alebo analýzu porúch.

Výrobcovia majú zvyčajne informácie o trhu so sofistikovaným náradím a o tom, kde sa dá takéto zariadenie zaobstarať. Výrobcovia spravidla kontrolujú aj väčšinu trhu s použitým náradím.

Efektívne používanie týchto nástrojov si vyžaduje buď veľmi dlhé skúsenosti, alebo sa spolu so zariadením najíma aj ľudská obsluha. Inými slovami, zariadenia na mieru obsluhuje len malý počet špecializovaných skúsených odborníkov. Napriek tomu nemožno vylúčiť, že určitý typ zariadenia môže byť dostupný prostredníctvom univerzitných laboratórií alebo rovnocenných zariadení, ale napriek tomu je pomerne ťažké získať odborné znalosti o používaní tohto zariadenia. Preto sa očakáva určitý súlad medzi hodnoteniami odborných znalostí a zariadení.

Upozorňujeme, že v prípade, že sú potrebné dodatočné prevádzkové zdroje, je potrebné ich zohľadniť aj v rámci faktora odbornosti v tabuľke hodnotenia útokov. Tabuľky uvedené v nasledujúcej časti zostavila skupina odborníkov z odvetvia a bude ich potrebné z času na čas revidovať, pretože sortiment zariadení, ktoré má potenciálny útočník k dispozícii, sa zvyčajne neustále zlepšuje:

- Zvýšenie výpočtového výkonu
- Zníženie nákladov na nástroje
- Dostupnosť nástrojov môže zvýšiť
- Nové nástroje sa môžu objaviť vďaka novým technológiám alebo novým formám útokov.

4.6.1 Nástroje

Hranicu medzi štandardnými, špecializovanými a na mieru šitými produktami nemožno vo všetkých prípadoch jasne vymedziť. Ako je uvedené vyššie, toto rozhodnutie sa prijíma od prípadu k prípadu v závislosti od „state of the art“ technológie, dostupnosti nástrojov, nákladov na nákup a príslušných prevádzkových zdrojov.

Ako pomôcka pri hodnotení by sa mala použiť nákupná cena zariadenia (či už ide o nové alebo renovované zariadenie) ako hlavný rozlišovací znak podľa tabuľky 8. Náklady uvedené v tejto tabuľke nepredstavujú náklady na útok, ale len nákupnú trhovú cenu každého zariadenia alebo pracovnej stanice.

Tento rozlišovač poskytuje najlepší praktický prístup vzhľadom na dostupnosť zariadenia (resp. obstaranie). Okrem toho dáva každej kategórii priradenie. Táto tabuľka sa bude pravidelne aktualizovať v nadväznosti na vývoj trhu so zariadeniami.

Tabuľka 8: *Hodnotenie zariadenia v porovnaní s obstarávacími nákladmi*

Nákupné náklady	Hodnotenie zariadenia
Do 10 K€	Štandard
Od 10 K€ do 200 K€	Špecializované
Viac ako 200 K€	Na mieru

V nasledujúcej tabuľke 9 sú uvedené typické príklady s použitím vybraných informácií z tabuľky 8 a všeobecných pravidiel z predchádzajúcej časti a implementuje sa všeobecné usmernenie.

Tabuľka 9: Kategorizácia nástrojov

Nástroj	Zariadenie
Vstrekovanie svetla nízkej intenzity (UV, bleskové svetlo)	Štandard
Elektrické poruchy pracoviska	Štandard
Binokulárny mikroskop	Štandard
Nástroje na tepelné namáhanie	Štandard
Napájacie napätie	Štandard
PC alebo pracovná stanica	Štandard
Softvérové nástroje (fuzzing, testovací balík)	Štandard
Nástroje na statickú analýzu kódu	Štandard
Osciloskop nižšej triedy	Štandard
Špičková grafická karta	Štandard
Nástroje na analýzu signálov	Štandard
Pracovné stanice EMFI, FBBI	Špecializované
Optický mikroskop	Špecializované
Pracovná stanica 3D röntgenového žiarenia	Špecializované
Pracovná stanica na mikrosondovanie	Špecializované
Špičková laserová pracovná stanica	Špecializované
Systém rozpoznávania vzorov v reálnom čase	Špecializované
Špičkový osciloskop	Špecializované
Analyzátor spektra	Špecializované
Nástroje pre mokrú chémiu (kyseliny a rozpúšťadlá)	Špecializované
Suchá chémia (plazma)	Špecializované
Mikrofrézovací a zrieďovací stroj	Špecializované
Skenovací elektrónový mikroskop (SEM)	Špecializované
Pracovná stanica na získavanie EM signálu	Špecializované
Emisný mikroskop nízkeho výkonu (EMMI)	Špecializované
Nízkofrekvenčný fokusovaný iónový lúč (FIB)	Špecializované
Špičkový skenovací elektrónový mikroskop (SEM)	Na mieru
Mikroskop atómových síl (AFM)	Na mieru
Špičkový fokusovaný iónový lúč (FIB)	Na mieru

Nástroj	Zariadenie
Nové technické nástroje na overovanie dizajnu a analýzu porúch	Na mieru
Špičkový emisný mikroskop (EMMI)	Na mieru
Pracovná stanica na reverzné inžinierstvo čipov	Na mieru

4.7 Otvorené vzorky/vzorky so známymi tajomstvami

V niektorých prípadoch je vhodné použiť v rámci procesu hodnotenia špeciálne vzorky. V ďalšom texte sa tieto vzorky budú nazývať "otvorené vzorky" alebo "vzorky so známym tajomstvom". Použitie "otvorených vzoriek" alebo "vzoriek so známym tajomstvom", ich rozsah a dôsledky na hodnotenie a hodnotenie útoku sú opísané v tejto časti.

4.7.1 Objasnenie pojmov platforma, aplikácia a HW-TOE

Pri zloženom hodnotení sa vlastnosti základnej platformy spravidla preberajú z informácií dodaných spolu s dokumentáciou z certifikácie základnej platformy. V prílohe 6, HODNOTENIE ZLOŽĚNÉHO PRODUKTU PRE SMART KARTY A PODOBNÉ ZARIADENIA, sa špecifikuje proces, ktorý sa nazýva "zložené hodnotenie smart kariet". V tejto prílohe sú platforma a aplikácia relatívne pojmy a všeobecné termíny. Platformou môže byť napríklad certifikovaný integrovaný obvod s jeho firmvérom, certifikovaný vstavaný softvér alebo kombinácia oboch. Certifikovaná platforma sa používa ako základ pre zložené hodnotenie. Aplikácia je ďalší vstavaný softvér, ktorý je pridaný na certifikovanú platformu. Môže to byť napríklad operačný systém na certifikovanom integrovanom obvode, aplikácia na certifikovanom integrovanom obvode a operačnom systéme, ako je aplikácia na produkte Java Card, alebo kombinácia operačného systému a aplikácií na certifikovanom integrovanom obvode. Pojmy platforma a aplikácia, ktoré sa používajú v nasledujúcich oddieloch, zodpovedajú pojmom použitým v prílohe 6.

V mnohých prípadoch je základom pre všetky následné certifikácie smart kariet a podobných zariadení certifikát hardvérového integrovaného obvodu. Tento hardvérový IC certifikát zahŕňa prinajmenšom HW-IC a firmvér na jeho prevádzku, ale môže obsahovať aj ďalší softvér, ktorý poskytuje napríklad kryptografické služby používateľovi. Kombinácia hardvéru IC, firmvéru a dodatočného softvéru sa dodáva so špeciálnymi dokumentmi s pokynmi pre používateľov, ktoré tiež patria k príslušnej definícii TOE.

Ďalšie softvérové komponenty pri hodnotení HW IC používajú pojem "aplikácia" nad HW IC a firmvérom. Definícia otvorených vzoriek v zmysle zloženého hodnotenia aplikácií uvedená v nasledujúcej kapitole sa vzťahuje aj na ďalšie SW komponenty, ktoré sa hodnotia v kontexte certifikácie HW IC.

Pre kombináciu HW IC a firmvéru sa v nasledujúcich častiach používa skratka HW-TOE.

4.7.2 Definícia "otvorených vzoriek / vzoriek so známymi tajomstvami"

V kontexte hodnotenia HW-TOE, s výnimkou SW komponentov, pojem "otvorená vzorka" označuje vzorky s možnosťou stiahnutia a/alebo spustenia akéhokoľvek testovacieho softvéru. Okrem toho môžu takéto vzorky umožniť nezabezpečené konfigurácie HW-TOE, napr. obísť protiopatrenia firmvéru alebo zmeniť vnútornú konfigurácu hardvéru IC. To môže zahŕňať podporu špecifických testovacích prostredí zo strany dodávateľa, keďže balík operačného systému nie je súčasťou HW-TOE. Hardvér integrovaného obvodu sa nesmie meniť, pretože by to vyvolalo otázky týkajúce sa platnosti a z hľadiska nákladov nie je odôvodnené, aby dodávateľ menil hardvér integrovaného obvodu len na účely hodnotenia.

V kontexte zloženého hodnotenia alebo v prípade SW komponentov pri certifikácii HW-IC sa pod pojmom "otvorené vzorky" rozumejú vzorky, pri ktorých hodnotiteľ môže na platformu alebo HW-TOE umiestniť aplikácie podľa vlastného uváženia, ktoré obchádzajú protiopatrenia predpísané v návode na používanie platformy alebo protiopatrenia implementované v samotných aplikáciách. Zámerom je používať testovacie aplikácie bez protiopatrení, ale nie deaktivovať akékoľvek protiopatrenia vlastné

platforme, resp.

Pri zloženom hodnotení môže testovacia aplikácia slúžiť na zvýraznenie vlastností platformy opísaných v ETR_COMP vzhľadom na osobitné použitie platformy v TOE, ale nesmie sa použiť na opakovanie hodnotenia platformy.

Okrem toho je ďalšou možnosťou umožniť hodnotiteľovi definovať jeden alebo viacero tajných údajov pre aktívum TOE, ako je PIN alebo kľúč, ak by táto možnosť nebola dostupná v rámci bežnej prevádzky TOE. Tieto vzorky budú pomenované ako "Vzorky so známym tajomstvom" a môžu sa použiť na vykonanie útokov na tento prostriedok bez deaktivácie protiopatrení. Umožniť hodnotiteľovi definovať tajné údaje pre jedno aktívum neznamená, že tieto informácie sa použijú na útok na iné aktívum TOE.

Ak bežná konfigurácia TOE poskytuje ITSEF možnosť plnej kontroly nad vstupnými a výstupnými údajmi, nemožno použiť termín "vzorky so známymi tajomstvami". O "vzorkách so známymi tajomstvami" však možno uvažovať aj počas hodnotenia HW, ak dodávateľ poskytne špecifický prístup k interným tajomstvám. Napríklad: kryptografické mechanizmy používané interne HW-TOE, napríklad používané na šifrovanie pamäte.

Upozorňujeme, že každé funkčné rozhranie alebo kľúč potrebný na funkčné testy TOE, ktoré dodávateľ poskytne ITSEF, sa nepovažuje za "otvorenú vzorku / vzorku so známymi tajomstvami".

4.7.3 Používanie "otvorených vzoriek / vzoriek so známymi tajomstvami"

V niektorých špeciálnych prípadoch môže analýza zraniteľnosti a definovanie útokov vyústiť do cesty útoku, ktorú je ťažké alebo v najhoršom prípade nemožné vyhodnotiť, pretože by si vyžadovala značný čas alebo rozsiahle predbežné testovanie, ak sa berie do úvahy len znalosť TOE.

Okrem toho sa platforma môže používať spôsobom, ktorý vývojár platformy a hodnotiteľ platformy nepredpokladali, alebo vývojár aplikácie nemusel dodržiavať odporúčania poskytnuté spolu s platformou a zaviedol iné protiopatrenia, ktorých efektívnosť ešte nebola preukázaná.

Nakoniec musí zložený hodnotiteľ zohľadniť časti funkčnosti platformy, ktoré nemusia byť zahrnuté v bezpečnostnom zámere platformy, a teda v predchádzajúcom hodnotení platformy.

V takýchto prípadoch existujú rôzne možnosti, ako skrátiť čas hodnotenia:

- Zložený hodnotiteľ sa môže poradiť s hodnotiteľom základnej platformy a so súhlasom dodávateľa platformy využiť jeho skúsenosti získané počas hodnotenia.
- Oddelenie protiopatrení v rámci aplikácie a protiopatrení aplikácie a platformy pomocou "otvorených vzoriek".
- Urýchliť vyhodnotenie, najmä ak ide o kryptografické operácie, použitím "vzoriek so známym tajomstvom". Pri týchto vzorkách hodnotiteľ pozná "tajomstvo" (kľúč). To umožňuje buď porovnanie získaných údajov (napr. odvodených z pasívnej analýzy) so "známym tajomstvom". "Otvorené vzorky" môžu byť užitočné v kroku profilovania, ktorý sa vyžaduje pri niektorých útokoch, ako sú napríklad útoky na šablóny. Vyhodnocovateľ má teda zjednodušený spôsob, ako určiť, či jeho útok odhalil správne tajomstvo. Môže sa zastaviť po získaní častí "tajomstva" a odhadnúť zostávajúci čas na nájdenie celého "tajomstva".

Aby bolo hodnotenie efektívne a zmysluplné v primeranom čase, ako už bolo spomenuté, môže byť potrebné použiť "otvorené vzorky / vzorky so známymi tajomstvami". V takom prípade by sa mali dodržiavať určité pravidlá:

- Účelom otvorených vzoriek/vzoriek so známymi tajomstvami je stanoviť testy na hodnotenie a nie, v prípade zloženého hodnotenia, opakovať hodnotenie platformy.
- Použitie otvorených vzoriek/vzoriek so známym tajomstvom, tok informácií medzi stranami a v prípade potreby podpora dodatočných služieb sa prerokuje a dohodne medzi certifikačným orgánom hodnotiteľ, vývojár a tvorca otvorených vzoriek. Patrí sem aj čas strávený pri testoch s otvorenými vzorkami / vzorkami so známym tajomstvom.
- Zlyhania a zistenia vyplývajúce z testov sa oznamujú a dávajú na vedomie aspoň certifikačnému orgánu TOE. V prípade zloženého hodnotenia certifikačný orgán zloženého TOE prijme príslušné opatrenia spolu s certifikačným orgánom hodnotenia základnej platformy v súlade s pravidlami prílohy 6.
- Hodnotenie musí obsahovať ustanovenie o tom, či by útok bol možný bez použitia "otvorených vzoriek / vzoriek so známym tajomstvom" (pozri oddiel 4.7.5).

4.7.4 Dôsledky na hodnotenie

Pomocou "otvorených vzoriek / vzoriek so známym tajomstvom" je možné umožniť alebo faktorizovať cesty útoku a tým znížiť zložitosť útoku. To šetrí čas pri vyhodnocovaní, pretože umožňuje získať cieľový výsledok oveľa rýchlejšie.

Otvorené vzorky môžu umožniť vykonať posúdenie úniku pred akýmkoľvek útokom bočným kanálom vyhodnotením úniku s ďalšími protiopatreniami a bez nich. Následne sa TOE môže overiť vhodnou metódou útoku.

Ak sa únik zistil vypnutím ďalších protiopatrení a ak sa dalo vykonať teoretické posúdenie, možno odhadnúť počet stôp potrebných na úspešný útok na TOE. Na získanie porovnateľných výsledkov pri hodnoteniach, pri ktorých sa nevykonáva posúdenie úniku, sa musí vopred obmedziť časový rámec alebo počet stôp akvizičnej kampane a teoretický odhad sa musí porovnať s týmto limitom.

Ďalším dobrým príkladom pre otvorené vzorky je získavanie tajných informácií (napr. kľúčov) pomocou ľahkých útokov. V dobre navrhnutom produkte bude mať platforma aj aplikácia ochranné mechanizmy na odvrátenie tohto útoku. V kombinácii s nimi budú útoky pomerne ťažké. Hodnotiteľ bude musieť vyskúšať veľmi vysoký počet kombinácií a variácií parametrov, ako je priemer lúča, frekvencia svetla, energia svetla, miesto použitia svetla, poloha v čase záblesku svetla. Obzvlášť ťažké to bude, ak aplikácia obsahuje prostriedky na znefunkčnenie TOE v prípade zistenia útoku. Útok by mohol byť nielen časovo veľmi náročný, ale vyžadoval by si aj veľký počet vzoriek.

Pri "otvorených vzorkách" je situácia úplne iná. Hodnotiteľ môže použiť vlastný optimalizovaný testovací program a skenovať IC na "slabé miesta" oveľa rýchlejšie a bez rizika zničenia zariadenia. Môže tiež optimalizovať svoju účinnosť na nájdenom "slabom mieste" predtým, ako sa vráti k útoku na TOE. Aj keby sa vedelo o existencii "slabých miest", stále sa potom musí optimalizácia a výber najlepšieho miesta vykonať na konečnom TOE. Pomocou "otvorených vzoriek" v týchto testoch môže potom útočník uskutočniť oveľa cielenejšie útoky na TOE.

Nasledujúce príklady opisujú napríklad použitie "vzoriek so známym tajomstvom":

- Extrahovanie celého kľúča môže byť časovo veľmi náročné. Pri niektorých chybách v získanom kľúči a bez možnosti rozhodnúť, ktorá časť tajomstva je nesprávna, by útok nemusel byť možný z dôvodu časových obmedzení.
- Na vykonanie niektorých útokov, napríklad útokov pomocou šablón, je niekedy potrebná fáza profilovania. Znalosť kľúča a následne medzihodnoty algoritmov potom môže umožniť útok, zatiaľ čo bez použitia takýchto vzoriek by útok nebol praktický.

4.7.5 Výpočet potenciálu útoku

V tabuľke potenciálu útoku je definovaný dodatočný faktor pre "otvorené vzorky / vzorky so známym tajomstvom", pričom body sa udeľujú len vo fáze identifikácie. Vzhľadom na definíciu "otvorených vzoriek / vzoriek so známymi tajomstvami" je jasné, že tieto je zakázané používať vo fáze zneužitia.

Pri hodnotení útoku, ktorý využíva "otvorené vzorky/vzorky so známymi tajomstvami", musí hodnotiteľ najprv spravodlivo určiť (aspoň teoreticky) a opísať spôsob, akým by útočník mohol vykonať útok na skutočné TOE (namiesto na otvorenú vzorku/vzorku so známymi tajomstvami). Po určení tohto faktu hodnotiteľ vykoná dva výpočty s použitím a bez použitia "otvorených vzoriek/vzoriek so známymi tajomstvami":

- Odhad hodnoty každého faktora pre útočníka bez prístupu k otvoreným vzorkám / vzorkám so známym tajomstvom.
- Uveďte hodnoty jednotlivých faktorov zodpovedajúce tomu, čo urobil (ak by dokončil celý útok):
  - strávený čas, zničené vzorky, odbornosť, znalosť TOE, vybavenie
  - Sčítanie bodov zodpovedajúcich použitým "otvoreným vzorkám / vzorkám so známym tajomstvom".

Ak by sa ukázalo, že:

1) útok je "Nepraktický", ak sa nepoužívajú otvorené vzorky alebo vzorky so známym tajomstvom, a
2) hodnotenie faktora "otvorená vzorka/vzorka so známym tajomstvom" v tejto oblasti nie je verejné a
3) vývojár oficiálne tvrdí, že funkcia použitá na otvorenej vzorke nie je dostupnou funkciou, ktorá je k dispozícii používateľom zariadenia v teréne,

potom je hodnotenie "Nepraktické" (t. j. hodnotenie "otvorené vzorky / vzorky so známym tajomstvom"

sa musí vyradiť). Ak vývojár zmení svoje formálne hodnotenie, musí sa vykonať nové hodnotenie TOE.

Vo všetkých ostatných prípadoch bude konečná hodnota minimálna z týchto dvoch výpočtov. Očakáva sa, že tieto dve hodnoty budú pomerne blízke. Ak tomu tak nie je, na rozhodnutie o hodnotení je potrebná ďalšia analýza.

V prípade existencie "otvorených vzoriek/vzoriek so známym tajomstvom" je možná tajná dohoda (alebo priamy útok, napríklad krádež) na ich získanie rovnakým spôsobom, ako sa pri hodnotení zohľadňuje možná tajná dohoda alebo priamy útok útočníka na získanie informácií, ako je definované v kapitole
o znalosti TOE.

V prípade "vzoriek so známym tajomstvom" je definovanie úrovne ochrany súčasťou hodnotenia celého produktu.

Body zodpovedajúce dostupnosti "vzoriek so známym tajomstvom" sú definované s prihliadnutím na úroveň kontroly prístupu k tajomstvu, ktorú vzorka poskytuje, a na ochranu tajomstva v rámci organizácie vývojára a mimo nej počas celého životného cyklu:

- Verejnosť:

  Tajomstvo je prístupné bez akýchkoľvek obmedzení (verejné dokumenty, vzor umožňujúci spoznať tajomstvo,...).

- Obmedzené:

  Tajomstvo je kontrolované v rámci organizácie vývojára. Mimo organizácie vývojára môžu mať k tajomstvu prístup všetci ľudia, ktorí podpísali NDA.

  Ak môže byť tajomstvo zverejnené vzorkou, musí byť chránené kontrolou prístupu pomocou prístupových údajov, ktoré sú chránené ako obmedzené tajomstvá.

- Citlivé:

  V rámci organizácie vývojára alebo mimo nej sa tajomstvá zdieľajú len v rámci oddelených tímov alebo zariadení, ktoré sú jasne identifikované a majú prísne kontroly prístupu. Nakladanie s tajomstvom sa riadi špecifickými a vhodnými písomnými postupmi na jeho ochranu a existuje jasná metóda, ktorou sa identifikuje, že tajomstvo si vyžaduje tieto postupy (napr. označením údajov).

  Ak sa má tajomstvo poskytnúť iným organizáciám, musí to byť na základe prísnej zásady "need-to-know", ktorá je chránená osobitnou zmluvou. Iná organizácia musí poskytnúť bezpečné prostredie, ktoré je vyhodnotené alebo zmluvne zhodné s kritériami prijateľnými pre certifikačný orgán.

  Ak môže byť tajomstvo zverejnené vzorkou, musí byť chránené kontrolou prístupu pomocou prístupových údajov, ktoré sú chránené ako citlivé tajomstvo.

- Kritické:

  Tajomstvo sa nezdieľa mimo organizácie vývojára.
  V rámci organizácie vývojára sa tajomstvá zdieľajú len s niekoľkými ľuďmi alebo niekoľkými jasne identifikovanými zariadeniami, pričom sa prísne kontroluje prístup na základe zásady "need-to-know". Nakladanie s tajomstvom sa riadi špecifickými a vhodnými písomnými postupmi na jeho ochranu a existuje jasná metóda, ktorou sa identifikuje, že tajomstvo si tieto postupy vyžaduje (napr. označením údajov). Môže sa uplatniť na nasledujúce príklady:

  - HW kľúč rozdelený medzi masku a Flash alebo PUF alebo iné.
  - Podpisovanie kľúčov na aktualizáciu firmvéru v teréne.

  Ak môže byť tajomstvo zverejnené vzorkou, musí byť chránené kontrolou prístupu pomocou prístupových údajov, ktoré sú chránené ako "kritické" tajomstvá.

- Nepraktické:

Tajomstvo sa nezdieľa mimo organizácie vývojára.

Vývojár nemá možnosť poznať tajomstvo. Vzorka nemôže zverejniť tajomstvo. Napríklad:

- Kľúče sa kompletne generujú vo vnútri zariadenia.
- Kľúče vygenerované v HSM, ku ktorým vývojár nemá prístup, a prenesené do TOE prostredníctvom zabezpečeného kanála v bezpečnom prostredí.

Tabuľka 5: *Hodnotenie vzoriek so známymi tajomstvami*

	Identifikácia	Využívanie
Verejnosť/nevyžaduje sa	0	NA
Obmedzené	2	NA
Citlivé	5	NA
Kritické	9	NA
Nepraktické	*	NA

Body zodpovedajúce dostupnosti "otvorených vzoriek" sú definované s prihliadnutím na počet, ochranu a kontrolu týchto otvorených vzoriek počas celého životného cyklu:

- Verejnosť:

  Otvorené vzorky: Vzorky nie sú chránené, dodávajú sa bez kontroly (bez NDA, bez kontroly zákazníka).

- Obmedzené:

  Otvorené vzorky sú chránené a kontrolované v rámci organizácie vývojára a môžu byť distribuované iným organizáciám na základe NDA.

- Citlivé:

  Počet otvorených vzoriek musí byť obmedzený, chránený a kontrolovaný v rámci organizácie vývojára. Ak sa vzorky majú distribuovať iným organizáciám, ich počet musí byť tiež obmedzený a prísne potrebný, chránený osobitnou zmluvou. Iná organizácia musí poskytnúť bezpečné prostredie, ktoré je hodnotené alebo vyhovuje zmluvným kritériám akceptovaným certifikačným orgánom.

- Kritické:

  Kritické otvorené vzorky sa nikdy nesmú šíriť mimo organizácie vývojára. V rámci organizácie vývojára musí byť ich počet obmedzený a sú k dispozícii tímom len na základe prísnej potreby. Kritické otvorené vzorky sú fyzicky a environmentálne chránené bezpečným hodnoteným fyzickým prostredím.

  Použitie "otvorenej vzorky" je silnejšie ako prístup k "vzorke so známymi tajomstvami", pretože môže umožniť získať prístup k tajomstvám, ktoré sú pre TOE klasifikované ako "Nepraktické".

Tabuľka 11: *Hodnotenie otvorených vzoriek*

	Identifikácia	Využívanie
Verejnosť/nevyžaduje sa	0	NA
Obmedzené	2	NA
Citlivé	5	NA
Kritické	9	NA

Upozorňujeme, že zdieľanie "otvorených vzoriek / vzoriek so známym tajomstvom" na účely hodnotenia s dôveryhodným systémom certifikačných orgánov a uznaných ITSEF nemá vplyv na vyššie uvedenú klasifikáciu.

V špecifických prípadoch, keď kategorizácia "otvorené vzorky/vzorky so známym tajomstvom" zodpovedá medzistupňu klasifikácie, by sa konečné hodnotenie udelené takýmto vzorkám muselo riešiť s príslušnými CB na individuálnom základe.

ITSEF musí definovať, či použitie "otvorených vzoriek" a "vzoriek so známym tajomstvom" kumuluje úsilie v čase počas hodnotenia a pridať body za každú z nich.

V prípade platforiem sa úroveň ochrany "otvorených vzoriek / vzoriek so známym tajomstvom" analyzuje počas hodnotenia základnej platformy a uvedie sa v ETR_COMP.

Formulácia "súrodenecký produkt" sa vzťahuje na produkty dostupné v danej oblasti, ktoré majú zaujímavé spoločné vlastnosti s TOE, pričom je aktivovaných menej protiopatrení a/alebo je k dispozícii viac funkcií. Tieto produkty nemusia mať implementovaných toľko protiopatrení ako TOE alebo môžu mať viac funkcií, pretože ich bezpečnostný problém je odlišný od TOE. Ak ITSEF používa funkciu
z otvorenej vzorky dodanej na hodnotenie, vývojár poskytne analýzu zaoberajúcu sa hrozbou "príbuzných produktov", ktoré tiež ponúkajú túto funkciu. V prípade, že hrozba zostáva uplatniteľná, hodnotenie týkajúce sa ochrany otvorenej vzorky (uvedené vo vyššie uvedenom zozname) sa musí upraviť tak, že sa zohľadní aj dostupnosť "súrodeneckého produktu". V prípadoch, keď by sa dostupnosť "súrodeneckého produktu" hodnotila ako verejná, ale nie je verejne známe, že "súrodenecký produkt" možno použiť ako náhradu použitej otvorenej vzorky, potom sa namiesto toho použije hodnotenie "obmedzené", aby sa pokrylo úsilie spojené s identifikáciou "súrodeneckého produktu" a jeho použitím ako náhrady otvorenej vzorky.

4.7.6 Dobré používanie otvorených vzoriek a usmernenie pre správne hodnotenie

Keďže privilegované používanie otvorených vzoriek/vzoriek so známym tajomstvom môže byť veľmi účinné na urýchlenie vyhodnotení, prináša aj úskalia, ktorým sa treba vyhnúť. Nižšie uvedené príklady poskytujú niekoľko rád a osvedčených postupov na správne vyžadovanie a používanie otvorených vzoriek / vzoriek so známymi tajomstvami.

Všeobecné pripomienky

Ako už bolo uvedené, cieľom faktora otvorená vzorka / vzorka so známymi tajomstvami je umožniť efektívne a zmysluplné hodnotenie v udržiavateľnom čase. ITSEF musí vývojárovi poskytnúť odôvodnenú žiadosť, v ktorej vysvetlí účel otvorených vzoriek / vzoriek so známymi tajomstvami vzhľadom na praktické testy, ktoré sa budú vykonávať na TOE. To zahŕňa opis cesty útoku bez použitia otvorených vzoriek / vzoriek so známymi tajomstvami, ako aj odhady dvoch rôznych hodnotení. Ak sa dosiahne dohoda medzi CB, ITSEF a vývojárom, vývojár požiada vývojára otvorenej vzorky, aby ITSEF poskytol otvorené vzorky / vzorky so známymi tajomstvami. Žiadanie otvorených vzoriek / vzoriek so známymi tajomstvami systematicky bez ohľadu na nastavenie potenciálneho útoku odvodeného
z analýzy zraniteľností sa nepovažuje za dobrú prax a bude odmietnuté.

ITSEF by mal tiež jasne rozlišovať medzi výhodami používania otvorenej vzorky počas prebiehajúceho hodnotenia a prenosnými výhodami získanými počas iných hodnotení. Ak sa prenosné výhody získali použitím otvorených vzoriek z iných hodnotení, potom sa musí preniesť aj hodnotenie tejto vzorky
a použije sa v poradí útokov. Je to dôležité najmä v prípade hodnotení podobných produktov.

Synchronizácia konkrétnych operácií, ktoré sú predmetom záujmu

Analýza zraniteľnosti si vyžaduje presnú synchronizáciu. Tú je zvyčajne oveľa jednoduchšie dosiahnuť pomocou otvorenej vzorky, ktorá umožňuje vykonávanie špecializovaného kódu. Otvorená vzorka by mohla poskytovať niektoré špecifické spúšťacie signály, ktoré indikujú napr. začiatok a/alebo koniec operácie, ktorá je predmetom záujmu.

V prípade úpravy vyhodnocovacieho firmvéru HW-TOE alebo iných zmien vnútornej konfigurácie môže odchýlka od bežnej konfigurácie produktu umožniť ďalšie synchronizačné funkcie. V tomto prípade môže byť otvorenou vzorkou aj vzorka, v ktorej boli deaktivované určité funkcie úspory energie (napr. dynamické škálovanie napätia a frekvencie), ktoré spôsobujú, že niektoré testovacie behy sú nepoužiteľné z dôvodu nepredvídateľného správania sa pri časovaní, alebo výkonnostné vylepšenia (napr. vyrovnávacia pamäť CPU).

Aktivácia dostupného vnútorného rozhrania

Niektoré TOE majú špeciálne rozhranie, ktoré môže odhaliť interné údaje na účely validácie. Ak je toto rozhranie už dostupné a prístupné bez úpravy HW, vývojár by mohol povoliť ITSEF, aby tieto údaje použil pri analýze zraniteľnosti. Mohlo by ísť napríklad o vzorku, ktorá odhaľuje rozhranie TRNG na testovanie entropie. V tomto prípade sa rozhranie, ktoré sa bežne používa na validáciu a je potrebné aj na posúdenie entropie TRNG, používa na priame pozorovanie straty entropie viac, ako je to zvyčajne možné. Tento druh vzorky sa potom hodnotí ako otvorená vzorka.

Úskalia pri hodnotení útokov s otvorenými vzorkami a bez nich

V tomto prípade uvažujme príklad chybových útokov, pri ktorých má hodnotiteľ možnosť nájsť slabé miesta vďaka otvoreným vzorkám, pričom je potrebné vypočítať hodnotenie útoku s otvorenými vzorkami a bez nich.

Bez otvorených vzoriek by útok na TOE (kombinácia platformy + aplikácie) nemusel byť realistický a mohol by byť nerealizovateľný, pretože počet TOE potrebných počas fázy identifikácie by mohol dosiahnuť stupeň "Nepraktické". Je naozaj dôležité dôkladne vyhodnotiť a neznižovať vplyv použitia otvorených vzoriek na každý faktor. V opačnom prípade by použitie otvorených vzoriek viedlo k neopodstatnenému hodnoteniu a v krajnom prípade k neúspechu produktu, ak by sa hodnotenie bez otvorených vzoriek nevykonalo správne a spravodlivo.

Postup hodnotenia útokov na učenie pod dohľadom s použitím otvorených vzoriek

V prípade profilovaných alebo kontrolovaných učebných útokov, ako sú šablónové útoky, kontrolované strojové učenie alebo kontrolované prístupy hlbokého učenia, je potrebné mať k dispozícii vzorku, v ktorej môžu byť tajné informácie, ktoré sa majú naučiť, nastavené na ľubovoľné hodnoty alebo sú známe. Ak sa to dá dosiahnuť len pomocou otvorenej vzorky, je potrebné dodržať postup opísaný na začiatku časti 4.7.5. Do úvahy sa musí vziať najmä odsek 88, pretože tieto druhy útokov nie sú praktické, ak sa nedá použiť fáza učenia útoku.

Okrem toho existuje hrozba, že fáza učenia by mohla byť vykonaná na inom produkte a použitá na útok na TOE. Preto sa na riešenie tejto hrozby musí použiť formulácia "súrodenecký produkt" a postup, ktorý bol predstavený vyššie.

Úvahy o načítavaní testovacích aplikácií pri hodnotení "otvorenej platformy

Počas hodnotení "otvorenej platformy" môže načítanie testovacích appletov pomôcť ITSEF rýchlo, dôkladne alebo presnejšie overiť robustnosť niektorých špecifických funkcií. Na tento účel sú ITSEF-u poskytnuté možnosti načítania. Body pridelené za túto výhodu je potrebné zohľadniť pri hodnotení celej cesty útoku.

Upozorňujeme, že znalosť jedného kľúča načítania "otvorenej platformy" neumožní načítať applety na všetkých produktoch založených na rovnakej platforme. Zvyčajne existuje viac ako jedna sada načítavacích kľúčov, ktoré môžu byť distribuované rôznym výrobcom.

Pre hodnotenie úplnej cesty útoku musí byť buď narušený mechanizmus načítania - a úsilie o narušenie načítavacieho mechanizmu musí byť hodnotené v rámci úplnej cesty útoku - alebo musí byť útočníkovi kompromitovaná jedna zo sád načítavacích kľúčov. V takom prípade sa pridelia body za "otvorené vzorky / vzorky so známym tajomstvom".

Počet bodov sa bude hodnotiť podľa definícií "otvorených vzoriek / vzoriek so známymi tajomstvami" a závisí od úsilia o ochranu kľúčov nakladania hodnotenej platformy, ktoré musia byť definované niektorými dodatočnými pravidlami uvedenými v bezpečnostnom zámere alebo v súvisiacom bezpečnostnom dokumente, ako je napríklad usmernenie. Napríklad, ak sa v ST alebo v usmernení k produktu neuvádza žiadne vyhlásenie o správe nakladacích kľúčov, ITSEF bude brať do úvahy faktor minimálnych kritérií (Verejné). Ak vývojár predáva presne tú istú platformu na rôznych produktoch s rôznymi úrovňami ochrany nakladacích kľúčov, musia sa uplatniť rovnaké pravidlá ako v prípade vzoriek so známym tajomstvom.

Je zrejmé, že ak ITSEF použije kľúče na načítanie, aby umožnil načítanie appletu, ktorý poskytuje len funkčné rozhrania k službám a ktorý neposkytuje žiadnu významnú výhodu pre realizáciu útoku (žiadna zmena v kategóriách faktorov, ktorá by vyvolala zmenu hodnotenia, napr. zmena intervalu pre

uplynulý čas), nebudú udelené žiadne body.

4.8 Výpočet potenciálu útoku

Tabuľka 12 identifikuje faktory uvedené v predchádzajúcich častiach a priraďuje číselné hodnoty k dvom aspektom identifikácie a zneužitia zraniteľnosti. Nahrádza tabuľku B.3 CEM pre produkty, ktoré patria do technickej doméne "Smart karty a podobné zariadenia".

Tabuľka 12: *Konečná tabuľka pre hodnotiace faktory*

Faktory	Identifikácia	Využívanie
Uplynulý čas		
< jedna hodina	0	0
< jeden deň	1	3
< jeden týždeň	2	4
< jeden mesiac	3	6
> jeden mesiac	5	8
> štyri mesiace[5656]	6	10
Nepraktické	*	*
Odbornosť		
Laik	0	0
Znalec	2	2
Odborník	5	4
Viacnásobný expert	7	6
Znalosť TOE		
Verejnosť	0	0
Obmedzené	2	2
Citlivé	4	3
Kritické	6	5
Veľmi kritické	9	*
Nepraktické	*	*
Prístup k TOE (1)		
< 10 vzoriek	0	0
< 30 vzoriek	1	2
< 100 vzoriek	2	4
> 100 vzoriek	3	6
Nepraktické	*	*
Zariadenie		
Žiadne	0	0
Štandard	1	2
Špecializované (2)	3	4
Na mieru	5	6
Viaceré na mieru	7	8
Otvorené vzorky / Vzorky so známym tajomstvom		
Verejnosť/nevyžaduje sa	0	NA

[56] Uplatniteľnosť tohto faktora je uvedená v časti 4.2.

Faktory	Identifikácia	Využívanie
Obmedzené	2	NA
Citlivé	5	NA
Kritické	9	NA
Nepraktické (len vzorky so známymi tajomstvami)	*	NA

(1) Ak sa o balíku tvrdí, že je súčasťou bezpečnosti TOE alebo k nej prispieva, potom sa môžu udeliť dodatočné body do kategórie "Prístup k TOE", ako je opísané v oddiele 4.5.1 a v tabuľke 6.

(2) Ak sa na jednotlivé kroky útoku vyžadujú jasne odlišné skúšobné zariadenia pozostávajúce zo špecializovaného vybavenia, hodnotí sa to ako na mieru. Testovacie pracoviská pre útoky bočnými kanálmi a útoky na poruchy sa zvyčajne považujú za príliš podobné a nedostatočne odlišné. V takýchto prípadoch, keď sa vyžaduje viacero podobných špecializovaných zariadení, sa to potom bude považovať za viacnásobne špecializované a k hodnoteniu sa pripočíta ďalší 1 bod.

* Označuje, že cesta útoku nie je zneužiteľná spôsobom, ktorý by bol pre útočníka užitočný. Akákoľvek hodnota * znamená vysoké hodnotenie.

Nasledujúca tabuľka nahrádza tabuľku B.4 CEM a mala by sa použiť na získanie hodnotenia zraniteľnosti.

Tabuľka 13: *Hodnotenie zraniteľnosti a odolnosti TOE*

Rozsah hodnôt*	TOE odolné voči útočníkom s potenciálom útoku:
0-15	Žiadne hodnotenie
16-20	Základné
21-24	Rozšírená základná verzia
25-30	Stredne
31 a viac	Vysoká

* konečný potenciál útoku = identifikácia + zneužitie.

5 PRÍKLADY METÓD ÚTOKU

Nasledujúce príklady zostavila skupina bezpečnostných expertov, ktorí zastupujú rôzne skupiny aktérov zapojených do vývoja, výroby, bezpečnostného hodnotenia a distribúcie produktu smart karty (dodávatelia hardvéru, dodávatelia kariet, poskytovatelia operačných systémov, hodnotiace laboratóriá, certifikačné orgány, poskytovatelia služieb).

Zbierka predstavuje „state-of-the-art“ v danom čase. Keďže „state-of-the-art“ nie je statický, tento dokument je predmetom revízie a v prípade potreby sa bude aktualizovať.

Pri hodnotení TOE je potrebné zohľadniť aspoň tieto príklady. To neznamená, že v každom prípade sa musia vykonať všetky útoky, ani by sa tento katalóg útokov nemal považovať za vyčerpávajúci zoznam. Naopak, výrobcom a laboratóriám sa odporúča, aby v rámci svojich hodnotiacich činností hľadali nové útoky a varianty útokov. Hodnotiace laboratórium, ktoré vykonáva hodnotenie, vyberie z tohto katalógu po dohode s certifikačným orgánom vhodné útoky pre každý TOE. Tento výber bude závisieť od typu TOE a pravdepodobne budú potrebné aj ďalšie testy.

V tomto dokumente je uvedený len všeobecný prehľad útokov. Podrobnejší opis a príklady nájdete v časti Certifikačné orgány. Môžu tiež poskytnúť príklady ako referenciu pre hodnotenie.

5.1 Fyzické útoky

5.1.1 Všeobecný opis

Mikroelektronické nástroje umožňujú prístup k IC alebo jeho úpravu odstránením alebo pridaním materiálu (leptanie, FIB atď.). V závislosti od nástroja a jeho použitia je pre útočníka zaujímavé získať

vnútorné signály alebo manipulovať so spojmi vo vnútri integrovaného obvodu pridaním alebo prerezaním vodičov vo vnútri kremíka.

V závislosti od technológie pamäte by sa k pamätiam mohlo pristupovať aj fyzicky, a to na čítanie alebo nastavovanie bitových hodnôt.

5.1.2 Vplyv na TOE

Útok je zameraný na integrovaný obvod a často je nezávislý od vstavaného softvéru (t. j. môže sa použiť na akýkoľvek vstavaný softvér a je nezávislý od softvérových protiopatrení).

Hlavné vplyvy sú:

- prístup k tajným údajom, ako sú kryptografické kľúče (extrakciou vnútorných signálov).
- Odpojenie bezpečnostných prvkov IC s cieľom uľahčiť ďalší útok (DPA, perturbácia)
- Vynútenie vnútorných signálov
- Dokonca aj neznáme signály by sa mohli použiť na vykonanie niektorých útokov

Potenciál využitia týchto techník je rôznorodý a musí sa starostlivo zvážiť v kontexte každého hodnotenia.

5.2 Prekonanie senzorov a filtrov

5.2.1 Všeobecný opis

Tento útok zahŕňa spôsoby deaktivácie alebo zabránenia rôznym typom senzorov, ktoré môže IC používať na monitorovanie podmienok prostredia a na ochranu pred podmienkami, ktoré by mohli ohroziť správnu činnosť TOE. Hardvér alebo softvér môže využívať výstupy zo snímačov na prijatie opatrení na ochranu TOE.

Senzory a filtre môžu byť prekonané:

- Odpojenie
- Zmena správania snímača
- Zistenie medzier v pokrytí monitorovaného stavu (napr. napätia) alebo v načasovaní monitorovania.

Senzory môžu byť zneužité aj na to, aby sa aktivácia senzora využila ako krok v útoku. Toto zneužitie senzorov je samostatným útokom.

Medzi rôzne typy senzorov a filtrov patria:

- Napätie (napr. vysoké napätie alebo napäťová špička)
- Frekvencia (napr. vysoká frekvencia alebo frekvenčný skok)
- Teplota
- Svetlo (alebo iné žiarenie)

5.2.2 Vplyv na TOE

Pri tomto útoku už nie je možné zaručiť správnu činnosť čipu mimo bezpečných prevádzkových podmienok. Vplyv prevádzky za týchto podmienok môže byť rôzneho druhu. Napríklad:

- Obsah pamäte alebo registrov môže byť poškodený
- Tok programu sa môže zmeniť
- Môžu sa vyskytnúť poruchy operácií (napr. CPU, koprocesory, RNG)
- Zmena prevádzkového režimu a/alebo parametrov (napr. z režimu používateľa na režim supervízora)
- Zmena iných prevádzkových vlastností (napr. zmena správania pri úniku; umožnenie iných útokov, ako je zmrazenie RAM, skenovanie elektrónovým lúčom).

Ak čip vráti nesprávne kryptografické výsledky, môže to umožniť útok DFA, pozri časť **Chyba! Nenašiel sa referenčný zdroj.**. Ďalšie dôsledky sú opísané v časti Všeobecné účinky porúch v časti **Error!**

Referenčný zdroj nebol nájdený.

5.3 Perturbačné útoky

5.3.1 Všeobecný opis

Perturbačné útoky menia normálne správanie integrovaného obvodu s cieľom vytvoriť zneužiteľnú chybu vo fungovaní TOE. Správanie sa zvyčajne mení buď prevádzkovaním integrovaného obvodu mimo jeho zamýšľaného prevádzkového prostredia (zvyčajne charakterizovaného z hľadiska teploty, Vcc a externe dodávanej hodinovej frekvencie), alebo použitím jedného alebo viacerých externých zdrojov energie počas prevádzky integrovaného obvodu. Tieto zdroje energie sa môžu aplikovať v rôznych časoch a/alebo na rôznych miestach integrovaného obvodu.

Útoky sa zameriavajú na ochranu mechanizmov a zvyčajne zahŕňajú tieto prvky:

- Zníženie sily kryptografických operácií,
- Manipulácia s mechanizmami ochrany pamäte,
- Ovplyvnenie nevolatilných hodnôt monotónneho počítadla.

Vytváranie chýb možno použiť na obnovenie kľúčov alebo otvoreného textu, na zmenu výsledkov overovania, ako je autentizácia alebo kontrola stavu životného cyklu, na zmenu toku programu, na zabezpečenie neoprávneného prístupu do chránenej pamäte alebo na umožnenie útokov typu rollback a replay.

Chyba v sekcii! **Reference source not found. sa** zaoberá skôr metódami na vyvolanie zmysluplných porúch, zatiaľ čo sekcia **Error! Reference source not found.** opisuje, ako sa tieto indukované poruchy môžu použiť na extrakciu kľúčov z kryptografických operácií.

5.3.2 Vplyv na TOE

Perturbancie možno aplikovať buď na hardvérovú TOE (integrovaný obvod), alebo na softvérový/zložený TOE (operačný systém alebo aplikáciu spustenú na integrovanom obvode).

Pre útočníkov sú typické tieto vonkajšie účinky na integrovaný obvod so softvérovou aplikáciou:

- Úprava hodnoty načítanej z pamäte počas operácie čítania: Hodnota uchovávaná v pamäti sa nemení, ale hodnota, ktorá sa dostane do cieľa (napr. CPU alebo koprocesor), sa mení. Môže sa to týkať údajov alebo informácií o adrese.
- Úprava hodnoty, ktorá je uložená vo volatilnej pamäti. Modifikovaná hodnota je platná, kým nie je prepísaná novou hodnotou, a preto by mohla byť použitá na ovplyvnenie výsledkov spracovania alebo bezpečnostnej politiky zariadenia.
- Úprava hodnôt nevolatilného monotónneho počítadla, ktoré sa používa na zabezpečenie čerstvosti údajov. Závada alebo zníženie napätia napájacieho zdroja pri inkrementácii čítača môže mať za následok okrajovú hodnotu, ktorá dáva možnosť vrátiť čítač späť, a tak umožňuje opakované útoky (ak nie sú implementované žiadne špeciálne protiopatrenia, ako je kontrolný súčet čítača).
- Zmena vlastností generovaných náhodných čísel (napr. vynútenie, aby na výstupe RNG boli všetky 1) - pozri časť **Chyba! Referenčný zdroj nebol nájdený.** "Útoky na RNG", kde nájdete viac informácií o útokoch na generátory náhodných čísel.
- Modifikácia toku programu: tok programu je modifikovaný a je možné pozorovať rôzne efekty:
  - Preskočenie pokynu
  - Nahradenie pokynu iným (neškodným) pokynom
  - Invertovanie testu
  - Generovanie skoku
  - Generovanie chýb výpočtu

Je potrebné poznamenať, že je pomerne ľahké spôsobiť chyby v komunikácii, pri ktorých sú konečné údaje vrátené IC modifikované. Tieto typy chýb však vo všeobecnosti nie sú pre útočníka užitočné, pretože indikujú len rovnaký typ chýb, aké sa môžu prirodzene vyskytnúť v komunikačnom médiu: Neovplyvnili správanie IC počas vykonávania operácie citlivej z hľadiska bezpečnosti (napr. kryptografický výpočet alebo rozhodnutie o riadení prístupu).

Rozsah možných techník rušenia je veľký a zvyčajne podlieha rôznym parametrom pre každú techniku. Tento veľký rozsah a ďalšie komplikácie spojené s kombináciou perturbácií znamenajú, že

perturbácia zvyčajne prebieha tak, že sa skúma, aké typy perturbácií spôsobujú nejaký pozorovateľný účinok,
a potom sa táto technika spresňuje tak z hľadiska parametrov perturbácie (napr. malé zmeny výkonu, umiestnenia alebo časovania), ako aj z hľadiska toho, ktoré časti softvéru sú napadnuté. Ak sa napríklad dá zistiť, že poruchy menia hodnotu jednotlivých bitov v registri, môže to byť užitočné najmä vtedy, ak softvér v TOE používa na bezpečnostné rozhodnutia jednobitové príznaky. Aplikačný kontext (t. j. ako sa TOE používa v zamýšľanom prevádzkovom prostredí) môže určiť, či účinok narušenia musí byť presný a istý, alebo či sa na útok na TOE môže použiť aj menej istá modifikácia (napr. jedna modifikácia z 10 alebo 100 pokusov).

5.4 Získavanie kľúčov pomocou FA

5.4.1 Všeobecný opis

Pomocou analýzy chýb (FA) chce útočník získať informácie o tajnom kľúči analýzou rozdielu medzi správnym a chybným kryptografickým výstupom alebo analýzou rôznych chybných kryptografických výstupov.

Táto metóda útoku vyžaduje analýzu chybných výstupov. Takýto chybný výstup by sa mohol získať vyvolaním fyzickej poruchy na zariadení počas príslušného kryptografického výpočtu, prípadne počas manipulácie s parametrami algoritmu. Takáto porucha sa môže vytvoriť buď neinvazívnymi (napríklad porucha napájania), alebo poloinvazívnymi (typicky laserom) technikami.

Podľa teórie tohto útoku by mala chyba injektovaná počas spracovania zariadenia spĺňať špecifické požiadavky, aby viedla k zneužiteľnému výstupu. Pri väčšine útokov sú tieto požiadavky založené na presnej synchronizácii a zároveň na očakávanej hodnote ako dôsledku poruchy. Nedostatočná presnosť týchto požiadaviek môže spôsobiť, že analýza na obnovenie kľúča bude oveľa zložitejšia.

Z praktického hľadiska možno proces uskutočnenia takéhoto útoku rozdeliť do nasledujúcich fáz:

- Hľadanie vhodného spôsobu vstrekovania poruchy
- V závislosti od kryptografického algoritmu, na ktorý sa má útočiť, nastavenie viac alebo menej presnej synchronizačnej techniky.
- Vyvolanie chyby (chýb) počas vykonávania zariadenia a následné zhromažďovanie príslušných chybných šifrových textov
- Analýza rozdielov medzi chybnými šifrovými textami a správnym šifrovým textom (prípadne otvoreným textom).

5.4.2 Vplyv na TOE

Tento útok sa môže uskutočniť neinvazívnym alebo invazívnym spôsobom. Neinvazívna metóda (power glitching) zabraňuje fyzickému poškodeniu. Invazívna metóda si vyžaduje, aby útočník fyzicky pripravil TOE na uľahčenie použitia svetla na časti TOE.

DFA dokáže prelomiť kryptografické kľúčové systémy a umožňuje získať napríklad kľúče DES, 3DES a RSA spustením zariadenia za neobvyklých fyzických podmienok. Útočník musí v správnom čase a na správnom mieste vniesť chybu, aby využil chybné kryptografické výstupy.

Keďže kľúče a kód sú zvyčajne prítomné v pamäti EEPROM, môže byť ťažké náhodne meniť bity bez toho, aby sa zrútil celý systém namiesto získania požadovaných chybných výsledkov, hoci zmena kódu môže tiež priniesť výsledky. Na určenie najlepšieho miesta a času na vnesenie chyby môžu byť užitočné aj iné techniky; napríklad analýza spotreby energie na určenie času, kedy dochádza ku kryptografickým výpočtom.

5.5 Útoky bočným kanálom - neinvazívne získavanie tajných údajov

5.5.1 Všeobecný opis

Útoky bočnými kanálmi sú zamerané na tajné informácie, ktoré unikajú neúmyselnými kanálmi v konkrétnej, t. j. fyzickej implementácii algoritmu. Tieto kanály sú spojené s fyzikálnymi vplyvmi, ako

sú časové charakteristiky, spotreba energie alebo elektromagnetické žiarenie.

SPA a DPA sú skratky pre "Simple" (jednoduchá) a "Differential Power Analysis" (diferenciálna analýza výkonu) a ich cieľom je využiť informácie, ktoré unikajú prostredníctvom charakteristických zmien
v spotrebe energie elektronických komponentov, zvyčajne bez poškodenia TOE. Aj keď existujú rôzne úrovne zložitosti, spotrebu energie zariadenia možno v podstate jednoducho merať pomocou digitálneho vzorkovacieho osciloskopu a rezistora umiestneného v sérii so zariadením.

Keď je integrovaný obvod v prevádzke, každý jednotlivý prvok vyžaruje elektromagnetické žiarenie rovnako ako akýkoľvek iný vodič, ktorým preteká elektrický prúd. Tak, ako sa tento prúd mení v závislosti od spracovávaných údajov, mení sa aj elektromagnetické žiarenie emitované TOE. Útoky elektromagnetickej analýzy (EMA) sú zamerané na tento variant úniku informácií. Tieto útoky sa niekedy označujú ako SEMA (Simple Electromagnetic Analysis) alebo DEMA (Differential Electromagnetic Analysis). Môžu využívať emisie z celého integrovaného obvodu (chip-EMA) alebo sa môžu zameriavať na emisie z konkrétnych oblastí matrice, kde sa nachádzajú kritické komponenty (local-EMA).

Experimentálne dôkazy ukazujú, že elektromagnetické údaje (najmä z lokalizovaných oblastí matrice) sa môžu dosť líšiť od údajov o výkonovej stope, a preto môžu byť integrované obvody, ktoré sú chránené proti analýze výkonu, zraniteľné voči EMA.

V záujme jednotnosti budú v ďalšom texte SPA a DPA označovať nielen útoky založené na meraní spotreby energie, ale budú sa vzťahovať aj na ich "príbuzných" v oblasti elektromagnetických útokov, ak nie je uvedené inak.

Implementácie, ktoré obsahujú protiopatrenia, ako je booleovské maskovanie, ktoré odolávajú DPA prvého rádu, môžu byť zraniteľné voči DPA vyššieho rádu. Tento útok vyžaduje, aby útočník dokázal korelovať viac ako jeden dátový bod na výpočet TOE pomocou hypotéz o prechodných stavoch, ktoré závisia od častí tajného kľúča.

Kombinovaná štatistická analýza pre DPA vyššieho rádu môže byť založená na zosúladených meraniach toho istého bočného kanála v rôznych časoch alebo na zosúladených simultánnych meraniach rôznych kanálov, napríklad spotreby energie a elektromagnetického vyžarovania zariadenia počas výpočtu.

Výsledok útoku bočným kanálom môže byť tak jednoduchý, ako je nájdenie charakteristického spúšťacieho bodu pre spustenie iných útokov (napríklad DFA), alebo tak úplný, ako je tajný kľúč použitý v kryptografickej operácii. Jeho cieľom môže byť aj získanie iných tajných údajov, ako sú PIN kódy alebo náhodné čísla vygenerované na použitie ako tajomstvo, alebo dokonca opkód kódu vykonávaného na TOE. V závislosti od cieľa útoku môže zahŕňať širokú škálu metód od priamej interpretácie zaznamenaného signálu až po komplexnú analýzu signálu pomocou štatistických metód. V druhom prípade bude počiatočné filtrovanie použité na analýzu signálu vo všeobecnosti závisieť od typu merania (t. j. spotreba energie alebo elektromagnetické žiarenie), ale matematika na získanie tajných informácií je nakoniec do veľkej miery rovnaká.

5.5.2 Vplyv na TOE

Podstata útokov SPA a (vyššieho rádu) DPA spočíva v tom, že ich možno v zásade použiť na akýkoľvek kryptografický algoritmus - buď samostatne, napr. na získanie tajných kľúčov alebo PIN kódov, alebo ako súčasť zloženého útoku. Okrem toho môže SPA slúžiť ako odrazový mostík pre ďalšie útoky. SPA sa môže napríklad použiť na zistenie kritickej operácie zápisu do EEPROM, ktorú je potrebné zachytiť. Analýza SPA sa môže vykonať aj ako súčasť časového útoku (napr. v algoritme RSA typu "štvorec
a násobenie") alebo na odvodenie toho, ktorá vetva podmieneného skoku bola vykonaná v toku programu. Alebo sa môže jednoducho použiť ako prvý krok na identifikáciu protiopatrení proti útokom bočnými kanálmi, ktoré je potrebné prekonať. Napokon, útok SPA by sa mohol použiť na určenie správneho spúšťacieho bodu pre následný glitch alebo light útok, alebo ako pomôcka na lokalizáciu vhodného časového okna pre fyzický sondážny útok

Útok DPA (alebo šablóny) nemusí byť úplne úspešný, aby sa stal nebezpečným. Pri vhodnej stratégii vyhľadávania kľúčov, ktorá zohľadňuje nedokonalé výsledky DPA, ako je uvedené ďalej, môže stačiť získať len časť tajného kľúča pomocou DPA a zvyšok získať metódami hrubej sily.

Implementácie, ktoré odolávajú útokom DPA, môžu byť stále zraniteľné voči útokom DPA vyššieho rádu, pretože tento typ útoku využíva dodatočné informácie, ktoré sa pri štandardnom útoku neberú do úvahy. Samozrejme, algoritmy, ktoré sú zraniteľné voči DPA prvého rádu, sú zraniteľné aj voči DPA vyššieho rádu. Zdá sa, že DPA vyššieho rádu je obzvlášť vhodný na riešenie booleovského a aritmetického maskovania/oslepovania symetrických algoritmov. Na druhej strane sa zdá, že rozšírenie DPA vyššieho rádu na algoritmy s verejným kľúčom (asymetrické) je veľmi zložité, a to z dôvodu široko uplatňovaných protiopatrení na zaslepenie, ktoré využívajú algebraické transformácie počas výpočtu, ktoré sú úplne odlišné od bežného maskovania.

Analýza výkonu, ako aj útoky EMA sa môžu vykonávať pre hardvérovú TOE (integrovaný obvod) alebo softvérový/zložený TOE (operačný systém alebo aplikácia spustená na integrovanom obvode). Niektoré protiopatrenia už môžu existovať v hardvérovom TOE, zatiaľ čo iné sa pridajú neskôr v softvéri. Spôsob, akým softvér využíva funkcie integrovaného obvodu, tak môže mať rozhodujúci vplyv na jeho zraniteľnosť voči tomuto typu útoku.

5.6 Využívanie funkcií testu

5.6.1 Všeobecný opis

Cieľom útoku je vstúpiť do testovacieho režimu IC a poskytnúť tak základ pre ďalšie útoky.

Tieto ďalšie útoky môžu viesť napríklad k odhaleniu alebo poškodeniu obsahu pamäte, zmene stavu životného cyklu alebo deaktivácii bezpečnostných funkcií. Keďže to však závisí od možností testovacieho režimu, podrobnosti o týchto ďalších útokoch tu neuvažujeme.

5.6.2 Vplyv na TOE

V dôsledku úspešného prístupu do testovacieho režimu IC môže byť útočník schopný:

- Odčítanie obsahu nevolatilnej pamäte pomocou testovacích funkcií. Implementácia testovacích funkcií môže mať vplyv na použiteľnosť načítaných používateľských údajov.
- Znovu nakonfigurujte údaje životného cyklu alebo počítadlá chýb pomocou testovacej funkcie. Útočník tak môže pokračovať v analýze na tom istom zariadení, aj keď by ho zmena stavu životného cyklu inak zastavila.

5.7 Útoky na RNG

5.7.1 Všeobecný opis

Útoky na RNG sa vo všeobecnosti zameriavajú na získanie schopnosti predpovedať výstup RNG (napr. zníženie výstupnej entropie), čo môže zahŕňať:

- minulé hodnoty výstupu RNG (vzhľadom na dané a prípadne známe aktuálne hodnoty),
- budúce hodnoty výstupu RNG (vzhľadom na prípadne známe minulé a súčasné hodnoty),
- vynútiť výstup na špecifické správanie, čo vedie k:
  - o známych hodnôt (preto umožňuje aj predikciu výstupu),
  - o neznáme, ale fixné hodnoty (zníženie entropie na 0 na limite),
  - o opakovanie neznámych hodnôt buď pre rôzne behy jedného RNG, alebo pre behy dvoch alebo viacerých RNG (klonovanie) .

RNG, o ktorom sa tu uvažuje, môže byť jeden z týchto typov[57]:

- true RNG (TRNG), ktorých výstup je generovaný ľubovoľným druhom vzorkovania inherentne náhodných fyzikálnych procesov,
- pseudo RNG (PRNG), ktorého výstup je generovaný ľubovoľným druhom algoritmického spracovania (algoritmus je vo všeobecnosti stavový, pričom počiatočný stav (seed) môže byť generovaný TRNG),
- hybridný RNG (HRNG), ktorý sa skladá z TRNG a PRNG s rôznymi schémami aktualizácie stavu. Aplikovateľné metódy útoku sa líšia podľa typu RNG.

[57] V kontexte smart kariet sa RNG založené na niektorých meraniach prostredia nepovažujú za relevantné.

Pravý RNG môže byť napadnutý[58]:

- trvalý alebo prechodný vplyv prevádzkových podmienok (napr. napätie, frekvencia, teplota, svetlo)
- neinvazívne využívanie úniku signálu (napr. signálu na vonkajších elektrických rozhraniach)
- fyzická manipulácia s obvodmi (zastavenie operácie, vynútenie úrovne linky, modifikácia a/alebo klonovanie správania, odpojenie zdroja entropie)
- odpočúvanie vnútorných signálov (kompromitácia vnútorných stavov) Pseudo RNG môže byť napadnutý:
- priamy (kryptografický) útok na deterministický prechod stavu a výstupnú funkciu (napr. na základe známych predchádzajúcich výstupov RNG)
- nepriamy útok na proces výpočtu prechodov medzi stavmi pomocou informácií z bočného kanála (t. j. únik informácií na vonkajších elektrických rozhraniach)
- útok na priebeh spracovania (modifikácia výsledkov)
- útok na semeno (zabránenie opätovnému nasadeniu, vynútenie semena na pevnú známu alebo neznámu (ale reprodukovateľnú) hodnotu, kompromitácia hodnoty semena)
- prekročenie limitu výstupného objemu RNG (napr. prinútenie RNG k opakovaniu hodnôt alebo k vytvoreniu dostatočného výstupu, ktorý umožní útočníkovi riešiť rovnice a na základe riešenia predpovedať výstup)

Útoky na hybridné RNG budú vo všeobecnosti kombináciou útokov na TRNG a PRNG.

Od všetkých návrhov RNG možno očakávať, že budú vyžadovať aj testovacie postupy proti útokom, ako sú uvedené vyššie. Uvedená analýza neberie do úvahy útoky na testovacie postupy, pretože takéto útoky budú dostatočne pokryté všeobecnejším scenárom útokov na softvér. Pozorujte, že testovacie postupy môžu byť predmetom útoku, ako je SPA/DFA, na odhalenie výstupných hodnôt RNG.

5.7.2 Vplyv na TOE

Úspešný útok na RNG bude mať za následok narušenie bezpečnostných mechanizmov čipu, ktoré sa spoliehajú na náhodnosť RNG. Týmito mechanizmami môžu byť protiopatrenia DPA/SPA, testovanie senzorov, kontrola integrity aktívneho štítu, šifrovanie zbernice a/alebo pamäte a šifrovanie. Aplikačný softvér je takýmito útokmi ovplyvnený nepriamo, napr. ak útočník vypne senzory a súvisiace testy, potom to vytvorí ďalšie možnosti útoku.

Vývojár softvéru sa môže spoľahnúť na možnosti hardvérovej platformy na testovanie RNG a použiť ich alebo môže na základe týchto možností implementovať a vykonať dodatočné testy. Vývojár softvéru môže implementovať aj testy na opakovanie výstupu RNG, ale pokrytie a uskutočniteľnosť takýchto testov môže závisieť od implementácie a zdá sa, že je to problém. Útoku na klonovanie výstupu RNG na rôznych inštanciách RNG sa nedá čeliť testami, preto je potrebné navrhnúť iné vhodné mechanizmy.

V prípade TRNG by sa mali vykonať dostatočné testy (buď samotnou platformou čipu, alebo vývojárom softvéru). AIS31[59] je príkladom metodiky na posúdenie efektívnosti testovacích mechanizmov.
V prípade PRNG je potrebné vynaložiť osobitné úsilie na ochranu seedu a algoritmu z hľadiska integrity
a dôvernosti. Toto úsilie sa týka všeobecných aspektov softvéru a ochrany údajov a v tejto časti sa ním nebudeme ďalej zaoberať.

5.8 Nesprávne vytvorené aplikácie Java Card

5.8.1 Všeobecný opis

Tento logický útok spočíva v spustení nesprávne vytvorených aplikácií, t. j. škodlivých aplikácií, ktoré sa skladajú z nelegálnych sekvencií inštrukcií bajtového kódu alebo ktoré nemajú platné parametre bajtového kódu.

Tento príklad sa vzťahuje len na karty Java (hoci môžu existovať ekvivalentné útoky pre iné operačné systémy). Ak sa tento útok nekombinuje s iným útokom, ako je napríklad obídenie autentizácie, musí

[58] Predpokladá sa, že priamy útok na pravé RNG (t. j. uhádnutie hodnoty) nie je pre žiadneho útočníka uskutočniteľný.
[59] Triedy funkcionalít a metodika hodnotenia fyzického generátora náhodných čísel, verzia 3, 15.05.2013 (BSI).

sa použiť na karty Java so známymi kľúčmi na načítanie (tie by sa mohli považovať za otvorené vzorky). Okrem toho, ak karta obsahuje zabudovaný overovač bajtového kódu, musí byť tento overovač vypnutý. Žiadna iná špecifická konfigurácia sa nevyžaduje.

Nesprávne formulované aplikácie vykonávajú sekvenciu bajtového kódu, ktorá porušuje pravidlá Javy. Neformálne aplikácie sa zvyčajne vytvárajú zo štandardných aplikácií, v ktorých sa ručne upravuje bajtový kód. To znamená, že takéto zle formulované aplikácie nemôžu byť výstupom normálneho generátora súborov CAP. V dôsledku toho väčšina platforiem Java Card nevynucuje pravidlá počas vykonávania aplikácií.

5.8.2 Vplyv na TOE

V najúspešnejších prípadoch môže útočník získať informácie (napr. výpis pamäte), vykonávať funkcie, ktoré zvyčajne vyžadujú špecifické oprávnenia, alebo sa dokonca prepnúť do kontextu poskytujúceho úplnú kontrolu nad kartou (kontext JCRE).

5.9 Softvérové útoky

Väčšina príkladov útokov v tomto dokumente si vyžaduje hardvérové kroky útoku pre celý útok alebo jeho časť. Je však zrejmé, že existuje mnoho relevantných útokov, ktoré sa dajú uskutočniť len na základe softvéru. Táto časť sa zaoberá niektorými z týchto útokov. V mnohých prípadoch sa softvérové útoky začínajú analýzou zdrojového kódu alebo rozsiahlym testovaním softvéru. Obidve sa zvyčajne kombinujú pre väčšiu účinnosť na pokrytie detekcie zraniteľností.

Vo všeobecnosti je dôležité poznamenať, že väčšina softvérových útokov vzniká:

- chyby (bugy) v TOE, či už v návrhu alebo implementácii;
- nekonzistentnosť, nedostatky alebo nejednoznačnosť v špecifikácii alebo normách;
- využívanie citlivých alebo kritických poznatkov získaných v TOE.

V prípade chýb (bugov) bude mať spravidla za následok nesplnenie požiadaviek jednej (alebo viacerých) z skupín ADV. Preto chyba tohto druhu spôsobí, že TOE nevyhovie hodnoteniu (alebo, čo je bežnejšie, bude vyžadovať úpravu TOE na odstránenie chyby).

V prípade problémov pochádzajúcich zo špecifikácie alebo noriem môže byť úprava špecifikácie návrhu nedostatočná na splnenie bezpečnostných cieľov TOE: napríklad samotná špecifikácia protokolu môže obsahovať kritické zraniteľnosti. To by tiež spôsobilo, že TOE by nevyhovelo hodnoteniu.

V prípade zneužitia znalostí TOE môže mať útočník prístup napríklad k autentizačným údajom, čo mu umožní využívať niektoré funkcie prístupné len vývojárom. Útočník môže napríklad používať proprietárne administračné príkazy vyžadujúce autentizáciu.

V tejto časti je preto uvedených niekoľko krokov útoku, ktoré možno použiť na odhalenie chýb softvéru. Ak sa objaví nejaká chyba, musí sa opraviť, ak má TOE prejsť hodnotením.

V nasledujúcom texte sa najprv zaoberáme krokom zhromažďovania informácií, ktorý môže byť relevantný pre viacero rôznych typov útokov. Predstavíme päť konkrétnych techník útoku, ktoré môžu využívať zraniteľnosti softvéru:

- Zhromažďovanie informácií o príkazoch
- Priame útoky na protokol
- Man-in-the-middle a replay útoky
- Pretečenie vyrovnávacej pamäte alebo pretečenie zásobníka
- Prepínanie komunikačných rozhraní

Útoky súvisiace s izoláciou aplikácií (načítanie, firewally atď.) nie sú opísané v tejto časti, ale v časti **Chyba! Nenašiel sa zdroj odkazu. "Chyba! Referenčný zdroj nebol nájdený."**

Útoky sú logickej povahy, na ich vykonanie je potrebné mať:

- prostriedok na počúvanie sekvencií správ (čítačka, analyzátor prevádzky)
- prostriedky na vytváranie správ (informácie o externom API, generátor vzorov)
- prostriedok na prerušenie správ bez detekcie (závisí od protokolu)
- prostriedok na analýzu zdrojového kódu pomocou nástroja

- prostriedok na vytváranie aplikácií
- prostriedok na zostavenie a spustenie väčších testovacích sád

Testovacie prostredie teda môže pozostávať z:

- POČÍTAČA
- čítačky smart kariet
- testovacieho softvéru na písanie a vykonávanie testovacích skriptov a komunikáciu so smart kartou
- nástroja na analýzu zdrojového kódu (na testovanie bielej skrinky alebo analýzu výpisu pamäte).
- analyzátora protokolov (na reverzné inžinierstvo komunikačných protokolov)
- rozvojového prostredia (na vývoj aplikácií, ktoré sa majú nahrať do TOE).

Nastavenie testovacieho prostredia a identifikácia útoku by sa mohli uskutočniť v pomerne krátkom čase, ako je uvedené nižšie:

- nástroje sa považujú za štandardné vybavenie (niektoré softvérové nástroje sú dokonca dostupné ako freeware na internete),
- príkazy sú často štandardom ISO, a preto sú verejne známe:
- Používanie nástrojov a prepojenie so zariadením na vytváranie testovacích skriptov si môže vyžadovať určitý čas na prípravu,
- ak je súbor príkazov proprietárny, sú potrebné o niečo vyššie odborné znalosti, pretože komunikácia sa musí interpretovať.

Všimnite si, že ak je úroveň záruky založená na princípe "security by obscurity", nepovažuje sa za platnú obranu proti útoku.

Odbornosť útočníka môže byť odborná alebo expertná a môže byť aj viacnásobne odborná, najmä pri kombinácii veľmi presných oblastí odbornosti (napríklad Java Card a kryptografia).

5.9.1 Všeobecný opis

Cieľom tohto typu útoku je získať neoprávnený prístup k údajom uloženým na smart karte a vykonať operácie, ktoré nezodpovedajú aktuálnemu stavu životného cyklu spracúvaných dátových objektov alebo operačného systému. Cieľom takéhoto útoku je napríklad čítanie alebo zmena personalizovaných údajov, ktoré sa nachádzajú na karte, alebo je jeho cieľom vykonať ďalšiu (neautorizovanú) inicializáciu alebo personalizáciu produktu.

Neoprávnený prístup k údajom uloženým na smart karte možno získať rôznymi technikami:

- Vydávanie sa za druhú stranu komunikácie (tzv. man-in-the-middle),
- pomocou časových rozdielov (zachytávaním a prehrávaním príkazov),
- skúšanie variantov príkazov (buď úprava platných príkazov, alebo nájdenie nedefinovaných príkazov),
- manipulácia so samotnými pravidlami prístupu,
- obchádzanie alebo manipulácia s požiadavkami a vyhodnocovaním pravidiel prístupu počas vykonávania programu.

Vykonávanie príkazov, ktoré nie sú povolené v aktuálnom stave životného cyklu operačného systému alebo dátového objektu, možno tiež získať rôznymi technikami:

- manipulácia s aktuálnym stavom životného cyklu,
- obchádzanie alebo manipulácia so žiadosťou a
- vyhodnotenie aktuálneho stavu životného cyklu počas vykonávania programu a
- skúšanie variantov príkazov (buď úprava platných príkazov, alebo nájdenie nedefinovaných príkazov).

Manipulácia s informáciami o stave životného cyklu a pravidlami prístupu si vyžaduje logický útok na smart kartu a jej operačný systém a aplikácie. Obchádzanie a manipulácia s požiadavkou
a vyhodnocovaním informácií o stave životného cyklu a pravidiel prístupu je založené na manipulácii so zamýšľaným tokom programu, ktorú možno dosiahnuť logickými prostriedkami (fyzické prostriedky sa
v tomto príklade neuvažujú).

Vo zvyšku tejto časti sú opísané rôzne typy techník softvérových útokov, ktoré treba považovať za základné stavebné prvky: úplná cesta útoku je zvyčajne kombináciou rôznych techník.

5.9.2 Zhromažďovanie informácií o príkazoch

5.9.2.1 Prehľad

Komunikačné protokoly sú vo svojej podstate náchylné na únik informácií. Tento nežiaduci efekt je dôsledkom toho, že sú navrhnuté na odovzdávanie informácií. Tento typ útoku sa snaží využiť protokoly spôsobom, ktorý nebol zamýšľaný tvorcom protokolu, a to tak, že najprv zhromažďuje informácie
a potom túto komunikáciu zmení s cieľom získať tajné údaje alebo iné zdroje.

Krok útoku je zvyčajne neinvazívna technika, ktorej cieľom je získať informácie o komunikačných príkazoch, ktoré smart karta podporuje, alebo využiť informácie zo sekvencií správ na umožnenie ďalších útokov. Treba poznamenať, že sa predpokladá, že ide o informácie, ktoré nie sú obsiahnuté v konštrukčných dokumentoch (napr. nedokumentované odpovede na príkazy). Tieto informácie potom môžu útočníkovi umožniť modifikovať interakciu alebo zverejniť informácie (napr. údaje používateľa alebo kľúče) s využitím slabých miest v implementácii softvéru. Tento krok útoku zvyčajne nepredstavuje úplnú cestu útoku vedúcu k získaniu tajných údajov, hoci v špecifických prípadoch sa tak môže stať (odhalenie tajných údajov týmto spôsobom by sa vo všeobecnosti považovalo za dostatočnú zraniteľnosť, ktorá by spôsobila neúspešné vyhodnotenie TOE[60]).

Tento krok útoku vedie k získaniu informácií o fungovaní TOE. Získané informácie sa analyzujú s cieľom zistiť, či sa dajú použiť na útok s cieľom získať tajné údaje z TOE pomocou niektorého z ďalších mechanizmov opísaných v tomto dokumente. Útočník vie, že útok bol úspešný, na základe analýzy odpovedí, ktoré smart karta poskytuje počas komunikácie.

5.9.2.2 Popisy krokov útoku

Pozorovanie sekvencií správ

Pozorovanie sekvencií správ môže viesť k:

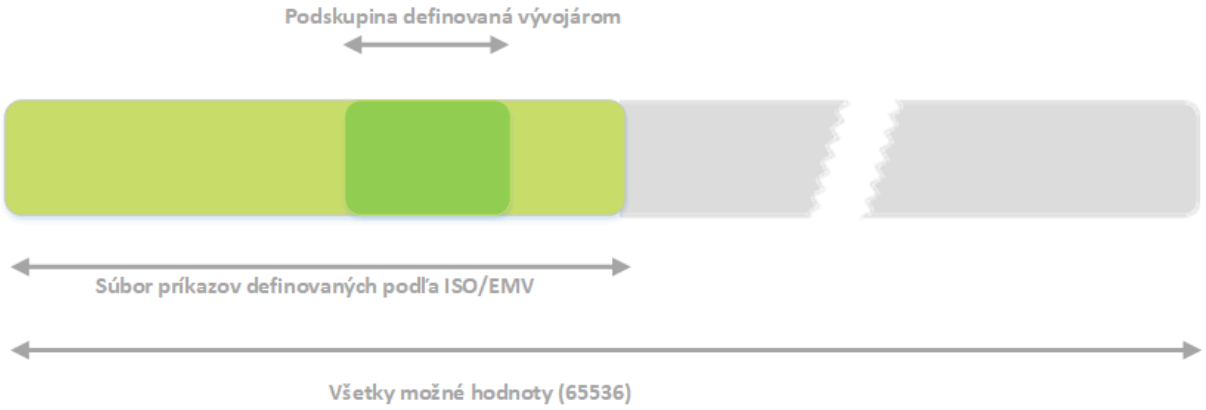
- získavanie informácií o neznámom protokole (napr. ak špecifikácia rozhrania nie je verejná) na prípravu útoku
- získavanie informácií o neznámych vnútorných štruktúrach produktu (zvyčajne dátové štruktúry v softvéri) na prípravu útoku.
- zverejňovanie informácií, kľúčov alebo bezpečnostných atribútov počas operácií importu alebo exportu.
- sledovanie aktivity produktu alebo správania používateľa (napr. na umožnenie útoku na opakovanie).

Takéto pozorovanie je možné len pri zachytení platnej komunikácie medzi smart kartou a terminálom. Ak útočník takúto možnosť nemá, musí pristúpiť k ďalšiemu kroku "Vyhľadávanie príkazov".

Vyhľadávanie príkazov

Celkový počet hodnôt, ktoré môže smart karta komunikovať pomocou typického protokolu, ako je ISO 7816 T=1, je 2^{16} alebo 65536 rôznych príkazov. Z tejto množiny ISO definovalo podmnožinu platných príkazov. A z tejto množiny ISO vývojár definuje podmnožinu a dokumentuje tieto príkazy ako platné príkazy pre túto kartu.

[60] V závislosti od rozsahu hodnotenia a prostredia môžu nastať situácie, keď sa takéto vystavenie informácií akceptuje, napr. v protokole určenom na použitie len v bezpečných personalizačných prostrediach.



Plán testov T=1 môže obsahovať nasledujúce testy:

- Prístup "hrubej sily", pri ktorom sa vyskúšajú všetky hodnoty mimo množiny definovanej ISO a overí sa, či karta reaguje (nevhodné správanie).
- Prístup "hrubej sily", pri ktorom sa vyskúšajú všetky hodnoty z množiny definovanej ISO, ale mimo množiny definovanej vývojárom (nedokumentované vyhľadávanie príkazov).
- Vyskúšanie všetkých zdokumentovaných príkazov pre vývojárov a kontrola odpovedí.
- Vyskúšajte všetky príkazy zdokumentované vývojárom, ale s dôrazom na limitné prípady a viacnásobné chybové prípady.
- Ovplyvňovanie komunikácie posielaním príkazov v rôznych sekvenciách.
- Prerušenie správy zo systému alebo z produktu

Útoky využívajúce nedokumentované príkazy a príkazy na úpravu sú úzko prepojené, ale odlišné útoky. Hľadanie nedokumentovaných alebo nedefinovaných príkazov je jednoduchý útok typu brute-force, pri ktorom útočník jednoducho spustí sadu príkazov definovaných v ISO a zistí, či karta odpovedá na jeden alebo viac príkazov, na ktoré by nemala odpovedať.

Ak však zdrojový kód nie je k dispozícii, jednoduché vyhľadávanie platných dvojíc CLA/INS nestačí, najmä v súvislosti s identifikáciou existujúcich príkazov: niekedy musia byť všetky CLA/INS/P1/P2/Lc správne. Predstavuje to teda 240 alebo 1 099 511 627 776 rôznych možností (pozri normu ISO/IEC 7816-4).

Hoci vyhľadávanie v nedokumentovaných príkazoch môže byť vysoko štandardizované a automatizované, identifikácia môže byť krátka alebo časovo veľmi nákladná, prípadne príliš nákladná na to, aby sa dala považovať za praktickú. Po vyskúšaní všetkých variantov parametrov a zaznamenaní odpovedí útočník analyzuje, či existuje nejaký zaujímavý prípojný bod útoku. Po určení zaujímavej odpovede útočník zostaví skript na zistenie správania identifikovaného príkazu a zneužitie potenciálnej zraniteľnosti. Toto by sa mohlo vykonať aj kontrolou zdrojového kódu. Všimnite si, že nájdenie jediného príkazu nemusí byť dostatočné, pretože útočník môže musieť hľadať špecifickú sekvenciu príkazov, niekedy podľa proprietárneho protokolu.

To, či nedokumentovaný príkaz môže predstavovať body útoku, závisí od kvality softvéru (oddelenie domén vykonávania) a typu objaveného príkazu.

Príkazy na úpravu

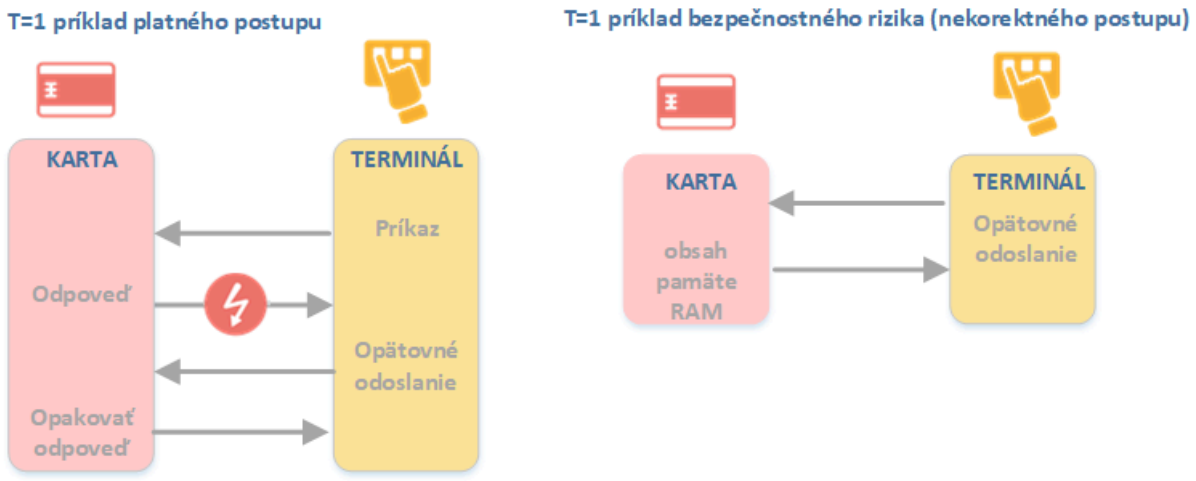
Úprava príkazov je krok útoku, pri ktorom sa útočník pokúša upraviť príkazy počas komunikačnej sekvencie, aby zistil, či karta poskytne neočakávanú odpoveď (tieto príkazy môžu byť v špecifikácii rozhrania alebo môžu byť objavené pozorovaním sekvencií správ alebo vyhľadávaním príkazov, ako je opísané vyššie). Tieto kroky útoku môžu umožniť objavenie a zneužitie zraniteľností (napr. úprava predtým pozorovaných správ s cieľom poskytnúť príliš dlhý parameter môže umožniť útok na pretečenie buffera). Môžu tiež odhaliť časové rozdiely, ktoré pomáhajú pri spätnom inžinierstve softvéru.

Podľa bezpečnostných mechanizmov spojených s rozhraním API a typom správy môže byť jednoduché alebo zložité správu sfalšovať (vzájomná autentizácia, zabezpečený kanál, MAC, šifrovanie, kľúč relácie,...). Ako však už bolo uvedené, ak sa takýto útok dá zistiť, potom spravidla spôsobí, že TOE nevyhovie hodnoteniu.

5.9.3 Priame útoky na protokol

Typickým protokolovým útokom je pokus o odoslanie príkazov, ktoré smart karta vo svojom aktuálnom stave neočakáva. Napríklad: protokoly ISO 7186-3 a 14443 pre smart karty obsahujú príkaz na spracovanie zlyhania v komunikácii. Namiesto spustenia skutočnej komunikácie môže útočník odoslaním tohto príkazu získať neinicializovaný buffer alebo posledný zapísaný buffer.

Tento príklad je zobrazený na nasledujúcich obrázkoch.



V tomto príklade to, či TOE skutočne vypíše obsah pamäte, závisí od správnej inicializácie ukazovateľa a dĺžky I/O buffera. Pamäť znázornená v príklade môže obsahovať zvyšné tajné údaje, napríklad nedávno vypočítaný kľúč relácie DES. Preto tento útok môže útočníkovi umožniť získať tajné údaje
z TOE.

Do kategórie priamych protokolových útokov patria aj útoky zamerané na stavový stroj TOE, kde niektoré citlivé operácie vyžadujú špecifické poradie. Takéto poradie môže zabezpečiť, že kľúče použité pri kryptografických výpočtoch nebudú odhalené (napríklad odoslanie výzvy pred podpisom).

5.9.4 Útoky typu Man-in-the-middle a Replay

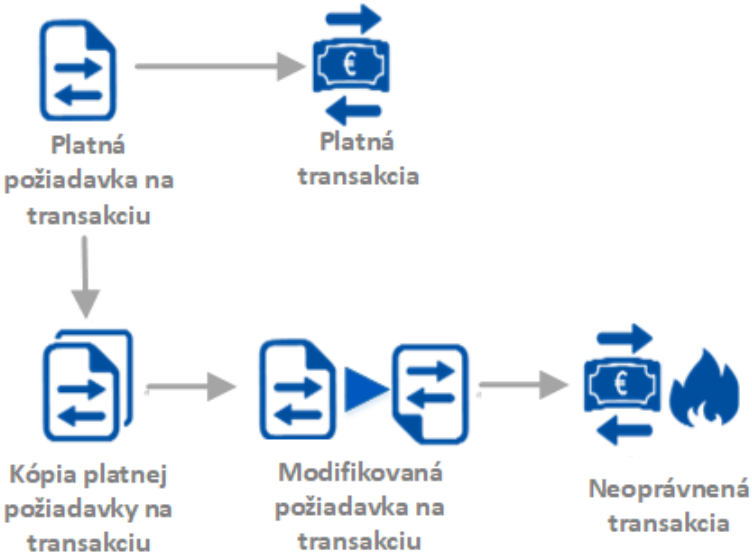
Pri tomto útoku sa útočník skrýva v komunikačnej ceste medzi dvoma entitami, ktoré vykonávajú platnú komunikáciu. Útočník sa jednej zo strán predstavuje ako druhá (platná) strana. Niektoré aplikácie útokov man-in-the-middle vo verejnej literatúre možno nájsť v nasledujúcich prácach:

- Príklad útoku Man-in-the-middle proti overeným SSL reláciám servera, Mattias Eriksson
- Man-in-the-Middle v tunelových autentizačných protokoloch, N. Asokan, Valtteri Niemi, Kaisa Nyberg, Nokia Research Center, Fínsko
- Prečo kryptosystémy zlyhávajú, Ross Anderson

Útoky Man in the middle sú založené na zachytení platných príkazov, a to buď na vykonanie replay útokov, alebo na zmenu niektorých parametrov s cieľom kompromitovať výmenu údajov (získať prístup k vymieňaným dôverným údajom, zmeniť vymieňané parametre).

Útoky na opakovanie sú možné, keď mechanizmus nekontroluje, či je príkaz skutočnou súčasťou aktuálnej sekvencie správ alebo či celá sekvencia správ nebola použitá už predtým (vo všeobecnosti by bezpečný protokol mal tomuto druhu útoku zabrániť už svojím návrhom[61]). Útočník používa analyzátor protokolu na monitorovanie a kopírovanie paketov počas ich toku medzi smart kartou
a čítačkou alebo hostiteľom. Pakety sa zachytávajú, filtrujú a analyzujú na zaujímavé informácie, ako sú digitálne podpisy a autentizačné kódy. Po extrakcii týchto paketov sa pakety znova odošlú (replayed), čím útočník získa možnosť získať neoprávnený prístup k zdrojom.

[61] Dokonca aj v prípade, že je protokol navrhnutý ako bezpečný, môže byť možné použiť útok opakovaním, ak sa použije ďalší krok útoku (ako napríklad narušenie), aby sa zabránilo kontrole, ktorá by inak odhalila a odmietla opakované príkazy.



Na obrázku je znázornená situácia, keď útočník skopíruje platnú požiadavku na transakciu, upraví ju a odošle druhú požiadavku s použitím rovnakých (alebo mierne upravených) verzií správ. Vo všeobecnosti môže tento typ útoku umožniť útočníkovi získať neoprávnený prístup k aktívam používateľa, napríklad k výberu z banky alebo k chráneným systémovým zdrojom.

Útok môže byť úplnou cestou útoku, napríklad ak sa podarí výber z bankového účtu. V prípade prístupu k systémovým prostriedkom môže ísť o čiastočnú cestu útoku v závislosti od povahy prostriedkov, ku ktorým sa pristupuje (napr. v dôsledku útoku môže byť útočník schopný komunikovať ako bežný používateľ a potom sa môže pokúsiť získať privilegovaný status).

Útoku na opakovanie by sa dalo čeliť použitím sekvenčných čísel s vhodnou ochranou integrity, čím by sa výrazne sťažilo používanie nahraných platných správ.

5.9.5 Pretečenie vyrovnávacej pamäte alebo pretečenie zásobníka

Tento útok je použiteľný na akýkoľvek vstavaný softvér alebo firmvér. Nižšie je uvedený príklad pre otvorenú platformu. Otvorené platformy sú v tomto dokumente definované ako operačné systémy smart kariet s možnosťou spúšťania a sťahovania viacerých aplikácií.

Otvorené platformy poskytujú aplikáciám súbor služieb, najmä služieb na ochranu ich citlivých údajov pred externými aplikáciami (neoprávnený prístup a neočakávaná modifikácia).

Tento útok môže byť vykonaný prostredníctvom pretečenia vyrovnávacej pamäte alebo pretečenia zásobníka, ktoré vznikne spustením škodlivej aplikácie. Preplnenie, ak ho platforma nekontroluje, môže mať rôzne účinky, napríklad prepísanie existujúceho obsahu v aktuálnom zásobníku.

Očakávaným účinkom útočníka je, že škodlivá aplikácia zmení aktuálny kontext vykonávania a získa systémové oprávnenia. Napríklad práva na vykonávanie aktuálneho kontextu sú zapísané v zásobníku; ak útočník dokáže tieto práva prepísať a vložiť práva správcu, všetky operácie vykonané po tejto operácii budú mať práva správcu. Ďalším príkladom je, že útočník môže prepísať pamäťové miesto, ktoré obsahuje ukazovateľ v pamäti. Útočník potom môže kontrolovať, odkiaľ aplikácia získava svoje údaje.

Získanie takýchto oprávnení umožňuje tejto aplikácii vykonávať prakticky všetky operácie a následne zverejniť alebo upraviť tajné údaje, napr. upraviť alebo zverejniť kód PIN inej aplikácie.

Ďalším účinkom je, že sa načítajú interné údaje alebo údaje, o ktorých sa nepredpokladalo, že ich príkaz vráti.

5.9.6 Prepínanie komunikačných rozhraní

Tento útok sa vzťahuje na karty s dvoma rozhraniami. Cieľom je využiť možnosť komunikovať s TOE na dvoch rôznych rozhraniach.

Napríklad v TOE vloženom do mobilného telefónu s rozhraním NFC je prístup k TOE možný buď prostredníctvom rozhrania NFC, alebo prostredníctvom aplikácií stiahnutých do telefónu (komunikácia v kontaktnom režime). Útočník môže čakať na platnú vzájomnú autentizáciu medzi terminálom a TOE a potom by mohol útočník prostredníctvom kontaktného rozhrania komunikovať s TOE a využiť to, že je otvorená zabezpečená relácia. Útočník tak môže obísť reťazenie stavového stroja a získať prístup k príkazom s privilegovaným prístupom.

5.10 Izolácia aplikácie

5.10.1 Úvod

Viacaplikačná platforma opisuje súbor hardvéru a softvéru vytvorený s cieľom spustiť viac ako jednu aplikáciu súčasne.

Kombinácia fyzických a logických opatrení viacaplikačnej platformy umožňuje izoláciu aplikácie, ktorú možno definovať ako: všetky bezpečnostné opatrenia a mechanizmy, ktoré chránia citlivé aktíva aplikácie a platformy pred modifikáciou a/alebo prezradením.

Aktíva, ktoré môže byť potrebné chrániť v prostredí s viacerými aplikáciami, sú:

- Načítané údaje aplikácie (vrátane kľúčov).
- Načítaný kód aplikácie.
- Základné údaje platformy.

Izolácia appletu je cieľom rôznych typov útočných techník na dosiahnutie týchto prostriedkov. Platforma viacerých aplikácií ako taká je predmetom typických útokov na smart karty, ako napr:

- Fyzické útoky,
- Perturbačné útoky,
- Útoky cez bočný kanál a,
- Softvérové útoky, ktoré môžu, ale nemusia byť kombinované s vyššie uvedenými útokmi, podrobne opísané ako:
  - Neoprávnené zverejnenie údajov načítanej aplikácie (napríklad údajov aplikácie, kódu a kľúčov).
  - Neoprávnené používanie pokynov, príkazov alebo postupnosti príkazov.
  - Obchádzanie obmedzení správcu načítaním škodlivej aplikácie na platforme s viacerými aplikáciami.
  - Čítať dôverné údaje alebo kód patriaci inej načítanej aplikácii bez oprávnenia pomocou načítanej aplikácie.
  - upravovať údaje alebo kód patriaci inej načítanej aplikácii bez jej oprávnenia pomocou načítanej aplikácie.
  - Prístup k dôverným údajom o systémových prostriedkoch (ako je systémová záplata) pomocou aplikácie Loaded.
  - Reverzné inžinierstvo mechanizmov abstrakčnej vrstvy pomocou načítanej aplikácie

5.10.2 Čiastočné útoky

Na zabezpečenie izolácie aplikácií existuje súbor technológií. Tieto technológie sú zvyčajne špecifikované v normách a možno ich kombinovať v zariadeniach s smart kartami.

Pri úplnom útoku môže útočník potrebovať prekonať jednu z týchto technológií alebo ich kombináciu. Termín čiastočné útoky sa tu používa na označenie útokov, ktoré je potrebné pri vykonávaní úplného útoku kombinovať.

5.10.3 Čiastočné útoky GlobalPlatform

Štandard GlobalPlatform (GP) obsahuje definíciu rámca pre interoperabilitu a správu aplikácií. Tento rámec je špecifikovaný v špecifikácii GP a jeho hlavné zložky môžeme identifikovať takto:

- Otvorené prostredie globálnej platformy (OPEN)

OPEN je dodatočná vrstva k JCRE, ktorá poskytuje karte ďalšie funkcie správy. Ak je na karte

prítomný OPEN, je zodpovedný za odosielanie príkazov, (voliteľnú) správu viacerých logických kanálov, správu aplikácie a životný cyklus karty.

OPEN poskytuje aj konkrétnu správu na vykonávanie inštalácie a odstraňovania aplikácií. Na tento účel špecifikácia GP definuje pojem bezpečnostnej domény.

- Bezpečnostná doména (SD)

Bezpečnostná doména predstavuje aktéra smart karty na karte. Na karte môžu byť prítomné tri hlavné subjekty: poskytovateľ aplikácie (AP), vydavateľ karty (CI) a kontrolný orgán (CA). SD je špeciálny druh aplikácie smart karty, ktorá poskytuje spoločné bezpečnostné služby pre aplikácie, ktoré sú s ňou spojené, napr. rôzne druhy kryptografických služieb, bezpečné posielanie správ, ako aj personalizáciu aplikácie. SD uchováva kryptografické tajomstvá aktéra, ktorého zastupuje. Karta GP je vždy vybavená bezpečnostnou doménou CI. Jednou z výhod, ktoré SD prinášajú poskytovateľom bezpečnosti, je to, že AP môže využívať určitú nezávislosť od CI najmä pri poskytovaní bezpečnostných služieb (napr. bezpečného posielania správ alebo personalizácie aplikácií) svojim pridruženým aplikáciám. SD môže získať ďalšie oprávnenia, ktoré by mu umožnili vykonávať správu obsahu karty (načítanie aplikácie, inštalácia atď.).

- Metódy overovania držiteľa karty

Ide o spoločné bezpečnostné služby, ktoré karta poskytuje všetkým aplikáciám. Poskytuje najmä možnosť, aby všetky aplikácie používali jedinečné číslo PIN používateľa.

5.10.3.1 Popis čiastočných útokov

Cieľom útoku na GlobalPlatform je umožniť útočníkovi nelegálne načítať aplikáciu do TOE, t. j. bez znalosti hodnôt načítavacích kľúčov.

Útok sa nevykonáva na kryptografické výpočty zapojené do procesu vzájomnej autentizácie GlobalPlatform a následných príkazov bezpečného posielania správ.

Útok sa vykonáva na vykonávanie kódu bezpečnostnej domény s oprávnením na správu obsahu. Útok tu využíva potenciálnu zraniteľnosť v odolnosti toku vykonávania kódu voči útokom na narušenie. Ide tu o vynútenie vykonania ľubovoľného príkazu APDU pre správu obsahu (INSTALL [pre načítanie], LOAD atď.), zatiaľ čo nebol otvorený žiadny bezpečný kanál. Ak je implementácia základná, môže to spočívať v jednoduchom overení, ako napr:

if (securityLevel == SecureChannel.NO_SECURITY_LEVEL) ISOException.throwIt(0x6985);

Potom útočníkovi stačí poslať príkaz na správu obsahu (bez predchádzajúceho príkazu INITIALIZE UPDATE a EXTERNAL AUTHENTICATE) a ak uvedie bajt CLA 0x80, nebude spracované žiadne bezpečné rozbalenie kanála: preto nie je potrebné útočiť na žiadne kryptografické výpočty.

Na úspešné načítanie a inštaláciu appletu sú potrebné dve rôzne sekvencie:

- Sekvencia na načítanie kódu, ktorá pozostáva z príkazu INSTALL [pre načítanie] a jedného alebo viacerých príkazov LOAD;
- Sekvencia pre inštanciu appletu, ktorá pozostáva z príkazu INSTALL [pre install & make selectable].

V prvej sekvencii musí byť útočník schopný úspešne reprodukovať útok na všetky príkazy v rámci sekvencie, pretože operácia načítania je atomická (aspoň 2^{62}). Ak útok zlyhá (čo vo všeobecnosti znamená vypnutie napájania), sekvencia sa znovu spustí od počiatočného príkazu INSTALL [pre načítanie].

5.10.3.2 Vplyv na TOE

Priamy vplyv spočíva v tom, že TOE môže obsahovať škodlivý kód, ktorý by mohol odhaliť alebo zmeniť iné aplikácie.

5.10.4 Čiastočné útoky na overovač bajtového kódu

[62] Optimalizovaný škodlivý applet, ktorý je schopný vykonávať kód načítaný do haldy (napr. v obsahu polí), sa zmestí do jedného príkazu LOAD APDU. V opačnom prípade je potrebné uvažovať v priemere o 2 alebo 3 príkazoch LOAD.

Všetky bajtkódy sa musia pred vykonaním overiť, aby sa predišlo vykonávaniu chybných appletov. V technológii Java sa na overenie súboru triedy vo virtuálnom stroji Java používa ByteCode Verifier, ktorý funguje dynamicky (napr.: aplikuje sa pri každom načítaní triedy). Úplný ByteCode Verifier sa však často neimplementuje na karte Java z dôvodu obmedzenia jej výpočtového výkonu a veľkosti pamäte. Na vyriešenie tohto problému existuje niekoľko riešení:

- Aplikáciu možno overiť mimo karty pomocou overovača mimo karty, ktorý nie je obmedzený obmedzeniami karty Java.
- Aplikáciu možno overiť na karte pomocou špeciálneho overovača na karte určeného pre kartu Java.

Ochranný profil karty Java stanovuje, že všetok bajtový kód by sa mal pred vykonaním overiť. Vyžadujú sa aj ďalšie overenia, aby sa zabezpečilo, že aplikácia neobsahuje škodlivý kód. Ak sú všetky overenia úspešné, súbor CAP sa môže nahrať na kartu.

V tomto kontexte je TOE smart karta, pretože všetky aktíva, ktoré sa majú chrániť, sú v nej. V overovači mimo karty sa nenachádza žiadne aktívum. V skutočnosti tento útok umožňuje útočníkovi požiadať
o načítanie svojho škodlivého appletu bez toho, aby bol odhalený.

5.10.4.1 Opis príkladu čiastočného útoku

Základné útoky na zámenu typov modifikujú referenciu objektu referenciou iného objektu. Napríklad môžeme priradiť adresu poľa bajtov ku krátkemu poľu, aby sme vymazali pamäť nachádzajúcu sa za poľom bajtov. Nasledujúce dva útoky sú založené na zámene typu:

- Vytvorenie zámeny typov, ktorú verifikátor na karte nezistil, čo nám umožňuje vypustiť a upraviť časť obsahu pamäte.

Na tento útok je potrebných niekoľko krokov. Najprv je potrebné charakterizovať overovač na karte, aby bolo možné pochopiť jeho správanie a analyzovať kontroly vykonávané týmto nástrojom. Po druhé, je potrebné napísať škodlivý applet vytvorením zámeny typov, ktorú nástroj On-Card Verifier nezistí.

Hlavným predpokladom tohto útoku je, že aplikáciu je možné načítať na kartu. Ak to tak nie je, tento útok sa stane kombinovaným útokom. V skutočnosti by mal hodnotiteľ použiť útok opísaný v časti **Chyba! Referenčný zdroj nebol nájdený.** "**Chyba! Reference source not found.**" s cieľom obísť mechanizmus načítania.

- Použitie dobre sformulovaného súboru CAP zneužívajúceho mechanizmus transakcií na vytvorenie zámeny typov.

Cieľom tohto útoku je vytvoriť typovú zámenu pomocou slabiny v implementácii platformy, ktorá nám umožní vypísať a modifikovať časť obsahu pamäte. Tento typ útoku využíva dobre vytvorený súbor CAP a zneužíva mechanizmus transakcií na vytvorenie typovej zámeny.

Hlavným predpokladom tohto útoku je, že aplikáciu je možné načítať na kartu. Ak to tak nie je, tento útok sa stane kombinovaným útokom. V skutočnosti by mal vyhodnocovateľ použiť útok opísaný v časti 5.10.3 "Čiastočné útoky na globálnu platformu", aby obišiel mechanizmus načítania.

5.10.4.2 Vplyv na TOE

Vplyv útoku typu zmätok závisí od implementácie softvéru. Hlavné vplyvy sú:

- získavanie tajných údajov (napríklad kryptografických kľúčov).
- Čítanie údajov/kódu mimo nášho kontextu.
- Úprava údajov inej aplikácie.
- Úprava zdrojového kódu inej aplikácie.

5.10.5 Obranné čiastočné útoky na virtuálny počítač

Existujú dva prístupy k zachovaniu typovej bezpečnosti vo virtuálnych počítačoch

- Polobezpečnostný virtuálny počítač: všetky bajtkódy sa overujú buď pred inštaláciou, alebo počas

nej (mimo karty alebo na karte).

Poloobranný virtuálny stroj zabraňuje zámene typov tým, že zakazuje vykonávanie určitých sekvencií bajtkódu. Virtuálne stroje s overovačmi bajtkódu mimo karty aj na karte sa považujú za poloobranné virtuálne stroje.

- Obranný virtuálny stroj: typová bezpečnosť je vynútená počas behu, pretože virtuálny stroj sa odvoláva len na typované údaje

Obranný virtuálny stroj[63] môže analyzovať bajtový kód dynamicky počas vykonávania APDU (napr.: overenie typu a štrukturálne overenie) a nevyžaduje analýzu bajtového kódu mimo karty alebo na karte, aby sa zabránilo zámene typov.

5.10.5.1 Opis príkladu čiastočného útoku

Cieľom útoku na obranný virtuálny počítač je oklamať virtuálny počítač, aby umožnil zámenu typov. Takýto útok môže byť možný, keď je defenzívny virtuálny stroj implementovaný len čiastočne.

Do cieľa sa načíta zle vytvorený applet obsahujúci kódy bajtov v nezákonnom poradí, ktorý potom, keď nie sú prítomné obranné kontroly alebo sú neúplné, spôsobí zámenu typu. Táto zámena typu sa potom môže prípadne použiť na čítanie trvalých a prechodných údajov JCRE a iných kontextov, ktoré nepatria do kontextu útočníka.

Plnohodnotný útok na zámenu typu využíva samotný útok na zámenu typu, znalosť metaúdajov virtuálneho počítača a jeho aplikáciu v jedinom útočnom applete schopnom čítať alebo zapisovať do trvalej a prechodnej pamäte.

5.10.5.2 Vplyv na TOE

Útok je zameraný proti iným aplikáciám nainštalovaným v TOE alebo proti operačnému systému. Hlavné dopady sú:

- Prístup k tajným údajom cieľového appletu,
- Úprava funkcií a stavu appletu

Keďže vnútorné zobrazenie údajov nie je verejná, útočník by mal mať rozhodujúce znalosti o TOE, aby mohol získané údaje interpretovať alebo experimentálnou analýzou na otvorených vzorkách odvodiť význam údajov.

5.10.6 Čiastočné útoky bránou firewall

Operačný systém Java Card je navrhnutý tak, aby všetky applety bežali v jednom virtuálnom počítači. Nemá prostriedky na poskytnutie virtuálneho stroja pre každú aplikáciu, ktorý by poskytoval izolované prostredie pre beh každého appletu.

Brána firewall karty Java je zavedená na zabezpečenie prostredia pieskoviska pre applety spustené v tom istom virtuálnom počítači.

Brána firewall karty Java obmedzuje prístup k referenciám na objekty podľa ich kontextu. Odkazovať sa možno len na objekty vytvorené v rámci toho istého kontextu. Prístup k zdrojom mimo kontextu objektu je možný prostredníctvom brány firewall karty Java Card pomocou mechanizmu zdieľaného objektu rozhrania. Statické členy sú z kontroly firewallu vylúčené a ich prístupnosť nezávisí od kontextov.

5.10.6.1 Opis čiastkových útokov

Škodlivé aplety v prostredí Java Card by sa mohli použiť na spochybnenie obmedzení zavedených bránou Java Card Firewall útokom na mechanizmy prepínania kontextu. Tieto škodlivé applety sú dobre formulované a prechádzajú overením bajtového kódu. Tento útok môže byť ľahšie uskutočniť

[63] Vo verzii 2.6 ochranného profilu systému Java Card už nie je definovaný obranný virtuálny stroj.

ako útoky na zle vytvorené applety, pretože škodlivý útok na applety sa nedá odhaliť overením bajtového kódu. Na druhej strane, tento útok môže byť úspešný len vtedy, ak je firewall TOE chybný.

5.10.6.2 Vplyv na TOE

Útok je zameraný proti iným aplikáciám nainštalovaným v TOE alebo proti operačnému systému. Hlavné dopady sú:

- Prístup k tajným údajom cieľového appletu,
- Úprava funkcií a stavu appletu

Potenciálne použitie týchto techník je špecializované a musí sa zvážiť v kontexte každého hodnotenia. Keďže vnútorné zobrazenie údajov nie je verejná, útočník by mal mať kritické znalosti o TOE, aby mohol interpretovať získané údaje, alebo experimentálnou analýzou na otvorených vzorkách odvodiť význam údajov.

5.10.7 Čiastočné útoky Multos

Platforma MULTOS poskytuje bezpečné prostredie na vykonávanie aplikácií a ukladanie údajov. Je to operačný systém s viacerými aplikáciami, ktorý presadzuje segregáciu aplikácií. Aplikácie MULTOS možno vyvíjať v jazyku C, v jazyku MULTOS Assembler (MEL) alebo v jazyku Java.

MULTOS nemá overovací nástroj pre kód MEL, pretože tento jazyk je menej zložitý. MULTOS má však podobné bezpečnostné mechanizmy, ako je firewall a bezpečné načítanie aplikácií.

Systém MULTOS implementuje tieto protiopatrenia:

- Inštrukcie, primitíva a príkazy APDU neumožňujú manipuláciu s adresami. V skutočnosti nemôžeme priradiť novú adresu premennej na rozdiel od Java Card (napríklad: aload_1 astore_3)
- Firewall: izolácia appletu, izolácia kódového priestoru a dátového priestoru (napríklad nemôžeme vykonať skok z kódu do dát). Preto aplikácia nemôže pristupovať do iného aplikačného priestoru, a tak k nej nemôžu pristupovať iné aplikácie.
- Aplikácia nahraná na karte môže obsahovať:
  - Pokyny MEL
  - Údaje
  - Záznam DIR: informácie o názve aplikácie po jej vložení na kartu
  - Záznam FCI: informácie, ktoré sa vrátia pri výbere aplikácie MEL
  - Podpis žiadosti (ak existuje)
  - KTU (ak existuje)
  - ...
  - Nie je možné manipulovať s komponentmi v rozpore s kartou Java Card (napríklad s cieľom sfalšovať adresu odstránením prvku v umiestnení Reference).
- Aplikačný abstraktný stroj MULTOS poskytuje každej aplikácii vlastný pamäťový priestor. Pamäťový priestor je v skutočnosti vždy relatívny voči aktuálne spustenej aplikácii. Namiesto absolútnych adries sa používajú označené adresy. Táto označená adresa sa skladá z:
  - Register: ST a SB pre statickú pamäť, DT, DB a LB pre dynamickú pamäť, PB a PT pre verejnú pamäť
  - Odsun
  - V závislosti od použitého registra sa vygeneruje iná inštrukcia. Napríklad:
    - Pokyn "LOAD SB[1], 0x10" bude "39 10 00 01".
    - Pokyn "LOAD PB[1], 0x10" bude "3E 10 00 01".
- Načítaná aplikácia môže byť zašifrovaná

5.10.7.1 Opis čiastočného útoku

Tento útok je kombinovaný. Jeho cieľom je pokúsiť sa prečítať blok údajov s neplatnou veľkosťou (veľkou) a vykonať injektáž chyby s cieľom obísť firewall.

Brána firewall zabezpečuje, že aplikácia nemá prístup do iného aplikačného priestoru. Ak sa útočník pokúsi vykonať inštrukciu, ktorá sa pokúsi prečítať blok dát s neplatnou dĺžkou bloku, firewall zistí, že sa aktuálna aplikácia pokúša o prístup do iného aplikačného priestoru, a preto vráti chybu. Vyhodnocovateľ musí vykonať injekciu chyby, aby túto kontrolu obišiel, a tak úspešne vypustil časť

pamäte.

5.10.7.2 Vplyv na TOE

Hlavné dôsledky tohto útoku sú:

- získavanie tajných údajov (napríklad kryptografických kľúčov),
- Čítanie údajov/kódu mimo nášho kontextu.

5.10.8 Úplná cesta útoku

Úplné cesty útoku kombinujú čiastkové útoky na získanie nezákonného prístupu k citlivým zdrojom (napríklad PIN a kľúče) cez izoláciu appletu.

5.10.9 Útoky na správu pamäte (získanie prostriedku z inej aplikácie)

Tento útok je kombináciou:

1. Získanie výpisu pamäte na lokalizáciu aktív a/alebo citlivého kódu prostredníctvom fyzických alebo softvérových útokov. Útočník je schopný fyzickým narušením počas vysielania bajtov prinútiť TOE, aby vydal viac bajtov, ako sa očakávalo. Získané výpisy pamäte, napríklad počas ATR alebo pri verejných príkazoch APDU, ktoré vracajú značný počet bajtov, môžu útočníkovi umožniť identifikovať prostriedky iných aplikácií a ich príslušné adresy v pamäti.

   Treba si všimnúť, že softvérové útoky, ako sú tie, ktoré sú opísané v časti "**Chyba! Reference source not found.**" alebo "**Chyba! Reference source not found.**" by sa namiesto toho mohli použiť na vykonanie takéhoto výpisu pamäte.

2. Načítanie appletu cez "**Chyba! Referenčný zdroj nebol nájdený.**".

   Útočník môže prostredníctvom tohto útoku nahrať do TOE škodlivú aplikáciu.

3. Zadajte zámenu na manipuláciu s objektmi identifikovanými v kroku 2 prostredníctvom "**Chyba! Referenčný zdroj nebol nájdený.**" alebo "**Chyba! Referenčný zdroj nebol nájdený.**".

   Útočník môže v škodlivom applete nezákonne manipulovať s pamäťovou adresou objektu iného kontextu. V tomto popise sa to dosahuje prostredníctvom útokov na zámenu typov.

4. Útok na firewall na vykonanie metódy getKey na objekte prostredníctvom "**Error! Referenčný zdroj nebol nájdený.**".

5. Útočník využíva fyzické poruchy na obídenie obmedzení Java Card/Multos Firewall a zároveň manipuluje s objektmi mimo legitímnych hraníc. Na platforme Java Card môže škodlivý applet nelegálne zavolať metódu getKey na adresu objektu iného kontextu.

Krok 1 a krok 2 sa používajú na kalibráciu útoku. Kroky 3 a 4 sú tu podrobne opísané, pretože v čiastkových útokoch opísaných v predchádzajúcich častiach predpokladáme, že jeden škodlivý applet môže vykonávať všetky operácie, zatiaľ čo v reálnejších príkladoch môže škodlivý applet manipulovať len s vlastnými objektmi. Preto sa tu na obídenie obmedzenia firewallu používa perturbácia.

5.10.9.1 Vplyv na TOE

Všetky bezpečnostné mechanizmy platformy by mohli byť obídené s cieľom odhaliť alebo zmeniť tajomstvá, pretože bezpečnostné postupy (dešifrovanie, aktualizácia *atď.)* sú nútené byť legálne vykonávané v kontexte, ktorý patrí napadnutej aplikácii.

5.10.10 Útoky na vykonávanie kódu (volanie kódu z inej aplikácie)

V tejto časti je popísaný útok podobný predchádzajúcemu, ale tu je aplikovaný na nezdieľanú metódu iného appletu.

Vyžaduje sa rovnaká kombinácia útokov s nasledujúcimi úpravami:

1. Získanie výpisu pamäte na lokalizáciu aktív a/alebo citlivého kódu prostredníctvom fyzických

útokov alebo softvérových útokov V porovnaní s predchádzajúcim útokom by útočník mal nielen lokalizovať objekty (a ich príslušné referencie), ale aj obrátiť časť kódu, aby identifikoval súkromné rutiny, ktoré sa majú zavolať (napríklad na vynulovanie bezpečnostného počítadla alebo vypnutie bezpečnostného mechanizmu).

2. Načítanie appletu cez "**Chyba! Referenčný zdroj nebol nájdený.**". Rovnaké ako pri predchádzajúcom útoku.
3. Zadajte zámenu, aby ste mohli manipulovať s objektmi identifikovanými v kroku 2 prostredníctvom "**Chyba! Referenčný zdroj nebol nájdený.**" alebo "**Chyba! Referenčný zdroj nebol nájdený.**".

Rovnaké ako pri predchádzajúcom útoku.

4. Útok na firewall na vykonanie metódy getKey na objekte prostredníctvom "**Error! Referenčný zdroj nebol nájdený.**".

   Útočník využíva fyzické poruchy na obídenie obmedzení Java Card/Multos Firewall a zároveň manipuluje s objektmi mimo legitímnych hraníc. Na platforme Java Card môže škodlivý applet nelegálne zavolať ľubovoľnú metódu na adresu objektu iného kontextu. Na umožnenie vyvolania metódy na objekte, ktorý nie je vo vlastníctve aktuálneho kontextu, cez obmedzenia firewallu však môže byť potrebných niekoľko perturbácií, pretože počas vykonávania metódy môže byť objekt, ktorý nie je vo vlastníctve aktuálneho kontextu, sprístupnený niekoľkokrát, pričom zakaždým sa vykoná kontrola firewallu[64] .

Krok 1 a krok 2 sa používajú na kalibráciu útoku. Kroky 3 a 4 sa tu nepripomínajú, pretože sú podobné v porovnaní s predchádzajúcim útokom. Je potrebné si všimnúť, že vykonanie viacerých perturbácií je náročné, avšak stále uskutočniteľné, pretože operáciu kontroly firewallu možno identifikovať prostredníctvom synchronizácie na vykonávanie bajtkódu.

5.10.10.1 Vplyv na TOE

Škodlivá aplikácia môže získať prístup k súkromným rutinám, ktoré umožňujú resetovať počítadlá alebo deaktivovať bezpečnostné mechanizmy.

DODATOK A

A.1 Prístup k faktoru TOE s ohľadom na odstránenie balíka

Je na rozhodnutí vývojára, či balíček (vrátane integračnej štruktúry a celkového formálneho faktora, napr. stohovanej matrice) zahrnie alebo nezahrnie do TOE a popíše ho ako taký v bezpečnostnom zámere s vedomím, že to bude mať vplyv aj na triedu ALC_DVS.

Hodnotenie odstránenia alebo prípravy balíka je v tomto dokumente vyjadrené vo faktore "Prístup k TOE" (pozri časť 4.5.1) v závislosti od úsilia potrebného na odstránenie balíka. Balík sa totiž dá považovať za bariéru, ktorá bráni útočníkovi v prístupe k TOE s cieľom vykonať fyzické alebo invazívne útoky.

Podrobnosti o troch úrovniach hodnotenia (nízka, stredná a vysoká náročnosť prípravy) sú definované v nasledujúcej časti. Upozorňujeme, že metódy prípravy balíkov a zodpovedajúca náročnosť hodnotenia sa nepovažujú za také vyspelé ako v iných oblastiach, ako sú SCA alebo FI. Preto bude obsah tohto dodatku v prípade potreby revidovaný.

A.2 Úrovne úsilia na prípravu balíka TOE

V tejto časti je podrobnejšie opísaný súčasný pohľad na úsilie potrebné na odstránenie balíka.

Nízka náročnosť prípravy:

[64] **Omyl!** Keďže getKey je implementovaný na úrovni platformy, je veľká pravdepodobnosť, že kód je v natívnom jazyku, a preto by sa mala vykonať len jedna kontrola firewallu.

Jednoduché obaly, ktoré nevyžadujú veľké úsilie na prípravu a ktoré možno odstrániť štandardným chemickým leptaním, mechanickým pôsobením, opätovným zapojením alebo podobne pre cestu útoku, napr:

- Bežné smart karty vo väčšine prípadov,
- Štandardné plasty ako DIP, SOIC, QFP, QFN,..., BGA (zamerané na prístupnejšiu stranu, zvyčajne zadnú stranu pre flip chip).

Stredne náročná príprava:

Balíky, ktoré si vyžadujú stredne náročnú prípravu a ktoré majú relatívne vysoké riziko fatálneho poškodenia TOE (strata funkčnosti, ktorá je cieľom alebo je potrebná na hodnotenie) z dôvodu špeciálnych konštrukcií, ako napr:

- Komplexný balík na balíku s lepenou doskou interposer,
- Obaly s pasívnym pletivom alebo obštrukčným drôtovým spojením: To znamená, že spojovacie drôty sa ťažko odstraňujú/obchádzajú alebo sa ťažko prepájajú. Vyžaduje si to napríklad značný manuálny reverzný inžiniering (> 1 týždeň) niekoľkých stoviek pinov, ktoré sa majú získať vygenerovaním mapy spájania. A úsilie na prevod mapy spájania do formátu súboru pre spojovací stroj na použitie automatického spojovacieho stroja. Upozorňujeme, že ak pri využívaní nie je potrebné opätovne vykonať reverzné inžinierstvo, následne sa body pri využívaní pridelia len vtedy, ak si zostávajúca cesta útoku stále vyžaduje špecializované vybavenie alebo vyššie. Oddelenie matríc môže byť zložité, pretože medzi matricami existujú určité funkčné závislosti, ktoré sa musia opätovne prepojiť, čo zahŕňa spätné inžinierstvo, vývoj testovacieho zariadenia medzi matricami
  a zvyšuje riziko vyradenia TOE z prevádzky,
- Odlievacie zmesi, napríklad na báze syntetického materiálu, ako je živica, ktoré si vyžadujú chemickú úpravu špecifickú pre daný materiál, pretože mechanické odstránenie obalu vedie s vysokou pravdepodobnosťou k fatálnemu poškodeniu TOE. Takéto odlievacie zmesi sa používajú napríklad v HSM (zariadenia na generovanie kľúčov v centrách dôvery). Špecifikácia materiálu
  a „state of the art“ metódy odstraňovania sú však potom predmetom hodnotenia. ITSEF by sa mal pokúsiť odstrániť obal pomocou štandardných chemických metód, napríklad vlnou horúcej dymiacej kyseliny sírovej, aplikáciou kyseliny fluórovej a iných.

Poznámka: V súčasnosti neexistuje harmonizácia medzi krajinami, pokiaľ ide o metódy odstraňovania obalov, a preto je potrebné rozhodnúť o každom jednotlivom prípade/diskutovať s CB, aby sa určilo, čo je štandardné.

Vysoké úsilie pri príprave:

Balíky, ktoré si vyžadujú veľké úsilie na prípravu, viacerých expertov a zriedkavé nástroje na mieru, ktoré nie sú deklarované ako bezpečnostné funkcie, ako napr:

- Čip na čipe s kritickou funkčnou závislosťou, ktorá si na fungovanie vyžaduje krídlovú dosku: Je dôležité zvážiť metódy obchádzania závislostí, napr. spustenie externej pamäte s nižšou frekvenciou a podobné. V tomto príklade TOE nie je funkčný bez externej pamäte alebo TOE kontroluje prítomnosť pamäte, ale SoC nepridáva žiadne prostriedky ochrany TOE.

Ak existujú kontroly TOE pre externé komponenty, potom je obchádzanie týchto kontrol dôležité pre hodnotenie,

- Balíky s aktívnou sieťou, čo napríklad znamená, že sieť je pripojená k TOE a TOE ju monitoruje z hľadiska poškodenia,
- Môžu sa vyskytovať licie zmesi, napríklad na keramickej báze, ktoré nie je možné odstrániť bez fatálneho poškodenia TOE pomocou mechanických a tiež štandardných chemických prostriedkov. Odstránenie preto buď nie je praktické podľa „state of the art“, ako je uvedené ďalej, alebo podlieha metódam na mieru, ktoré sú známe len predajcovi a o ktoré sa v priebehu hodnotenia podelil
  s ITSEF. T. j. nemala by existovať žiadna verejne známa metóda na jednoduché odstránenie

obalového materiálu alebo pomocou „state of the art“ chemických metód. Z tohto dôvodu musí byť špecifikácia materiálu a kontrola „state of the art“ metód odstraňovania predmetom hodnotenia, na ktorom sa môžu podieľať externí odborníci z iných fakúlt, napr. chemickej a inej. Od dodávateľa možno tiež požadovať, aby poskytol vzorky materiálu na chemickú analýzu a pokusy. Tieto vzorky materiálu môžu, ale nesmú obsahovať TOE.

A.3 Príklady hodnotenia odstránenia balíkov

Nasledujúce opisy balíkov nie sú založené na existujúcich produktoch a slúžia len ako príklady pre metodiku hodnotenia:

Príklad 1

Toto je základná situácia, keď balík neprispieva k odolnosti voči útoku. Príklad predpokladá jednoduchý útok Prienik ľahkej chyby – Light Fault Injection – LFI (napr. obídenie autentizácie) na zraniteľnú TOE
v balení Chip Scale Package alebo v holom telese. V tomto prípade sú úsilie a zručnosti potrebné na prípravu TOE na LFI veľmi obmedzené, pretože CSP sa dá ľahko rozpustiť chemickým leptaním.
V prípade holých matríc nie je potrebná žiadna príprava.

***Tabuľka 14:** Kombinované základné hodnotenie laserového vstrekovania porúch a odstraňovania obalu pre nízke nároky na prípravu obalu*

LFI na CSP alebo holom telese			
Faktory	**Popis**	**Identifikácia**	**Využívanie**
Uplynulý čas	Na nastavenie zariadenia a vykonanie útoku útočník by strávil viac ako týždeň, ale menej ako mesiac.	< jeden mesiac (3)	< jeden týždeň (4)
Odbornosť	Vyžadujú sa len odborné znalosti, pokiaľ ide o napadnutá funkčnosť.	Znalec (2)	Znalec (2)
Znalosť TOE	Útok je možné vykonať pomocou verejne dostupných informácií.	Verejnosť (0)	Verejnosť (0)
Prístup k TOE	Pri otváraní nehrozí poškodenie TOE. Preto sa tu nebudú udeľovať žiadne body.	<10 vzoriek (0) **Nízke nároky na prípravu +(0)**	<10 vzoriek (0) **Nízke nároky na prípravu +(0)**
Zariadenie	Vyžaduje sa len štandardné nastavenie LFI. Žiadne vybavenie pre odstránenie balíka.	Špecializované (3)	Špecializované (4)
Otvorené vzorky		nevyžaduje sa (0)	-
Medzisúčet		8	10
Celkom		**18 (základné)**	

Príklad 2

Prienik ľahkej chyby na zraniteľnom zariadení TOE v konfigurácii balík na balíku. Ide o rovnaký TOE ako v príklade 1, ale v inom type balíka. Dodávateľ tvrdí, že balík pridáva do TOE dodatočné zabezpečenie. TOE (spodný balík) môže fungovať nezávisle od podporného zariadenia vo vnútri vrchného balíka. Výbrus vo vnútri spodného obalu je vložený medzi spodnú nosnú dosku a hornú nosnú dosku. Horná nosná doska úplne zakrýva TOE. Dutiny medzi nosnými doskami sú vyplnené živicou. Otvorenie tohto obalu si vyžaduje podstatne viac času a nástrojov v porovnaní s CSP a holými matricami. Najprv sa musí odstrániť horný obal. Potom sa musí urobiť otvor v hornej nosnej doske bez toho, aby sa poškodila SoC matrica v spodnom obale. Výstupok SoC sa musí odkryť na prípravu LFI, čo si vyžaduje leptanie. Nakoniec sa TOE musí namontovať do prípravku LFI a musí sa vykonať útok.

Tabuľka 15: Kombinované základné hodnotenie laserového vstrekovania porúch a odstraňovania obalu pri stredne náročnej príprave obalu

LFI v balíku na balíku bez závislosti od podporného zariadenia (tučný text predstavuje dodatočný odpor poskytovaný balíkom)			
Faktory	**Popis**	**Identifikácia**	**Využívanie**
Uplynulý čas	Na nastavenie zariadenia a vykonanie útoku útočník by strávil viac ako týždeň, ale menej ako mesiac.	< jeden mesiac (3)	< jeden týždeň (4)
Odbornosť	Vyžadujú sa len odborné znalosti, pokiaľ ide o napadnutú funkčnosť.	Znalec (2)	Znalec (2)
Znalosť TOE	Útok je možné vykonať pomocou verejne dostupných informácií.	Verejnosť (0)	Verejnosť (0)
Prístup k TOE	Počas oddeľovania a otvárania sa s najväčšou pravdepodobnosťou zničia niektoré TOE, ale pred úspešnou prípravou ich pravdepodobne nebude viac ako 10. **Na základe vyššie uvedeného opisu odbalenia sa príprava SoC na vykonanie útoku považuje za náročnú (stredne náročná).**	<10 vzoriek (0) **Stredné úsilie pri príprave** **+(1)**	<10 vzoriek (0) **Stredné úsilie pri príprave** **+(2)**
Zariadenie	Vyžaduje sa len štandardné nastavenie LFI.	Špecializované (3)	Špecializované (4)
Otvorené vzorky		nevyžaduje sa (0)	-
Medzisúčet		9	12
Celkom		**21 (rozšírené základné)**	

Príklad 3

Prienik ľahkej chyby na zraniteľnom TOE v konfigurácii čip na čipe s prepojeniami s vysokou rýchlosťou prenosu dát. Ide o ten istý TOE ako v príklade 1, ale opäť v inom type obalu. Tieto vysokorýchlostné prepojenia si vyžadujú kritické smerovanie na zaručenie integrity signálu. Čipy sú zlepené, čo mimoriadne sťažuje ich oddelenie bez poškodenia. Rozstup medzi kontaktmi je malý. Po oddelení je na opätovné prepojenie oboch čipov potrebná doska s rozhraním. Pripojenie dosky s rozhraním k obom čipom pomocou spojenia vodičov nie je triviálne kvôli malej rozteči a požiadavkám na smerovanie. Ďalšie predpoklady: Bezpečnostné požiadavky na balenie zo strany vývojára, horná doska úplne zakrýva TOE.

Tabuľka 16: Kombinované základné hodnotenie laserového vstrekovania porúch a odstraňovania obalu pri vysokom úsilí pri príprave obalu

LFI v balíku čip na čipe so závislosťou od podporného čipu (tučný text predstavuje dodatočný odpor poskytovaný balíkom)			
Faktory	**Popis**	**Identifikácia**	**Využívanie**
Uplynulý čas	Na nastavenie zariadenia a vykonanie útoku útočník by strávil viac ako týždeň, ale menej ako mesiac.	< jeden mesiac (3)	< jeden týždeň (4)
Odbornosť	Vyžadujú sa len odborné znalosti, pokiaľ ide o napadnutú funkčnosť.	Znalec (2)	Znalec (2)
Znalosť TOE	Útok je možné vykonať pomocou verejne dostupných informácií.	Verejnosť (0)	Verejnosť (0)
Prístup k TOE	**Počas oddeľovania a otvárania bude pravdepodobne zničených mnoho TOE, najmä počas zisťovania najlepšieho prístupu.** **Na základe opisu odbalenia sa považuje za ťažké pripraviť (vysoké úsilie na prípravu) SoC na vykonanie útoku.**	<10 vzoriek (0) **Vysoké úsilie pri príprave** **+(2)**	<10 vzoriek (0) **Vysoké úsilie pri príprave** **+(4)**
Zariadenie	Vyžaduje sa štandardné nastavenie LFI.	Špecializované (3)	Špecializované (4)
Otvoriť vzorky		nevyžaduje sa (0)	-
Medzisúčet		10	14
Celkom		**24 (rozšírený základ)**	

34. PRÍLOHA 8: MINIMÁLNE POŽIADAVKY NA ITSEF PRE HODNOTENIA BEZPEČNOSTI SMART KARIET A PODOBNÝCH ZARIADENÍ

ÚČEL

V tejto prílohe sa uvádzajú požiadavky týkajúce sa minimálnych schopností, ktoré musí mať akreditované ITSEF vo svojich priestoroch na vykonávanie rôznych typov útokov uvedených v prílohe 7, UPLATNENIEPOTENCIÁLU ÚTOKU NA SMART KARTY A PODOBNÉ ZARIADENIA. Tieto kapacity zahŕňajú znalosti a zručnosti ich hodnotiteľov a potrebné vybavenie a opis metodiky hodnotenia, ktoré sú potrebné na vykonanie uvedených útokov.

Schopnosti majú pokryť minimálne požiadavky na vykonanie hodnotenia integrovaného obvodu (IC), kryptografickej knižnice, platformy a karty integrovaného obvodu (ICC) s dostatočnými zárukami.

Cieľom tejto prílohy nie je poskytnúť návod na to, ako sa má vykonať hodnotenie IC, kryptografickej knižnice, platformy (IC + OS) alebo ICC (IC + OS + aplikácia), ale poskytuje usmernenie na zabezpečenie toho, aby ITSEF mali potrebné kapacity na vykonávanie takýchto hodnotení.

KONKRÉTNY STAV

Žiadne.

KRÍŽOVÝ ODKAZ NA KAPITOLU(-Y), V KTOREJ(-ÝCH) SÚ PRVKY VYHLÁSENÉ ZA UPLATNITEĽNÉ

Kapitola 6, ŠPECIFICKÉ POŽIADAVKY VZŤAHUJÚCE SA NA CAB Kapitola 8, ŠPECIFICKÉ KRITÉRIA A METÓDY HODNOTENIA.

1 POŽADOVANÉ SCHOPNOSTI PRE HODNOTENIE IC

1.1 Prehľad hodnotenia IC

Hodnotenie IC si vyžaduje rozvoj špecifických zručností a vedomostí. Cieľom je poskytnúť technické usmernenie pre hodnotiteľov, ktorí vykonávajú hodnotenie IC, a odhaliť súvisiace minimálne požiadavky. Na dosiahnutie tohto cieľa budú nasledujúce oddiely obsahovať:

- Pochopenie návrhu bezpečného integrovaného obvodu (ako je smart karta, bezpečný prvok atď.) a výrobného procesu vo všeobecnosti návrhu a výrobného procesu integrovaného obvodu (pozri časť 1.2).
- Pochopenie technológie bezpečných integrovaných obvodov, jej základných princípov a vývojových zariadení používaných výrobcami bezpečných integrovaných obvodov (pozri časť 1.3).
- Znalosti a skúsenosti s technikami fyzického útoku na hardvér, ktoré by mohli ohroziť zabezpečený integrovaný obvod, a schopnosť používať súvisiace zariadenia na zaťaženie hardvérových vrstiev. To zahŕňa pochopenie základných fyzikálnych princípov IC (pozri časť 1.4).
- Znalosti a skúsenosti s fyzickými narušeniami, ktoré by mohli zmeniť bezpečné správanie IC s cieľom následne znížiť bezpečnosť zariadenia založeného na IC. Schopnosť používať súvisiace

zariadenia na vykonávanie fyzických narušení a pochopenie súvisiacich fyzických účinkov na hardvér (pozri oddiel 1.4).

- Znalosti a skúsenosti v oblasti techník kryptografických útokov a schopnosť vykonávať analýzu (vrátane postupov zachytávania údajov a spracovania signálov) (pozri časť 1.4).

1.2 Proces návrhu a výroby integrovaných obvodov

Hardvér a softvér integrovaných obvodov vo všeobecnosti vyvíjajú rôzne spoločnosti. Tieto komponenty sa potom integrujú a do karty sa vkladajú ďalšie údaje dôležité z hľadiska bezpečnosti.

Bezpečnostné ciele IC sú dvojaké:

- Zabezpečenie úrovne bezpečnosti karty v teréne.
- Udržiavanie úrovne zabezpečenia počas celého procesu vývoja a výroby.

Hoci sa mnohí odborníci sústreďujú na bezpečnosť v teréne (keďže smart karta sa dodáva do nepriateľského, neregulovaného prostredia a môže byť predmetom manipulácie), dôležitá je aj bezpečnosť počas procesu vývoja, výroby a personalizácie. Bezpečnostné ciele, na základe ktorých sa posudzuje komponent smart karty, veľmi závisia od kontextu aplikácie, ktorý zasa môže závisieť od procesu výroby a personalizácie. Najmä personalizácia ovplyvňuje bezpečnostné funkcie, ktoré má smart karta poskytovať.

CEM znázorňuje ideálny proces vývoja, ktorý začína definíciou požiadaviek, po ktorej nasleduje proces návrhu, implementácie, testovania, akceptácie, dodania a používania. Pri pohľade na komponenty zloženého produktu sa tento proces musí interpretovať a usporiadať inak.

Výrobca čipov napríklad vyvíja návrh hardvéru a softvéru na testovanie čipov. Od vývojára softvéru dostane softvér na vytvorenie obrazu ROM. Potom sa súbory s maskou pošlú výrobcovi masky. Masky alebo sieťovky sa vrátia výrobcovi čipu. Po výrobe waferov sa čipy otestujú a inicializačné údaje (transportné kľúče, údaje o sledovateľnosti) sa vložia do EEPROM (alebo inej nevolatilnej pamäte). Inicializačné údaje definuje výrobca karty. Operačné matrice sa dodávajú alebo priamo zabudovávajú do modulov. Ochrana dodávky matrice môže byť zložitá. Mechanizmus autentizácie realizuje výrobca softvéru, ale používa ho výrobca karty (alebo personalizačné centrum). Kľúče generuje výrobca karty a do karty ich vkladá výrobca čipu pomocou postupu (pre diverzifikáciu atď.) definovaného výrobcom karty.

V prípade integrovaných obvodov s pamäťou flash je možností ešte viac. IC sa môže dodávať buď bez akéhokoľvek obsahu, čo vyžaduje, aby vývojár softvéru použil testovacie rozhranie na inicializáciu flash pamäte s firmvérom, zavádzačom alebo so zavádzacím softvérom, hardvérovými ovládačmi alebo dokonca s operačným systémom. V každom prípade musí správne používanie autentizačných mechanizmov zabezpečiť, aby sa integrita obsahu flash pamäte a prístup k funkcii sťahovania IC riešili bezpečným spôsobom.

Tieto príklady ukazujú, že skutočný vývojový proces môže byť zložitejší, ako predpokladá CEM pre bežné softvérové alebo hardvérové produkty, pretože celý životný cyklus smart karty môže byť pomerne zložitý. Vstupy a výstupy nie sú vždy také jednoduché, ako predpokladá CEM. V dôsledku toho sa musia príslušné komponenty záruk CEM (napríklad doručovanie) podľa potreby interpretovať, spresniť
a zmeniť ich usporiadanie. Okrem toho musí zabezpečiť, aby procesy rôznych komponentov (a ich opis
v zmysle komponentov záruk podľa spoločných kritérií) do seba zapadali.

Hodnotiteľ musí rozumieť dodávateľskému reťazcu smart kariet a jeho integrácii do kontextu aplikácie, aby mohol vhodným spôsobom interpretovať požiadavky bezpečnostných záruk CEM. Tieto požiadavky bezpečnostných záruk sú najmä:

- Usmernenie
- Doručovanie
- Postup prípravy
- Nástroje a techniky
- Definícia životného cyklu
- Bezpečnosť vývoja

Okrem toho rozdiely medzi hodnotením smart kariet a hodnotením softvéru znamenajú, že je potrebná

aj interpretácia komponentov záruk CC časť 3 tried ASE, ADV, ATE a AVA.

Tieto výklady komponentov záruk CC časť 3 a ďalšie usmernenia sú opísané v niekoľkých podporných dokumentoch EUCC pre smart karty a podobné zariadenia, ktoré sú uverejnené na webovej stránke agentúry ENISA venovanej certifikácii kybernetickej bezpečnosti.

1.3 Technológia integrovaných obvodov smart kariet

Hodnotiteľ musí rozumieť technológii integrovaných obvodov smart kariet a základným princípom v rozsahu potrebnom na pochopenie konštrukčných rozhodnutí výrobcu integrovaného obvodu. Vyžadujú sa základné znalosti o:

- Elektrónová teória polovodičov (fyzika) a elektrické správanie polovodičov a tranzistorov.
- Fyzikálne a elektrické správanie všetkých štandardných materiálov používaných pri výrobe integrovaných obvodov (napríklad kremík, polykremeň, kov, izolačný a pasivačný materiál).
- Výrobné kroky a výsledná štruktúra vrstiev na povrchu čipu.

Okrem toho musí mať hodnotiteľ podrobné znalosti o:

- Fyzické rozloženie (implementácia na povrchu polovodiča) štandardných buniek (jednoduché hradlá), pamäťových buniek (E2PROM, RAM, ROM) a pamäťových blokov.
- Princípy rozvrhnutia a metódy smerovania a vrstvenia.
- Digitálne a analógové obvody (digitálne hradlá rôznej zložitosti a štandardné analógové obvody).
- Statické a dynamické správanie digitálnych a analógových obvodov.
- Architektúra a funkčnosť mikrokontroléra.
- Realizácia štandardných obvodov používaných v mikrokontroléroch.

Hodnotiteľ musí byť schopný porozumieť schémam (blokové schémy, schémy na úrovni hradiel a tranzistorov). Funkčné komponenty môžu byť opísané vo forme štandardných schém alebo v zdrojoch VHDL.

Hodnotiteľ musí mať znalosti o procese návrhu VLSI a musí rozumieť procesu od schém alebo zdrojov VHDL (logické zobrazenie čipu) až po skutočné rozloženie a kocky/waferov (fyzické zobrazenie). Hodnotiteľ musí rozumieť procesom technologickej kvalifikácie, funkčného testovania, charakterizácie a testovania spoľahlivosti.

Hodnotiteľ musí rozumieť vývojovému zariadeniu, ktoré výrobcovia používajú pre softvér mikrokontrolérov. Patria sem simulátory, emulátory, analyzátory protokolov a špeciálne vyhodnocovacie softvérové masky. Hodnotiteľ musí byť schopný čítať zdrojový kód mikrokontrolérov a vyvíjať softvér na penetračné testy a iné vyšetrovania.

Preto musí hodnotiteľ rozumieť inštrukčnej sade CPU, mape pamäte a použitiu ostatných periférnych jednotiek mikrokontroléra.

1.4 Útoky špecifické pre smart karty

Nasledujúci text poskytuje prehľad o útokoch špecifických pre smart karty. Nejde o úplný zoznam, ale o niekoľko príkladov. Podrobnejšie informácie o špecifických útokoch na smart karty v kontexte hodnotenia založeného na CC nájdete v prílohe 7, UPLATNENIE POTENCIÁLU ÚTOKU NA SMART KARTY A PODOBNÉ ZARIADENIA,

Hodnotiteľ musí mať znalosti o štandardných podvodoch s smart kartami a scenároch útokov a v zásade musí byť schopný vyvinúť nové nápady na takéto útoky. Aby sme boli konkrétnejší, hodnotiteľ musí poznať scenáre útokov na smart karty a softvér smart kariet, ako sú fyzická manipulácia a sondovanie, útoky na poruchy, útoky na vlastné a vynútené úniky, zneužitie testovacích funkcií, útoky na implementáciu kryptografických funkcií implementovaných v hardvéri, softvéri alebo v kombinácii oboch, kryptografické útoky alebo softvérové útoky. Množstvo takýchto scenárov útokov - spolu s citáciami - je opísané v citovanej prílohe.

Hodnotiteľ musí byť schopný prispôsobiť a kombinovať tieto scenáre útoku pre jednotlivé čipy alebo smart karty, ktoré sú predmetom hodnotenia. Počas analýzy zraniteľnosti musí byť hodnotiteľ schopný nájsť možné slabé miesta (v schémach a ich realizácii na čipe a ich kombinácii) a musí byť schopný použiť štandardné techniky na ich posúdenie.

Hodnotiteľ musí mať znalosti a skúsenosti s analýzou porúch integrovaných obvodov, ktoré sa majú použiť na fyzickú manipuláciu a sondovanie. Hodnotiteľ musí aspoň rozumieť fyzikálnym princípom a musí byť schopný pracovať (podľa potreby) so zariadeniami klasifikovanými ako "štandardné" a "špecializované". Okrem toho musí byť hodnotiteľ schopný používať "špeciálne" nástroje s pomocou vyškolených operátorov. Hodnotiteľ musí vedieť, ako sa tieto nástroje a techniky môžu použiť počas analýzy zraniteľnosti s cieľom posúdiť bezpečnostné vlastnosti a funkcie IC. Spôsob a účel použitia zariadení (najmä fokusovaného iónového lúča (FIB), skenovacieho elektrónového mikroskopu (SEM), EMMI alebo E-beam testera) počas posudzovania zraniteľnosti nemusí nevyhnutne zodpovedať očakávaniam obslužného personálu. Hodnotiteľ by mal inštruovať prevádzkový personál, aby sa dosiahlo zmysluplné a nezávislé hodnotenie. Samotný hodnotiteľ by si mal udržiavať dostatočné technické znalosti (napríklad o tom, ako obsluhovať zariadenia na analýzu porúch IC), ktoré sú potrebné na zmysluplné poučenie.

Hodnotiteľ musí mať dostatočné znalosti z teórie pravdepodobnosti a princípov návrhu RNG. Hodnotiteľ musí byť schopný identifikovať a analyzovať tie vlastnosti systému alebo procesu, ktoré majú významný vplyv na rozdelenie náhodných čísel, a posúdiť náhodnosť generovania čísel.

Hodnotiteľ musí mať vedomosti a skúsenosti s inými útokmi na smart karty (útoky na bočné kanály, ako je analýza časovania, diferenciálna analýza výkonu (DPA), diferenciálna analýza EM žiarenia (DEMA), útoky na šablóny (TA); útoky na zavádzanie chýb, ako je DFA a súvisiace útoky) a musí mať vybavenie (fyzické a analytické nástroje) potrebné na vykonanie takýchto útokov. Hodnotiteľ musí byť schopný obsluhovať toto vybavenie (vrátane postupov zachytávania údajov) a vykonávať analýzu (matematiku). Vyžadujú sa znalosti a skúsenosti v oblasti kryptografie a štandardných techník kryptografických útokov pre všetky typy príslušných algoritmov. Základné princípy útokov bočnými kanálmi, ako aj útokov na zavádzanie chýb (ako je diferenciálna analýza chýb (DFA) a iné útoky) musia byť v zásade pochopené. Na úplné preskúmanie potenciálnych slabých miest musí byť hodnotiteľ schopný odhaliť zraniteľnosti súvisiace s takýmito útokmi, ktoré zahŕňajú analýzu EM vyžarovania, jedno- a viaclaserové útoky atď.

Hodnotiteľ musí byť schopný vyvinúť softvér na komunikáciu so smart kartou. Hodnotiteľ preto musí rozumieť podporovanému I/O protokolu, prevádzkovým podmienkam a externému príkazovému rozhraniu, ak sa používa alebo napáda. Hodnotiteľ musí tiež rozumieť bezpečnostným koncepciám softvéru smart kariet vrátane štruktúr súborov, kódovania prístupových práv atď.

Hodnotiteľ musí vedieť, ako zaobchádzať s čítačkami čipových kariet, a musí byť schopný ich upraviť tak, aby sa čipy mohli používať v rôznych obaloch a aby sa mohli použiť neštandardné prevádzkové podmienky. Hodnotiteľ preto musí byť schopný používať štandardné zariadenia, ako sú napäťové zdroje, generátory signálov a funkcií, osciloskopy a spájkovačky. Okrem toho musí hodnotiteľ vedieť, ako fyzicky pripraviť vzorky (napr. otvoriť obal a odstrániť kovové vrstvy); napríklad na uľahčenie sofistikovaných svetelných útokov alebo EM meraní, zabezpečiť prístup k laseru, umožniť sondovanie FIB, umožniť reverzné inžinierstvo atď.

Hodnotiteľ musí byť schopný kombinovať výsledky rôznych vyššie opísaných schopností. To zahŕňa aplikáciu metód analýzy porúch na lokalizáciu komponentov na smart kartách s cieľom posúdiť, či je možné nahradiť konštrukčné údaje, alebo posúdiť efektívnosť rôznych metód útoku na ten istý cieľ.

1.5 Zariadenia na hodnotenie IC

Na vykonanie analýzy zraniteľností, fyzických manipulácií a scenárov útokov uvedených v časti 1.4 musí mať ITSEF neobmedzený prístup k väčšine nástrojov potrebných na vykonanie týchto útokov, musí ich vlastniť a musí byť schopný ich efektívne používať. Kategórie tohto vybavenia sú uvedené ďalej
(v prílohe 7, UPLATNENIE POTENCIÁLU ÚTOKOV NA SMART KARTY A PODOBNÉ ZARIADENIA, sú uvedené ďalšie podrobnosti o potrebnom vybavení s ich kategorizáciou):

- zariadenia na riadenie prostredia (napr. na riadenie komunikácie, napätia, hodín a teploty)
- chemické a mechanické laboratórne vybavenie (napr. na prípravu a analýzu vzoriek)
- Zobrazovacie zariadenia (napr. kamery, mikroskopy, SEM)
- Fyzikálne manipulačné zariadenia (napr. sondážna stanica, fokusovaný iónový lúč)
- Nástroje na analýzu návrhu (napr. na analýzu rozloženia čipu, analýzu RNG)
- Analyzátory protokolov (napr. špionážne zariadenia)
- Logické testovacie nástroje (napr. na testovanie rozhraní, skenovanie zraniteľností)
- Zariadenia na analýzu bočných kanálov (napr. sondy, osciloskopy, analytický softvér)

- Perturbačné zariadenia (napr. generátory impulzov, lasery, smart spúšťanie)

V prípade zariadení zaradených do kategórie "na mieru" musí hodnotiteľ dobre rozumieť základným fyzikálnym princípom a možnostiam nástrojov.

Nástroje musia umožňovať flexibilné použitie v rámci svojich technických limitov. Použitie nesmie byť obmedzené na očakávania obsluhujúceho personálu, ako už bolo opísané v oddiele 1.4. Nástroje musia umožniť hodnotiteľovi prispôsobiť útoky tak, ako to možno predpokladať u expertov na základe posudzovanej implementácie.

2 POŽADOVANÉ SCHOPNOSTI PRE ZLOŽENÉ HODNOTENIA

Zložené hodnotenia vychádzajú z predchádzajúceho certifikovaného produktu. Zložený TOE môže byť IC doplnený o kryptografickú knižnicu, platformu alebo celý ICC vrátane aplikácie. Zvyčajne sa TOE týka softvéru pridaného k certifikovanému základnému produktu.

2.1 Prehľad operačného systému integrovanej karty

2.1.1 Preskúmanie zdrojového kódu

V súčasnosti je väčšina softvéru pre smart karty napísaná v programovacom jazyku C a potom v jazyku Java, zatiaľ čo manuálne programovanie v jazyku Assembler je dnes skôr zriedkavé (s výnimkou špecializovaných základných rutín). Hodnotiteľ potrebuje dôkladnú znalosť použitia jazyka C alebo Java v kontexte špecifickej hardvérovej architektúry a obmedzení smart karty IC; to sa týka najmä obmedzení jazyka Java pre produkty Java Card. (Preto je ďalej uvedená časť 2.4 venovaná virtuálnym strojom.)

Okrem toho je na hĺbkovú bezpečnostnú analýzu potrebná znalosť asemblerového kódu a medzikódu (napríklad bajtového kódu karty Java). Najmä rôzne bezpečnostné vplyvy (a chyby) nemožno pochopiť na úrovni vyššieho jazyka, ako je C alebo Java, pretože sa prejavia až v assemblerovom kóde alebo
v bajtovom kóde. Preto sa výslovne zdôrazňuje dôležitosť pochopenia kódu Assembleru vytvoreného kompilátorom a bezpečnostných vplyvov nástrojov na generovanie.

2.1.2 Natívny vstup/výstup

Natívny vstup/výstup sa vzťahuje na technológie "v spodnej časti" prenosu údajov medzi smart kartou a terminálom (čítačkou smart kariet).

Hodnotiteľ musí rozumieť a byť schopný interpretovať rôzne vrstvy vstupov a výstupov od základnej špecifikácie rozhrania, ako je UART (na odosielanie a prijímanie jednotlivých bajtov); cez základnú štruktúru príkazov smart kariet (APDU - Application Protocol Data Unit); až po úroveň bežne používaných protokolov na výmenu údajov, napr. (T0 / T1 pre kontaktné a TCL / Single Wire Protocol (SWP) pre bezkontaktné.

2.1.3 (Zabezpečenie) Protokol I/O

Na rozdiel od natívneho I/O zahŕňa protokolový I/O bezpečnostné (väčšinou kryptografické) protokoly používané pri komunikácii s smart kartou.

V kontexte protokolov smart kariet je Secure Messaging termín, ktorý zahŕňa bezpečnostné funkcie prenosu údajov medzi smart kartou a terminálom (alebo vzdialeným serverom). Secure Messaging môže zahŕňať vzájomnú alebo jednostrannú autentizáciu medzi smart kartou a hostiteľom, integritu správ, ako aj dôvernosť správ.

Hodnotiteľ musí rozumieť rôznym štandardizovaným protokolom, ktoré existujú pre bezpečné zasielanie správ, ako napríklad špecifikované pre otvorenú platformu, ECC (European Citizen Card), BAC (Basic Access Control), PACE (Password Authenticated Connection Establishment), EAC (Extended Access Control) atď. Tieto normy často umožňujú vysoký stupeň flexibility pri konfigurácii možností zabezpečenia, čo si vyžaduje dôkladnú kontrolu pri hodnotení konkrétneho výberu na základe súboru predpokladaných požiadaviek.

2.1.4 Správa obsahu a zdrojov

Určujúcou úlohou operačného systému je správa výpočtových zdrojov (ako je pamäť, RAM, I/O atď.) a správa prístupu (rozhrania) k týmto zdrojom.

Zatiaľ čo predchádzajúce odseky sa zaoberali komunikáciou medzi smart kartou a vonkajším svetom, tu sa zameriame na správu zdrojov vo vnútri samotnej smart karty.

Hodnotiteľ musí najprv pochopiť štruktúru súborov (napr. koncept hierarchie hlavných súborov, vyhradených súborov a základných súborov) a správu prístupových práv k súborom v rámci operačného systému smart karty. Vyžaduje sa znalosť typov pamäte (EE, Flash, ROM, RAM, špeciálna vyhradená RAM (ako Crypto-RAM, Buffer-RAM)) a postupov správy pamäte (napr. obmedzenia prístupu).

V prípade kariet Java je potrebné dôkladne pochopiť koncept bezpečnostných domén a izolácie aplikácií (predtým firewall). Je to dôležité najmä pre správu aplikácií, ktorá sa týka bezpečného načítavania, správy a odstraňovania aplikácií, ako aj prístupových práv týchto aplikácií k prostriedkom smart karty.

2.2 Proces výrobného cyklu IC karty

Kartu IC vyrába vývojár softvéru na základe IC alebo platformy (iného) výrobcu. Softvér pre IC sa nazýva vstavaný softvér.

Bezpečnostné ciele karty IC sú dvojaké:

- Zabezpečenie úrovne bezpečnosti karty IC v teréne.
- Udržiavanie úrovne zabezpečenia počas celého procesu vývoja a výroby.

Hoci sa mnohí odborníci sústreďujú na bezpečnosť v teréne (keďže karta IC sa dodáva do nehostinného, neregulovaného prostredia a môže byť predmetom manipulácie), dôležitá je aj bezpečnosť počas procesu vývoja, výroby a personalizácie. Bezpečnostné ciele, na základe ktorých sa posudzuje komponent smart karty, budú do veľkej miery závisieť od kontextu aplikácie, ktorý môže byť závislý od procesu výroby a personalizácie. Najmä personalizácia ovplyvňuje bezpečnostné funkcie, ktoré má smart karta poskytovať.

CEM znázorňuje ideálny proces vývoja, ktorý začína definíciou požiadaviek, nasleduje proces návrhu, implementácie, testovania, akceptácie, dodania a používania. Pri pohľade na komponenty zloženého produktu sa tento proces musí interpretovať a usporiadať inak.

Napríklad vstavaný softvér je vyvinutý pre konkrétny integrovaný obvod. IC prešiel hodnotením hardvéru a poskytuje dokumenty s bezpečnostnými pokynmi, aby bol zložený produkt bezpečný. Táto sprievodná dokumentácia obsahuje informácie o tom, ako sa musí IC používať, aby bola karta IC bezpečným produktom - zvyčajne je v nich zahrnutých niekoľko informácií, od bezpečného používania kryptografických komponentov, generátora náhodných čísel a bezpečného postupu zavádzania. Zložený hodnotiteľ preto musí chápať význam povinnej sprievodnej dokumentácie týkajúcich sa IC (bezpečnosti). Musí posúdiť, či bezpečnostné mechanizmy, ktoré boli implementované do vstavaného softvéru, spĺňajú požiadavky uvedené v dokumentoch s (bezpečnostnými) usmerneniami.

Na zostavovaní karty IC sa podieľa niekoľko subjektov. V prípade integrovaných obvodov založených na pamäti ROM sa vložený softvér odošle výrobcovi integrovaného obvodu, zatiaľ čo v prípade integrovaných obvodov založených na pamäti flash môže načítanie softvéru vykonať vývojár vstavaného softvéru alebo dokonca tretia strana. Po zostavení karty IC ju vývojár softvéru pripraví na dodanie konečnému zákazníkovi alebo personalizačnej kancelárii. To môže zahŕňať predbežnú personalizáciu IC karty a aplikácií. Tieto procesy zvyčajne zahŕňajú ochranu pomocou kryptografických operácií. Zložený hodnotiteľ musí pochopiť, ako sú všetky tieto bezpečnostné mechanizmy implementované, aby sa zaručil bezpečný proces výroby IC karty (vrátane personalizácie).

Vývojár vstavaného softvéru môže zaviesť bezpečnostné mechanizmy na zmenu správania karty integrovaného obvodu, napríklad prostredníctvom mechanizmu záplatovania. Mechanizmus záplatovania umožňuje načítať nový (potenciálne škodlivý) programový kód na kartu IC Card a vyžaduje autentizáciu pred použitím záplaty. Zložený hodnotiteľ musí byť schopný posúdiť bezpečnostné mechanizmy zahrnuté v takomto opravnom mechanizme.

Tieto príklady ukazujú, že skutočný proces vývoja môže byť zložitejší ako proces, ktorý predpokladá CEM pre bežné softvérové alebo hardvérové produkty, pretože celý životný cyklus smart karty môže byť pomerne zložitý. Tento životný cyklus zahŕňa niekoľko "hráčov", ako napríklad výrobcu integrovaného obvodu, výrobcu zabudovaného softvéru, vydavateľa karty (ktorý zvyčajne zostáva právnym vlastníkom karty aj po jej vydaní), poskytovateľov aplikácií a koncových používateľov ("držiteľov karty"). Vstupy a výstupy nie sú vždy také jednoduché, ako očakáva CEM, pretože medzi uvedenými subjektmi dochádza ku komplexnej interakcii, pokiaľ ide o bezpečnostné relevantné postupy, ako je výmena kódu, správa kľúčov alebo načítanie appletu. V dôsledku toho sa musia príslušné komponenty záruk CEM (napríklad doručovanie) interpretovať, spresniť a v prípade potreby zmeniť ich usporiadanie. Okrem toho sa musí zabezpečiť, aby procesy rôznych komponentov (a ich opis v zmysle komponentov záruk CC časť 3) do seba zapadali.

Hodnotiteľ musí rozumieť dodávateľskému reťazcu smart kariet a jeho integrácii do aplikačného kontextu, aby mohol vhodným spôsobom interpretovať požiadavky bezpečnostných záruk podľa časti 3 CC. Tieto požiadavky bezpečnostných záruk sú najmä:

- Usmernenie,
- Doručovanie,
- Postup prípravy,
- Nástroje a techniky,
- Definícia životného cyklu,
- Bezpečnosť vývoja.

Okrem toho rozdiely medzi hodnotením smart kariet a hodnotením softvéru znamenajú, že je potrebná aj interpretácia komponentov záruk podľa spoločných kritérií tried ASE, ADV, ATE a AVA.

Tieto výklady komponentov záruk podľa časti 3 CC a ďalšie usmernenia sú opísané v niekoľkých podporných dokumentoch EUCC pre smart karty a podobné zariadenia, ktoré sú uverejnené na webovej stránke agentúry ENISA venovanej certifikácii kybernetickej bezpečnosti.

2.3 Kryptografický softvér

Zložené produkty môžu obsahovať (čiastočné) softvérové implementácie kryptografických algoritmov. Okrem pochopenia algoritmov by mal hodnotiteľ rozumieť aj aspektom interakcie medzi softvérom a hardvérom a vplyvu útokov na softvérovú implementáciu.

2.3.1 Kryptografická knižnica využívajúca kryptografický koprocesor

Táto časť sa týka typicky asymetrickej kryptografie využívajúcej kryptografický koprocesor, napríklad RSA, ECC, ale môže sa týkať aj symetrických algoritmov, ktoré sa nachádzajú na kryptografickom akcelerátore.

Takéto implementácie kombinujú softvérový algoritmus so špeciálnym súborom kryptografických funkcií. Obidve tieto možnosti sa vzhľadom na povahu kryptografického akcelerátora úzko dopĺňajú. Hodnotiteľ musí byť schopný identifikovať slabé miesta v interakcii medzi hardvérom a softvérom.

Existuje značné množstvo rôznych implementácií hardvérovo akcelerovaných algoritmov, najmä pokiaľ ide o veľké celočíselné operácie. V dôsledku toho je potrebná dobrá znalosť rôznych implementácií a silné algebraické a aritmetické matematické zázemie.

Okrem toho môže algoritmy ohroziť veľké množstvo spôsobov útoku a mnohé z nich sú špecifické pre implementáciu. Preto je veľmi dôležité, aby mal hodnotiteľ dobré znalosti o útokoch a protiopatreniach, aby mohol poskytnúť hĺbkovú analýzu zabudovanej kryptografickej knižnice.

Okrem toho hodnotiteľ nebude môcť v tejto fáze hodnotenia predpokladať konkrétne použitie algoritmu. Napríklad formát vstupných údajov musí zostať agnostický. Hodnotiteľ preto musí vziať do úvahy rôzne scenáre zahŕňajúce najreprezentatívnejšie kryptografické protokoly, ktoré sa potenciálne spoliehajú na kryptografické algoritmy.

2.3.2 Kryptografický softvér bez špecializovanej hardvérovej (HW) podpory

Rôzne implementácie tajných kľúčov bez akejkoľvek HW podpory alebo s čiastočnou HW podporou možno nájsť vo viacerých produktoch. Takéto softvérové implementácie môžu zahŕňať niekoľko protiopatrení, ako sú náhodné permutácie, fiktívne operácie alebo náhodné maskovanie, ako sa

uvádza v rôznych publikáciách na ochranu produktu pred útokmi postranných kanálov prvého a vyššieho rádu. Veľmi dôležitá je aj analýza manipulácií s kľúčovými bitmi (bajtmi), ktoré musia chrániť pred inými štatistickými útokmi, ako sú útoky šablón.

Je veľmi dôležité, aby mal hodnotiteľ dobré znalosti o rôznych technikách útokov bočnými kanálmi a chybami, ktoré môžu všetky tieto protiopatrenia prekonať, ak nie sú dostatočne silné ani správne implementované.

Hodnotiteľ rozumie algoritmom, ktoré patria do rozsahu hodnotenia TOE. Môžeme uviesť nasledujúce prípady softvérovo implementovaných algoritmov, ktoré sa často vyskytujú v produktoch:

- "samostatná" implementácia AES, DES (napriek existujúcej HW podpore sa stále používajú SW implementácie). Celá implementácia sa vykonáva v softvéri, ktorý sa spolieha na súbor inštrukcií poskytovaných jadrom integrovaného obvodu (CPU).
- Zmiešaná softvérovo-hardvérová implementácia DES a AES, kde sa k zrýchleniu, ktoré ponúka HW, vyžaduje ďalší softvér a protiopatrenia.
- Implementácia algoritmov, pre ktoré zvyčajne neexistuje žiadna HW podpora na smart kartách, ako napr:
  - Hashovacie algoritmy: Sha1, Sha2, Sha3, Ripemd160, Md5 atď...
  - Rôzne autentizačné algoritmy pre mobilné siete (Milenage, TUAK; okrem toho množstvo vlastných algoritmov).
  - Iné algoritmy tajných kľúčov z rôznych štandardov NIST alebo národných schém.

2.4 Virtuálny stroj

Virtuálny počítač je podľa definície softvérová implementácia počítačového prostredia, v ktorom možno nainštalovať a spustiť operačný systém alebo program. Hodnotiteľ musí rozumieť tomu, ako virtuálny stroj a prostredie na spúšťanie funguje a chráni bezpečnostné aktíva, ktoré sa na túto platformu spoliehajú. Vyžadujú sa rôzne základné znalosti a zručnosti:

- Všeobecné znalosti a skúsenosti s interpretovanými jazykmi, ako je Java Card, so špecifickými znalosťami architektúry a častí virtuálneho stroja, podporovanej inštrukčnej sady a dátových typov a štruktúr.
- Znalosť rôznych programovacích jazykov používaných pre natívne časti a implementáciu interpretu (nižšie vrstvy) a tiež pre aplikácie (vyššie vrstvy).
- Vyžadujú sa znalosti a skúsenosti s vývojovým procesom a príslušnými nástrojmi pre rôzne časti platformy. Vyžaduje sa znalosť kompilátorov, konvertorov a simulátorov, ako aj s nimi súvisiacich typov a konfigurácií medziproduktov a konečných súborov.

2.4.1 Bežecké prostredie

Hodnotitelia musia pochopiť, ako prostredie Runtime Environment (RE) zabezpečuje dodržiavanie bezpečnostného modelu virtuálnej platformy. To zahŕňa hlboké znalosti o vzťahoch a interakciách medzi RE, operačným systémom, aplikáciami a hardvérom, o mechanizmoch životnosti a transakcií RE, o tom, ako RE umožňuje izoláciu aplikácií a mechanizmy zdieľania údajov a ako sa aplikácie načítavajú
a spravujú, sú súčasťou základných znalostí o RE, ktoré je potrebné hlboko pochopiť.

2.4.2 Rozhranie na programovanie aplikácií

Rozhranie pre programovanie aplikácií (API) definuje súbor služieb, ktoré sú k dispozícii vývojárom aplikácií a poskytujú systémové služby, ako je správa aplikácií, správa transakcií, komunikácia alebo kryptografické funkcie. Hodnotitelia musia poznať rozsah služieb API a spôsob, akým aplikácie pristupujú k službám RE, a ich bezpečnostné dôsledky. Služby API pre overovanie držiteľov kariet, správu obsahu kariet alebo kryptografické operácie sú príkladmi kritických služieb, ktorým musia hodnotitelia veľmi konkrétne rozumieť. Vyžaduje sa aj schopnosť vyvíjať a používať rôzne poskytované API s cieľom vyvíjať aplikácie na testovanie bezpečnosti.

2.5 Útoky

V nasledujúcom texte bude uvedený stručný prehľad typických útokov, ktoré je potrebné zohľadniť pri zložených hodnoteniach. Úplnejší zoznam je uvedený v prílohe 7, UPLATNENIE POTENCIÁLU ÚTOKOV NA SMART KARTY A PODOBNÉ ZARIADENIA. Táto časť sa vo veľkej miere prekrýva
s časťou 1.4 venovanou hodnoteniu integrovaných obvodov, ale teraz sa zameriava na vstavaný

softvér, ktorý sa má pridať v rámci zloženého hodnotenia, a na vzájomné pôsobenie medzi už certifikovanou(-i) časťou(-ami) a novým softvérom.

Zvyčajne je potrebné vykonať niektoré dodatočné útoky na hardvér, hoci hardvér patrí k už certifikovanej časti: Hodnotiteľ sa bude musieť prostredníctvom meraní bočných kanálov a útokov na poruchy uistiť, že softvér správne využíva funkcie hardvérovej ochrany a v prípade potreby pridáva ďalšiu ochranu. Môže sa napríklad vyžadovať, aby sa určitým spôsobom nakonfigurovali registre, správne interpretovali pokusy o útok hlásené hardvérom alebo implementovali softvérové protiopatrenia na zvýšenie odolnosti voči bočným kanálom alebo injektovaniu chýb. Musí sa zabezpečiť, aby TOE ako celok udržiaval požadovanú úroveň bezpečnosti, a hodnotiteľ musí zvážiť aj účel, prípady použitia a frekvenciu používania kryptografických kľúčov, algoritmov a tajných údajov uložených v TOE. Znalosti potrebné na vykonanie týchto útokov sú totožné s tými, ktoré sú opísané v príslušnom odseku v časti 1.4.

Ďalšou témou, ktorá sa týka správnej súhry hardvéru a softvéru, sú útoky na generátor náhodných čísel. Opäť je potrebné overiť správne používanie hardvérového TRNG a ďalších softvérových opatrení, ako je následné spracovanie a on-line testovanie náhodných čísel. Metódy útoku zahŕňajú hardvérové útoky, ako je napríklad injektovanie poruchy, a softvérové nástroje, ako je napríklad štatistická analýza.

Hodnotiteľ sa zameriava predovšetkým na vstavaný softvér implementovaný nad už certifikovanou časťou. Vstavaný softvér môže byť veľmi zložitý a hodnotiteľ musí dobre porozumieť jeho architektúre, rozhraniam a protokolom používaným na externú komunikáciu, ako aj prostriedkom, ktoré má chrániť. Hodnotiteľ musí byť schopný preskúmať kód a zároveň sledovať používanie aktív a identifikovať zraniteľnosti.

Pri útoku na softvérovú implementáciu z externých rozhraní je veľmi dôležité, aby bol hodnotiteľ schopný komunikovať s TOE, posielať ľubovoľné príkazy a vykonávať všetky stavy životného cyklu. Hodnotiteľ bude mať vedomosti o nástrojoch na ladenie softvéru a na ich efektívne ovládanie musí mať vedomosti o programovacom jazyku použitom na implementáciu, o inštrukciách assembleru dostupných na CPU a o funkciách debuggeru (body prerušenia, kontrola pamäte). Podpornou technikou je použitie automatizovaných nástrojov na zdrojový kód, ktoré vykonávajú statickú analýzu. Hodnotiteľ musí byť schopný interpretovať a posúdiť výsledky.

Okrem toho niektoré TOE, ako napríklad karty Java, môžu umožňovať inštaláciu ďalšieho softvéru, napríklad appletov. V takom prípade musí byť hodnotiteľ schopný nahrať na kartu ďalšie applety.
V tomto prípade sú potrebné dobré programátorské zručnosti a presná znalosť vnútorných oddeľovacích mechanizmov TOE, ako sú firewally, správa pamäte a overovanie bajtkódu.

Na základe svojich znalostí o TOE a technických schopností opísaných v predchádzajúcich odsekoch musí hodnotiteľ vypracovať scenáre útoku zamerané na odhalenie citlivých aktív alebo obídenie zamýšľanej bezpečnostnej funkcie TOE. Môže ísť o logické útoky (napr. vedľajšie účinky alebo neúmyselné účinky legálnych príkazov a funkcií API, chybné príkazy, parametre alebo zámena vnútorného stavu TOE) na dostupné rozhrania alebo o kombináciu logických a hardvérových útokov (ako je napr. injektovanie poruchy). Široká škála nápadov na útok je uvedená v prílohe 7, UPLATNENIE POTENCIÁLU ÚTOKU NA SMART KARTY A PODOBNÉ ZARIADENIA.

Okrem toho musí hodnotiteľ vyvinúť nové útoky alebo upraviť a prispôsobiť štandardné útoky na posúdenie konkrétnej implementácie aktuálneho TOE. Aby bol hodnotiteľ úspešný, musí vykonať dôkladnú analýzu zraniteľností a mať dobré znalosti o všetkých technológiách opísaných v častiach 2.1 až 2.4 tejto kapitoly a o možných útokoch proti nim.

2.6 Vybavenie na hodnotenie zložených materiálov

Pri zloženom hodnotení sa neočakáva použitie zariadenia na analýzu porúch na mieru, pretože vnútorná odolnosť TOE proti fyzickým útokom už bola preskúmaná počas hodnotenia IC a tento druh útokov nie je ovplyvnený vstavaným softvérom. Na druhej strane, väčšina IC vykazuje niektoré zostávajúce úniky alebo citlivosť na poruchy, ktoré by mohol útočník využiť, ak zabudovaný softvér neimplementuje dodatočné protiopatrenia. Napokon, softvérové útoky a kombinované útoky sa môžu skúmať len počas zloženého hodnotenia, pretože sú plne spojené s vstavaným softvérom.

Aby bolo možné vyhodnotiť odolnosť konečného produktu, musí mať ITSEF neobmedzený prístup k zariadeniam a nástrojom, ktoré možno použiť na vyššie uvedenú triedu útokov. Kategórie požadovaného vybavenia zahŕňajú:

- zariadenia na riadenie prostredia (napr. na riadenie komunikácie, napätia, hodín a teploty)
- chemické a mechanické laboratórne vybavenie (napr. na prípravu a analýzu vzoriek)
- Zobrazovacie zariadenia (napr. kamery, mikroskopy)
- Logické testovacie nástroje (napr. na testovanie rozhraní, skenovanie zraniteľností, testovanie operačného systému, analýzu náhodnosti)
- Analyzátory protokolov (napr. špionážne zariadenia)
- Zariadenia na analýzu bočných kanálov (napr. sondy, osciloskopy, analytický softvér)
- Perturbačné zariadenia (napr. generátory impulzov, lasery, smart spúšťanie)

Na hĺbkovú analýzu sa zdá byť potrebné mať nástroje s dostatočnou flexibilitou na prispôsobenie útokov v súlade s hodnotenou implementáciou. To zahŕňa kombináciu nástrojov (testovacích zariadení) opísanú vyššie.

35. PRÍLOHA 9: UPLATNENIE POTENCIÁLU ÚTOKU NA HARDVÉROVÉ ZARIADENIA S BEZPEČNOSTNÝMI SKRINKAMI

ÚČEL

Táto príloha obsahuje opisy metód útoku, ktoré sú špecifické pre hardvérové zariadenia s bezpečnostnými skrinkami, a poskytuje orientačné metriky na výpočet potenciálu útoku, ktorý útočník potrebuje na uskutočnenie útoku. Základným cieľom je pomôcť vyjadriť celkové úsilie potrebné na uskutočnenie úspešného útoku aplikovaného na prevádzkové správanie hardvérového zariadenia s bezpečnostnou skrinkou.

KONKRÉTNY STAV

Žiadne.

KRÍŽOVÝ ODKAZ NA KAPITOLU(-Y), V KTOREJ(-ÝCH) SÚ TIETO PRVKY VYHLÁSENÉ ZA UPLATNITEĽNÉ

Kapitola 8, ŠPECIFICKÉ HODNOTIACE KRITÉRIA A METÓDY.

1 ÚVOD

Táto príloha obsahuje opisy metód útoku, ktoré sú špecifické pre hardvérové zariadenia s bezpečnostnými skrinkami, a poskytuje orientačné metriky na výpočet potenciálu útoku, ktorý útočník potrebuje na uskutočnenie útoku. Základným cieľom je pomôcť vyjadriť celkové úsilie potrebné na uskutočnenie úspešného útoku aplikovaného na prevádzkové správanie hardvérového zariadenia s bezpečnostnou skrinkou.

Pre každý z útokov sa analyzuje hodnotenie potenciálu útoku podľa tabuliek uvedených v časti 2, Útoky podmienené parametrami.

POZNÁMKA: ďalšia analýza má byť podrobná a má poskytnúť hodnotenia pre konkrétne skutočné prípady a zohľadniť možné protiopatrenia zavedené na zmiernenie útokov.

2 ÚTOKY PODMIENENÉ PARAMETRAMI

2.1 Faktor rozsahu

Veľkosť je jedným z faktorov, ktoré podmieňujú útoky na zariadenia s bezpečnostnými skrinkami. V závislosti od veľkosti zariadenia môže byť útok odlišný a jeho náročnosť sa môže v závislosti od tejto veľkosti zvýšiť alebo znížiť.

Kategorizáciu podľa veľkosti možno vykonať nasledujúcim spôsobom.

2.1.1 Makroskopická mierka

Táto škála zahŕňa útoky na celé zariadenia s ich kompletným vonkajším krytom. Kryt môže mať vo vnútri niekoľko komponentov, ako sú dosky plošných spojov, batérie atď., takže cieľom útoku je získať prístup k vnútorným častiam krytu.

2.1.2 Mikrotechnológia

V tomto prípade sa rozsah týka útokov na zostavené elektronické komponenty, ako sú dosky plošných spojov obsahujúce zbernice a integrované obvody. Útoky sa môžu uskutočniť proti zberniciam prenášajúcim údaje medzi komponentmi alebo možno proti konektorom integrovaných obvodov.

2.1.3 Nano-technológie

Táto stupnica zohľadňuje vnútorné časti integrovaných obvodov. Na vykonanie útokov na vnútorné časti integrovaných obvodov sú potrebné veľmi presné a špecializované nástroje. Cieľom týchto útokov môže byť zmena správania integrovaného obvodu alebo získanie údajov uložených v integrovanom obvode.

2.2 Faktory pre výpočet potenciálu útoku

Poznámka o spoločných kritériách (CC): CC nerozlišujú medzi fázou identifikácie a fázou využívania. Ale vzhľadom na bezpečnostné skrinky sa pri riadení rizík, ktoré vykonáva používateľ certifikátov CC, jednoznačne vyžaduje, aby sa rozlišovalo medzi nákladmi na "identifikáciu" (definícia útoku) a nákladmi na "zneužitie" (napr. po zverejnení skriptu). Preto sa toto rozlíšenie zachováva pri výpočte potenciálu útoku pre hodnotenie bezpečnostných skriniek. Hoci je rozlišovanie medzi identifikáciou a zneužitím nevyhnutné pre hodnotenie bezpečnostnej skrinky na pochopenie a zdokumentovanie cesty útoku, konečný súčet potenciálu útoku sa vypočíta sčítaním bodov týchto dvoch fáz, keďže obe fázy vytvárajú kompletný útok.

2.2.1 Ako vypočítať útok

Identifikácia cesty útoku a analýza a testy zneužitia sú mapované na relevantné faktory: čas útoku, odborné znalosti, znalosť bezpečnostnej skrinky, prístup k TOE na jednotku potrebnú na útok, potrebné vybavenie alebo požadované okno pre príležitosť na vykonanie útoku.

Aj keď útok pozostáva z viacerých krokov, identifikáciu a hodnotenie zneužitia stačí vypočítať pre celú cestu útoku. Nie je povolené vypočítať hodnotenie pre každý krok zvlášť a následne body sčítať, pretože v takom prípade by sa rôzne faktory počítali viacnásobne (napr. nástroje a odborné znalosti). Celá cesta útoku alebo úplný útok sa začína prípravnými činnosťami na útok a končí, keď útočník mohol získať prístup k prostriedku TOE. Úplný útok nekončí porušením SFR, ak sa nepodarilo získať prístup
k prostriedku TOE.

Identifikačná časť útoku zodpovedá úsiliu potrebnému na vytvorenie útoku a preukázanie, že ho možno úspešne aplikovať na TOE (vrátane nastavenia alebo vytvorenia potrebného testovacieho zariadenia). Pri demonštrácii, že útok sa dá úspešne aplikovať, je potrebné zvážiť všetky ťažkosti pri rozširovaní výsledku preukázaného v laboratóriu na vytvorenie užitočného útoku. Nemusí byť potrebné vykonať všetky experimenty na identifikáciu úplného útoku, ale zabezpečiť, aby bolo jasné, či útok skutočne dokazuje, že bol získaný prístup k prostriedku TOE, a či by sa celý útok mohol reálne vykonať. Jeden
z výstupov z identifikačnej fázy predpokladá skript, ktorý poskytuje popis vykonania útoku krok za krokom - predpokladá sa, že tento skript sa použije v časti využitia.

Niekedy fáza identifikácie zahŕňa vývoj nového typu útoku (prípadne vytvorenie nového zariadenia), ktorý sa môže následne použiť na iné TOE. V takomto prípade vzniká otázka, ako naložiť s uplynulým časom a ďalšími parametrami pri opätovnom použití útoku. V tejto prílohe sa vykladá, že čas vývoja (a prípadne odbornosť) na identifikáciu bude zahŕňať čas vývoja na počiatočné vytvorenie útoku až do bodu, ktorý určí príslušný certifikačný orgán. Keď certifikačný orgán určí tento bod, potom sa pri výpočte potenciálu útoku nemôžu použiť žiadne hodnotiace body za vývoj útoku (z hľadiska času alebo odborných znalostí).

Využitie útoku zodpovedá dosiahnutiu útoku na inú inštanciu TOE pomocou analýzy a techník definovaných v identifikačnej časti útoku. Predpokladá sa, že zneužitie vykoná iný útočník, ale technika (a príslušné základné informácie) je k dispozícii pre zneužitie vo forme skriptu alebo súboru inštrukcií definovaných počas identifikačnej časti útoku. Predpokladá sa, že skript identifikuje potrebné vybavenie. To znamená, že uplynulý čas, odborné znalosti a hodnotenia znalostí TOE pre zneužitie budú niekedy nižšie pre zneužitie ako pre identifikáciu.

V mnohých prípadoch hodnotitelia skôr odhadnú parametre pre fázu využívania, než aby vykonali úplné využívanie. Odhady a ich zdôvodnenie budú zdokumentované v ETR.

Na dokončenie výpočtu potenciálu útoku je potrebné sčítať body za identifikáciu a zneužitie, pretože obe fázy vytvárajú kompletný útok. Pri prezentácii výpočtu potenciálu útoku v ETR hodnotitelia uvedú argumentáciu vhodnosti použitých hodnôt parametrov, a preto dajú vývojárovi možnosť spochybniť výpočet pred certifikáciou. Konečný výsledok potenciálu útoku bude preto vychádzať z diskusií medzi vývojárom, ITSEF a CB, pričom CB prijme konečné rozhodnutie, ak sa nedosiahne dohoda.

2.2.2 Uplynulý čas

Uplynulý čas sa počíta v hodinách, ktoré útočník potrebuje na identifikáciu alebo zneužitie útoku. Čas je rozdelený do nasledujúcich intervalov:

Tabuľka 6: *Hodnotenie uplynulého času*

Uplynulý čas	Identifikácia	Využívanie
< jedna hodina	0	0
≤ jeden deň	1	2
≤ jeden týždeň	2	3
≤ jeden mesiac	3	4
> jeden mesiac	5	7

Na účely výpočtu času platí, že deň = 8 hodín, týždeň = 40 hodín a mesiac = 180 hodín.

Ak útok pozostáva z viacerých krokov, možno určiť uplynulý čas a sčítať ho, aby sa dosiahol celkový uplynulý čas pre každý z týchto krokov. Namiesto uplynulého času sa musí použiť skutočný čas práce, pokiaľ neexistuje minimálny Elapsed Time (uplynulý čas) vynútený použitou metódou útoku (napríklad čas potrebný na vykonanie analýzy bočných kanálov alebo čas potrebný na vytvrdnutie epoxidu).
V prípadoch, keď sa počas časti uplynulého času nevyžaduje prítomnosť, sa uplynulý čas musí brať ako uplynulý čas vydelený 3. Myšlienka delenia tromi spočíva v tom, že napr. počítač je schopný pracovať 24 hodín denne, nielen 8 hodín denne.

2.2.3 Odbornosť

Odbornosť sa vzťahuje na úroveň všeobecných vedomostí a zručností v oblasti aplikácie alebo typu produktu (napr. mikroelektronika, chémia, zručnosti pri práci so špecifickými vrtákmi). Na účely bezpečnostných skriniek sú definované tri typy expertov:

- Laici sú v porovnaní s odborníkmi alebo odborníkmi neznalí, bez osobitných odborných znalostí alebo zručností v danej oblasti.
- Odborne spôsobilé osoby majú znalosti v tom zmysle, že poznajú bezpečnostné správanie produktu alebo majú určité (amatérske) odborné znalosti v oblasti práce s konkrétnymi strojmi alebo technikami útokov na bezpečnostné skrinky.
- Odborníci majú profesionálne skúsenosti s konkrétnymi strojmi (manipulácia a konfigurácia), hardvérovými štruktúrami bezpečnostných skriniek, materiálmi atď. implementovanými v danom type produktu alebo systému a s použitými princípmi a koncepciami zabezpečenia.

Odbornosť potrebná na vykonanie útoku môže zahŕňať niekoľko oblastí: chemické látky, schopnosť riadiť sofistikované nástroje atď.

Tabuľka 7: Definícia odbornosti

	Definícia podľa CEM	Podrobná definícia, ktorá sa má použiť v bezpečnostných skrinkách
Odborníci	Oboznámený s implementovanými - Algoritmy - Protokol - Štruktúry hardvéru - Princípy a koncepty bezpečnosti.	Profesionálne skúsenosti s - Bezpečnostnými skrinkami hardvérové štruktúry - konfiguráciou a obsluhou špecifických zariadení (frézy/vŕtačky, röntgenové prístroje) - Znalosťou v oblasti elektroniky a mikroelektroniky (senzory, aktuátory atď.). a - Technikou a nástrojmi na definovanie nových útokov.
Znalec	Oboznámený s - bezpečnostné správanie	Oboznámený so - správaním a klasickými útokmi na bezpečnostné skrinky.
Laici	Žiadne osobitné odborné znalosti	Žiadne osobitné odborné znalosti

Tabuľka 8: Rozsah odborných znalostí

Rozsah odborných znalostí (v poradí podľa rozšírenia znalostí o vybavení alebo TOE)	
Vybavenie: Úroveň odborných znalostí závisí od toho, do akej miery si nástroje vyžadujú skúsenosti s ich riadením: • Frézovacie stroje • Vŕtacie stroje • CNC frézovacie stroje • Röntgenové prístroje • Lasery • Optický mikroskop • Chémia (leptanie, brúsenie) • [..]	**Znalosti:** Úroveň odbornosti závisí od zručností a znalostí: • Informácie o spoločných bezpečnostných skrinkách • Špecifické hardvérové štruktúry TOE • Zásady a koncepcie bezpečnosti • Deštruktívne/nedeštruktívne techniky. • Mikroelektronika (typy senzorov a technológie) • [..]

Môže sa stať, že na sofistikované útoky je potrebných niekoľko typov odborných znalostí. V takýchto prípadoch sa vyberie vyšší z rôznych odborných faktorov.

Bola zavedená nová úroveň "Viacnásobný expert", ktorá umožňuje situáciu, keď sa na úrovni experta vyžadujú rôzne oblasti expertízy pre rôzne kroky útoku. Je potrebné poznamenať, že odbornosť sa musí týkať oblastí, ktoré sú striktne odlišné, ako napríklad manipulácia s HW a strojmi a mikroelektronika alebo chémia.

Tabuľka 9: Hodnotenie odbornosti

	Identifikácia	Využívanie
Laik	0	0
Znalec	1	1
Odborník	2	3
Viacnásobný expert	5	6

2.2.4 Znalosť TOE

V CEM sa uvádza, že "vyžadovať citlivé informácie na účely využívania by bolo neobvyklé", avšak jasne sa rozumie, že akékoľvek informácie požadované na identifikáciu sa nepovažujú za ďalší faktor využívania.

Keďže všetky citlivé a kritické informácie o návrhu musia byť dobre kontrolované a chránené vývojárom, nemusí byť zrejmé, ako pomáhajú pri určovaní vyhradenej cesty útoku. Preto sa vo výpočte potenciálu útoku musí jasne uviesť, prečo sa požadované kritické informácie nedajú nahradiť súvisiacou kombináciou času a odborných znalostí, napr. plánovacou zložkou pre špecializovaný útok.

Použije sa táto klasifikácia:

- **Verejné informácie** o TOE (alebo žiadne informácie): Informácie sa považujú za verejné, ak ich môže ktokoľvek ľahko získať (napr. z internetu) alebo ak ich predajca poskytuje ktorémukoľvek zákazníkovi.
- **Obmedzené informácie** týkajúce sa TOE (napr. získané z technických špecifikácií dodávateľa): Informácie sa považujú za obmedzené, ak sa šíria na požiadanie a ich šírenie je registrované. Vhodným príkladom môže byť funkčná špecifikácia (ADV_FSP).
- **citlivé informácie** o TOE (napr. poznatky o vnútornom dizajne, ktoré možno bude potrebné získať "sociálnym inžinierstvom" alebo vyčerpávajúcim reverzným inžinierstvom). Vhodným príkladom môžu byť informácie o návrhu na vysokej úrovni (HLD), informácie o návrhu na nízkej úrovni (LLD).

Tu treba dbať na rozlišovanie medzi informáciami potrebnými na identifikáciu zraniteľnosti a informáciami potrebnými na jej zneužitie, najmä v oblasti citlivých informácií. Vyžadovanie citlivých informácií na zneužitie by bolo neobvyklé.

Môže sa stať, že pre sofistikované útoky je potrebných niekoľko typov znalostí. V takýchto prípadoch sa vyberie vyšší z rôznych faktorov znalostí.

Tabuľka 10: *Hodnotenie znalostí TOE*

Znalosti	Identifikácia	Využívanie
Verejnosť	0	0
Obmedzené	2	2
Citlivé	3	4

Poznámka: Špecializované odborné znalosti a vedomosti o TOE sa týkajú informácií potrebných na to, aby osoby mohli zaútočiť na TOE. Existuje implicitný vzťah medzi odbornými znalosťami útočníka a schopnosťou efektívne využiť zariadenie pri útoku. Čím slabšie sú odborné znalosti útočníka, tým nižší je potenciál efektívneho využitia zariadenia. Podobne, čím väčšie sú odborné znalosti, tým väčší je potenciál na využitie zariadenia pri útoku.

Hoci je tento vzťah medzi odbornosťou a používaním zariadení implicitný, neplatí vždy - napríklad keď opatrenia prostredia bránia odbornému útočníkovi v používaní zariadení alebo keď sa vďaka úsiliu iných vytvoria a voľne šíria (napr. prostredníctvom internetu) útočné nástroje, ktoré si na účinné použitie vyžadujú len malé odborné znalosti.

2.2.5 Prístup k TOE: Vzorky

Dôležitým faktorom je aj prístup k TOE. Predpokladá sa tu, že útočník získa TOE a že okrem iných faktorov neexistuje žiadne časové obmedzenie pri analýze alebo modifikácii TOE. Rozdiely sú definované v stave a funkčnosti analyzovaného/testovaného zariadenia. Týmto sa nahrádza faktor CEM "Prístup k TOE".

- **Mechanické vzorky** sú nefunkčné. Vzorky v tejto kategórii by mohli byť vonkajšie tienenie TOE, ktoré sa môže použiť na zistenie prístupových bodov. Tieto vzorky by sa mohli použiť len na štúdium mechanickej konštrukcie, ale nie na štúdium vnútornej štruktúry alebo konštrukcie HW.
- **Nefunkčné vzorky** sa môžu použiť na identifikáciu hardvérovej štruktúry TOE s cieľom odhaliť možné protiopatrenia odolné voči manipulácii, reagujúce alebo zjavné protiopatrenia na vykonanie útoku. TOE nefunguje ako v TSF (poškodené TOE, senzory TOE môžu byť deaktivované atď.)

- **Plne funkčné vzorky** fungujúce podľa TSF. Tieto vzorky umožňujú vykonávať skutočné simulácie s TOE.

Tabuľka 11: Hodnotenie prístupu k TOE

Prístup k TOE (vzorky)	Identifikácia	Využívanie
Mechanická vzorka	1	1
Nefunkčné vzorky	2	2
Plne funkčné vzorky	4	4

Ak sa vyžaduje viac ako jedna jednotka, hodnoty sa musia vynásobiť nižšie uvedenými koeficientmi.

Tabuľka 7: Faktor hodnotenia vzoriek

Počet zariadení	Faktor
1	1
2	1,5
3-4	2
5-10	4
>10	5

Mala by sa zohľadniť aj bezpečnostná politika vyjadrená v bezpečnostnom zámere.

2.2.6 Vybavenie a nástroje

Zariadenie sa vzťahuje na vybavenie, ktoré je potrebné na identifikáciu alebo zneužitie určitej zraniteľnosti. Na objasnenie kategórie zariadenia je potrebné zohľadniť cenu a dostupnosť.

- **Štandardné vybavenie** je vybavenie, ktoré je útočníkovi ľahko dostupné buď na identifikáciu zraniteľnosti, alebo na útok. Toto vybavenie sa dá ľahko získať - napr. v blízkom obchode alebo zakúpiť na internete. Toto vybavenie môže pozostávať z jednoduchých útočných skriptov, osobných počítačov, napájacích zdrojov alebo jednoduchých mechanických nástrojov, ako sú štandardné vŕtačky, chemické produkty na bežné použitie, spájkovačky atď.
- **Špecializované vybavenie** nie je pre útočníka ľahko dostupné vzhľadom na jeho cenu alebo veľkosť, ale mohlo by sa získať bez zbytočného úsilia. Mohlo by ísť o nákup stredne veľkého množstva vybavenia (napr. špecializované testovacie pracovisko, chemický pracovný stôl, presné frézy/vŕtačky atď.) alebo vývoj rozsiahlejších útočných scenárov a dôkazov.
- **Vybavenie na mieru** nie je ľahko dostupné verejnosti, pretože môže byť potrebné ho špeciálne

vyrobiť (napr. veľmi sofistikované nástroje), alebo preto, že toto vybavenie je natoľko špecializované, že jeho distribúcia je kontrolovaná, prípadne dokonca obmedzená. Prípadne môže byť zariadenie veľmi drahé (napr. abrazívne laserové zariadenie). Zariadenia na mieru, ktoré si možno prenajať, sa môžu považovať za špecializované zariadenia.

V ideálnom svete je potrebné uviesť definície, aby sme vedeli, aké sú pravidlá a charakteristiky pre priradenie kategórie k zariadeniu alebo súboru zariadení. Do úvahy sa berie najmä cena, vek zariadenia, dostupnosť (verejne dostupné, predaj kontrolovaný výrobcom s možnými viacerými úrovňami kontroly, môže byť prenajaté). Nižšie uvedené tabuľky zostavila skupina odborníkov z odvetvia a **bude potrebné** ich z času na čas **revidovať**.

Rozsah vybavenia, ktoré má potenciálny útočník k dispozícii, sa zvyčajne neustále zlepšuje:

- Zvýšenie výpočtového výkonu
- Zníženie nákladov na nástroje
- Dostupnosť nástrojov môže zvýšiť
- Nové nástroje sa môžu objaviť v dôsledku nových technológií alebo nových foriem útokov.

Môže sa stať, že na sofistikované útoky je potrebných niekoľko typov zariadení. V takýchto prípadoch sa štandardne vyberie vyšší z rôznych faktorov vybavenia.

Hranicu medzi štandardnými, špecializovanými a zákazkovými produktami tu nemožno jasne vymedziť. Hodnotenie nástrojov je len typickým príkladom. Ide o individuálne rozhodnutie v závislosti od „state of the art“ a príslušných nákladov. Nasledujúce tabuľky sú len všeobecným usmernením.

Tabuľka 8: *Hodnotenie nástrojov*

Nástroj	Zariadenie
Spájkovačka	**Štandard**
Tepelné pištole	**Štandard**
Lepidlo	**Štandard**
Ihla	**Štandard**
Injekčná striekačka	**Štandard**
Nože	**Štandard**
Oceľové rezné čepele	**Štandard**
Skrutkovač	**Štandard**
Kladivo	**Štandard**
Štandardná vŕtačka	**Štandard**
Vŕtací lis	**Štandard**
Kotúčová píla	**Štandard**
Píla s radiálnym ramenom	**Štandard**
Napájanie napätím	**Štandard**
Multimeter	**Štandard**
Analógový osciloskop	**Štandard**

Nástroj	Zariadenie
PC alebo pracovná stanica	Štandard
Softvér na analýzu signálov	Štandard
Súbor dentálnych nástrojov (zrkadlá)	Štandard
Borescope	Štandard
Fiberscope	Štandard
Spájkovacia pasta	Štandard
Šunty	Štandard
Drôty a elektrické sondy	Štandard
Pochodeň	Štandard
Mikrokamery	Štandard
Mikrofóny	Štandard
Chemické produkty	Štandard
Antény	Štandard
Frézovací stroj	Špecializované
Pieskovací stroj	Špecializované
CNC frézovací stroj	Špecializované
Laserové frézovanie	Špecializované
Laserové zariadenia	Špecializované
Elektrostatické vysielacie zariadenia	Špecializované
Elektromagnetické vysielacie zariadenia	Špecializované
Tlačiareň s vodivým atramentom	Špecializované
Elektromagnetické vysielacie zariadenia	Špecializované
Procesor signálov a funkcií	Špecializované
Digitálny osciloskop	Špecializované
Analyzátor signálov/protokolov	Špecializované
Nástroje na chemické leptanie (mokré)	Špecializované
Nástroje na chemické leptanie (plazma)	Špecializované
Nástroje na brúsenie	Špecializované
Klimatická komora	Špecializované
Anechoická komora	Špecializované
Štandardné röntgenové zariadenie	Špecializované
Rádiofrekvenčný generátor	Špecializované
Generátor gama žiarenia	Špecializované
Štandardný tomograf	Špecializované
Štandardná termokamera	Špecializované
Systémy FIB	Špecializované

Výrobcovia poznajú odberateľov týchto nástrojov a ich umiestnenie. Väčšinu trhu s použitým náradím tiež kontrolujú výrobcovia.

Efektívne používanie týchto nástrojov si vyžaduje veľmi dlhé skúsenosti a môže ho vykonávať len

malý počet ľudí. Napriek tomu nemožno vylúčiť, že určitý typ zariadenia môže byť dostupný prostredníctvom univerzitných laboratórií alebo rovnocenných zariadení, ale odborné znalosti o používaní tohto zariadenia je pomerne ťažké získať.

Tabuľka 9: *Hodnotenie nástrojov (II)*

Nástroj	Zariadenie
Röntgenový 3-D tomograf	Na mieru
Nové technické nástroje na overovanie dizajnu a analýzu porúch	Na mieru

Všimnite si, že používanie zariadení na mieru by malo viesť minimálne k miernemu potenciálu.

Úroveň "Viaceré na mieru" sa zavádza s cieľom umožniť situáciu, keď sú pre jednotlivé kroky útoku potrebné rôzne typy na mieru vyrobeného vybavenia.

Tabuľka 10: *Hodnotenie zariadení*

Zariadenie	Identifikácia	Využívanie
Žiadne	0	0
Štandard	1	2
Špecializované (1)	3	4
Na mieru	5	6
Viaceré na mieru	7	8

(1) Ak sa na jednotlivé kroky útoku vyžadujú jasne odlišné skúšobné zariadenia pozostávajúce zo špecializovaného vybavenia, hodnotí sa to ako na mieru.

2.2.7 Okno pre príležitosť

Príležitosť je tiež dôležitým faktorom a súvisí s faktorom uplynulého času. Tento faktor sa uplatňuje vtedy, keď si identifikácia alebo zneužitie nejakej zraniteľnosti môže vyžadovať značný prístup k TOE, ktorý môže zvýšiť pravdepodobnosť odhalenia. Niektoré metódy útoku si môžu vyžadovať značné úsilie mimo siete a na zneužitie len krátky prístup k TOE. Prístup môže byť potrebný aj nepretržite alebo počas viacerých relácií.

Na účely tejto prílohy:

- **Neobmedzený**: prístup znamená, že útok nepotrebuje na realizáciu žiadnu príležitosť, pretože počas prístupu k TOE nehrozí žiadne riziko odhalenia.
- **Ľahký**: znamená, že prístup je potrebný na menej ako hodinu.
- **Stredne**: znamená, že prístup je potrebný na menej ako jeden deň.
- **Náročný**: znamená, že je potrebný prístup aspoň týždeň alebo dlhšie.
- **Žiadne**: znamená, že okno pre príležitosť nie je dostatočné na vykonanie útoku (dĺžka, počas ktorej je aktívum, ktoré sa má zneužiť, dostupné alebo je citlivé, je kratšia ako dĺžka príležitosti

potrebná na vykonanie útoku - napríklad ak sa kľúč k aktívu mení každý týždeň a útok potrebuje dva týždne).

Zohľadnenie tohto faktora môže viesť k stanoveniu, že nie je možné dokončiť prieskum z dôvodu požiadaviek na časovú dostupnosť, ktoré sú väčšie ako časová príležitosť.

Tabuľka 11: *Hodnotenie okien pre príležitosť*

Príležitosť	Identifikácia	Využívanie
Neobmedzene	0	0
Ľahko	1	1
Stredne	2	3
Náročne	4	5
Žiadne	-*	-*

* Označuje, že cesta útoku nie je zneužiteľná z dôvodu iných opatrení v plánovanom operačnom prostredí TOE.

2.2.8 Konečná tabuľka

Tabuľka 12: *Konečná tabuľka pre hodnotiace faktory*

Faktory	Identifikácia	Využívanie
Uplynulý čas		
< jedna hodina	0	0
≤ jeden deň	1	2
≤ jeden týždeň	2	3
≤ jeden mesiac	3	4
> jeden mesiac	5	7
Odbornosť		
Laik	0	0
Znalec	1	1
Odborník	2	3
Viacnásobný expert	5	6
Znalosti		
Verejnosť	0	0
Obmedzené	2	2
Citlivé	3	4
Prístup k TOE (vzorky)		
Mechanická vzorka*	1	1
Funkčné vzorky bez funkčných kľúčov*	2	2
Funkčné vzorky bez funkčných kľúčov*	4	4
Zariadenie		
Žiadne	0	0
Štandard	1	2
Špecializované**	3	4
Na mieru	5	6
Viaceré na mieru	7	8

Faktory	Identifikácia	Využívanie
Príležitosť		
Neobmedzene	0	0
Ľahko	1	1
Stredne	2	3
Náročne	4	5
Žiadne	-***	-***

* Tabuľka 7 obsahuje faktor na hodnotenie počtu zariadení.

** Ak sú pre jednotlivé kroky útoku potrebné jasne odlišné testovacie pracoviská pozostávajúce zo špecializovaného vybavenia, hodnotí sa to ako na mieru.

*** Označuje, že cesta útoku nie je zneužiteľná z dôvodu iných opatrení v plánovanom operačnom prostredí TOE.

2.2.9 Rozsah

Nasledujúca tabuľka nahrádza tabuľku 4 v časti B.4 CEM pre doménu "Hardvérové zariadenia s bezpečnostnými skrinkami".

Tabuľka 13: *Hodnotenie zraniteľností*

Rozsah hodnôt	TOE odolné voči útočníkom s potenciálom útoku
0 - 13.5	Žiadne hodnotenie
14- 15.5	Základné
16 - 24.5	Rozšírené - základné
25 - 34.5	Stredne
35 a viac	Vysoká

* Konečný potenciál útoku = identifikácia + využitie

3 UPLATNENIE POTENCIÁLU ÚTOKU

Hodnotenie potenciálu útoku sa vykonáva podľa stratégie uvedenej v **časti 2 Parametre podmieňujúce útoky**. Výpočet potenciálu útoku sa vykoná sčítaním hodnotení dvoch fáz: identifikácie a zneužitia.

Ku každému útoku opísanému v nasledujúcich častiach bola pridaná špeciálna anotácia s názvom **Rating hint**. Táto poznámka pozostáva z niekoľkých nápovedí, ktoré môžu hodnotiteľovi pomôcť určiť správne hodnotenie potenciálu útoku, ktoré sa má vypočítať s prihliadnutím na rôzne scenáre, ktorým bude útočník čeliť.

3.1 Invazívne útoky na fyzickú bezpečnosť

3.1.1 Útoky na externé kryty

3.1.1.1 Útoky na ručné odstraňovanie materiálu

Nasledujúce útoky obchádzajú akýkoľvek externý kryt s cieľom odhaliť kritické informácie o konštrukcii

alebo tajné údaje (údaje prechádzajúce cez akúkoľvek zbernicu):

- Odstránenie nálepiek s dôkazom o neoprávnenej manipulácii: otvorte bezpečnostnú skrinku zapečatenú nálepkami s dôkazom o neoprávnenej manipulácii, pričom nezanechajte žiadne dôkazy o neoprávnenej manipulácii, napr. priložením horúceho vzduchu na nálepku, kým sa nezlepí, a potom ju len opatrne odstráňte.
- Skrutky so špeciálnou hlavou sa dajú niekedy odstrániť mechanickými postupmi, napr. navŕtaním hlavy skrutky a následným odstránením skrutky pomocou klieští.
- Odstránenie (prilepených) krytov: teplo môže spôsobiť, že lepidlo sa stane poddajným, napr. zahriatie lepidla fénom ho urobí lepkavým a ľahko odstrániteľným.
- Chirurgia mozgu: útočník sa pokúša za veľa času a veľmi opatrne odstrániť materiál z nádoby alebo uzavretej nádoby, pričom sa zastaví pred spustením senzora, napr. pomocou noža alebo iného presného rezného nástroja.

Tip na hodnotenie: berte do úvahy, že v závislosti od typu plomb použitých na zanechanie dôkazov o neoprávnenej manipulácii môže útočník odstrániť nálepky od jednoduchého použitia iba fénu až po zložitý proces, pri ktorom sa snaží nezanechať žiadne dôkazy, ak sa používa skutočne špecializovaná nálepka na zanechanie dôkazov o neoprávnenej manipulácii. Okrem toho nemožno podceňovať útok mozgovou operáciou, ak má útočník dobrú koordináciu ruka-oko a dostatok času, možno vykonať mimoriadne jemnú prácu.

Hlavné vplyvy sú:

- Zverejnenie vnútorných častí PCB.
- Zverejnenie akýchkoľvek údajov v otvorenom texte odoslaných cez stopy PCB.

3.1.1.2 Útoky mechanickým opracovaním

Nasledujúce útoky obchádzajú akýkoľvek externý kryt s cieľom odhaliť kritické informácie o konštrukcii alebo tajné údaje (údaje prechádzajúce cez akúkoľvek zbernicu):

- Automatické odstraňovanie materiálu: automatické odstraňovanie zalievacieho materiálu, napr. vyfrézovaním epoxidovej živice, aby sa odhalilo zariadenie pod ňou.

Tip na hodnotenie: proces mechanického obrábania, od figurálnych nástrojov až po stroje s počítačovým číslicovým riadením (CNC), mimoriadne závisí od faktora mierky bezpečnostnej skrinky. Výskum môže hodnotiteľovi umožniť posúdiť požadovanú presnosť útoku, aby mohol určiť, aký druh stroja je potrebný a koľko času si vyžaduje .

Hlavné vplyvy sú:

- Zverejnenie vnútorných častí PCB.
- Zverejnenie akýchkoľvek údajov v otvorenom texte odoslaných cez stopy PCB.

3.1.1.3 Útoky na vodné opracovanie

Nasledujúce útoky obchádzajú akýkoľvek externý kryt s cieľom odhaliť kritické informácie o konštrukcii alebo tajné údaje (údaje prechádzajúce cez akúkoľvek zbernicu):

- Opracovanie vodou: Odstránenie zalievacieho materiálu pomocou frézy s vodným prúdom, napr. odstránenie epoxidového materiálu vrstvu po vrstve.

Tip na hodnotenie: proces rezania vodným lúčom mimoriadne závisí od faktora mierky bezpečnostnej skrinky. Výskum môže hodnotiteľovi umožniť posúdiť požadovanú presnosť útoku, aby mohol určiť, aký druh stroja je potrebný a koľko času si vyžaduje.

Hlavné vplyvy sú:

- Zverejnenie vnútorných častí PCB.
- Zverejnenie akýchkoľvek údajov v otvorenom texte odoslaných cez stopy PCB.

3.1.1.4 Útoky laserovým opracovaním

Nasledujúce útoky obchádzajú akýkoľvek externý kryt s cieľom odhaliť kritické informácie o konštrukcii alebo tajné údaje (údaje prechádzajúce cez akúkoľvek zbernicu):

- Laserové opracovanie: odstránenie zalievacieho materiálu pomocou laserovej frézy, napr.

odstránenie epoxidového materiálu vrstvu po vrstve.

Tip na hodnotenie: proces rezania laserom mimoriadne závisí od faktora mierky bezpečnostnej skrinky. Výskum môže hodnotiteľovi umožniť posúdiť požadovanú presnosť útoku, aby mohol určiť, aký druh stroja je potrebný a koľko času si vyžaduje.

Hlavné vplyvy sú:

- Zverejnenie vnútorných častí PCB.
- Zverejnenie akýchkoľvek údajov v otvorenom texte odoslaných cez stopy PCB.

3.1.1.5 Útoky pieskovaním

Nasledujúce útoky obchádzajú akýkoľvek externý kryt s cieľom odhaliť kritické informácie o konštrukcii alebo tajné údaje (údaje prechádzajúce cez akúkoľvek zbernicu):

- Pieskovanie: Odstránenie zalievacieho materiálu pomocou pieskovania, napr. odstránenie epoxidového materiálu vrstvu po vrstve.

Tip na hodnotenie: proces pieskovania mimoriadne závisí od faktora mierky bezpečnostnej skrinky. Výskum môže hodnotiteľovi umožniť posúdiť požadovanú presnosť útoku, aby mohol určiť, aký druh stroja je potrebný a koľko času si vyžaduje.

Hlavné vplyvy sú:

- Zverejnenie vnútorných častí PCB.
- Zverejnenie akýchkoľvek údajov v otvorenom texte odoslaných cez stopy PCB.

3.1.2 Útoky na deaktiváciu prepínačov

3.1.3 Odstránenie a deaktivácia snímačov

Nasledujúce útoky obchádzajú akýkoľvek senzor s cieľom odhaliť kritické informácie o návrhu alebo tajné údaje (údaje prechádzajúce cez akúkoľvek zbernicu):

- Obídenie snímača: Snímače založené na detekcii typu "všetko alebo nič" možno obísť v závislosti od ich konštrukčnej povahy, napr. spájkovaním podložiek medzi mikrospínačmi.
- Odstránenie snímača: Snímač možno mechanicky odstrániť z jeho polohy, napr. opatrným zatĺkaním snímača páčidlom.
- Deaktivácia snímača: snímač možno odpojiť od zdroja merania, napr. zakrytím snímača okolitého svetla čiernym epoxidom.

Tip na hodnotenie: hodnotiteľ môže zohľadniť špecifickú topológiu snímačov. Pri výpočte potenciálu útoku je potrebné zohľadniť faktor mierky ako rozhodujúci faktor. Keď útočník čelí akémukoľvek makrorozmernému senzoru, metodika útoku bude menej časovo náročná ako pri iných typoch. Keďže integrácia integrovaných obvodov sa stáva mimoriadne bežnou, útočník bude v mnohých prípadoch čeliť senzorom s veľkosťou okolo nanometrov.

Hlavné vplyvy sú:

- Zverejnenie vnútorných častí PCB.
- Zverejnenie akýchkoľvek údajov v otvorenom texte odoslaných cez stopy PCB.

3.1.4 Útok na siete senzorov reagujúce na manipuláciu

Nasledujúce útoky obchádzajú akúkoľvek sieť senzorov s cieľom odhaliť kritické informácie o návrhu alebo tajné údaje (údaje prechádzajúce cez akúkoľvek zbernicu):

- Sniffovanie siete: Sieť senzorov možno monitorovať pomocou externého zariadenia, ako sú čítačky/analyzátory zberníc, napr. ak je senzor prístupný zvonku, možno ho monitorovať pomocou ľubovoľnej čítačky zberníc.
- Modifikácia správania senzora: senzor možno modifikovať pridaním pevnej hodnoty do jeho dátového registra, napr. k dátovému registru možno pristupovať pomocou ľubovoľného JTAG, čo môže útočníkovi umožniť fixovať nameranú hodnotu.

Tip na hodnotenie: hodnotiteľ musí brať do úvahy, že niektoré implementácie môžu byť ľahšie odhaliteľné ako iné. Ak je zbernica (I2C, SPI, RS232, ...) šifrovaná, úsilie bude extrémne vyššie v porovnaní s týmito zbernicami v otvorenom texte.

Hlavné vplyvy sú:

- Zverejnenie vnútorných častí PCB.
- Zverejnenie akýchkoľvek údajov v otvorenom texte odoslaných cez stopy PCB.

3.1.5 Odstránenie a penetrácia zalievacích materiálov

Nasledujúce útoky umožňujú obísť akýkoľvek kryt založený na epoxidových materiáloch s cieľom odhaliť kritické informácie o konštrukcii alebo tajné údaje (údaje prechádzajúce cez akúkoľvek zbernicu):

- Riešenie epoxidového materiálu: epoxidovú živicu možno odstrániť pomocou chemických prípravkov, napr. vstreknutím vhodného chemického rozpúšťadla nad epoxidový materiál.
- Odstránenie epoxidovej živice mechanicky: epoxidovú živicu možno odstrániť mechanicky, pričom sa odstraňuje vrstva po vrstve, napr. opatrným zatĺkaním epoxidovej živice páčidlom.

Tip na hodnotenie: Čím viac času strávite štúdiom epoxidových vzorcov, tým účinnejšie rozpúšťadlo nájdete pre proces chemického odstraňovania. Okrem toho sa niekedy do epoxidu vloží sabotážna sieťka, zvyčajne veľmi dlhá slučka drôtu. Ak je materiál drôtu podobný chemickým receptúram epoxidu, použité rozpúšťadlo zároveň zničí drôt na detekciu sabotáže, čo spôsobí vysoké riziko odhalenia sabotáže alebo zničenia vnútorných častí.

Hlavné vplyvy sú:

- Zverejnenie vnútorných častí PCB.
- Zverejnenie akýchkoľvek údajov v otvorenom texte odoslaných cez stopy PCB.

3.1.6 Prenikanie do ôk reagujúcich na manipuláciu

Nasledujúce útoky obchádzajú akúkoľvek sieť reakcie na manipuláciu s cieľom odhaliť kritické informácie o návrhu alebo tajné údaje (údaje prechádzajúce cez akúkoľvek zbernicu):

- Otvorenie otvoru pridaním a odrezaním častí vodivých dráh: obídenie niektorých vodivých dráh sieťoviny môže umožniť vyvŕtanie otvoru priamo na sieťovine, napr. vložením ihly medzi dve dráhy.
- Skratovanie konektora sieťoviny: ak sú stopy ku konektoru medzi sieťovinou a doskou plošných spojov dosiahnuteľné, vodivé stopy možno skratovať pridaním akéhokoľvek vodivého materiálu, napr. spájkovaním konektorových plôšok medzi sebou.

Tip na hodnotenie: Čas strávený štúdiom rozloženia dráhy v sieti umožní útočníkovi zvýšiť šancu na úspech pri vkladaní ihly alebo podobného nástroja. Na druhej strane, niektoré siete reagujúce na manipuláciu môžu obsahovať vodivé stopy s veľmi podobným zložením ako izolačné vrstvy na sieti. Tento problém môže zvýšiť riziko odhalenia sabotáže v prípade mechanického odstránenia alebo prieniku do sieťky.

Hlavné vplyvy sú:

- Zverejnenie vnútorných častí PCB.
- Zverejnenie akýchkoľvek údajov v otvorenom texte odoslaných cez stopy PCB.

3.1.7 Priamy útok na procesor proti sabotáži

Nasledujúce útoky obchádzajú akýkoľvek procesor proti sabotáži s cieľom odhaliť kritické informácie o návrhu alebo tajné údaje (údaje prechádzajúce cez akúkoľvek zbernicu):

- Streľba tvarovanými nábojmi: extrémne presná streľba tvarovanými nábojmi môže preniknúť do obalu a spôsobiť vyradenie jeho obvodov skôr, ako môžu reagovať, napr. obvod na vynulovanie pamäte môže byť vyradený skôr, ako sa energia z pamäte odstráni.
- Energetické útoky: zameraním vysoko energetického lúča na procesor možno zmeniť alebo zastaviť jeho funkčnosť, napr. vystrelením elektromagnetického impulzu zameraného na procesor proti manipulácii.

Tip na hodnotenie: Pri tomto druhu útokov sa môže zvážiť iná cesta útoku. Keďže je potrebné presne určiť umiestnenie procesora vo vnútri dosky plošných spojov, môžu sa použiť tomografické alebo röntgenové technológie. Na druhej strane, niektoré prípady môžu zahŕňať metódy proti reverznému inžinierstvu, 3D mapovanie alebo ochranu pomocou röntgenového snímania. Tento problém sa dá vyriešiť sondovaním vnútorných častí krabice cez štrbinu alebo otvor, ktorý patrí ku konštrukcii alebo bol možno vytvorený ručne, čím sa obchádzajú iné druhy detekcie neoprávnenej manipulácie. Všimnite si, že útok zvýši svoje potenciálne hodnotenie, pretože môžu byť aktívne aj iné ochrany, napr. detektory svetla na hornej strane dosky plošných spojov môžu zistiť svetlo vychádzajúce z malého otvoru.

Hlavné vplyvy sú:

- Zverejnenie vnútorných častí PCB.
- Zverejnenie akýchkoľvek údajov v otvorenom texte odoslaných cez stopy PCB.

3.1.8 Priamy útok na pomocnú batériu

Nasledujúce útoky umožňujú obísť akýkoľvek procesor proti sabotáži, ktorý je závislý od externého napájania, s cieľom odhaliť kritické informácie o konštrukcii alebo tajné údaje (zbernice otvoreného textu):

- Deaktivácia pomocného zdroja napájania: prerušenie napájania, ktoré udržiava bezpečnostný procesor v chode, keď je externý zdroj napájania vypnutý, napr. prestrihnutím kábla alebo stopy pomocného externého batériového zdroja.
- Extrémne vysoká spotreba energie: zameraním vysoko energetického lúča na miesto pomocnej batérie, napr. vystrelením elektromagnetického impulzu zameraného na pomocnú batériu.

Tip na hodnotenie: Pri tomto druhu útokov sa môže zvážiť iná cesta útoku. Keďže je potrebné presne určiť umiestnenie batérie vo vnútri dosky plošných spojov, môžu sa použiť tomografické alebo röntgenové technológie. Na druhej strane, mnohé prípady môžu obsahovať externú pomocnú batériu; v takýchto prípadoch je prerušenie napájania veľmi jednoduché.

Útočník však môže vziať do úvahy, že čas, ktorý uplynie medzi prerušením drôtu a vynulovaním pamäte, môže byť veľmi krátky.

Hlavné vplyvy sú:

- Zverejnenie vnútorných častí PCB.
- Zverejnenie akýchkoľvek údajov v otvorenom texte odoslaných cez stopy PCB.

3.2 Polovičné útoky na fyzickú bezpečnosť

3.2.1 Perturbačné útoky

Nasledujúce útoky umožňujú obísť akýkoľvek procesor proti sabotáži, ktorý je závislý od externého napájania, s cieľom odhaliť kritické informácie o návrhu alebo tajné údaje (údaje prechádzajúce cez akúkoľvek zbernicu):

- Trvalé narušenie prostredia: útočník môže potrebovať meniť podmienky prostredia počas celého času vykonávania útoku, napr. zvyšovať/znižovať teplotu vykonávacieho prostredia, až kým sa nedosiahne maximálna/minimálna povolená teplota pri pokuse získať informácie z modulu RAM.
- Prechodné poruchy: zmenou hodnôt podmienok prostredia v krátkych časových úsekoch doby chodu napr. náhlym zvýšením napätia v napájacom zdroji možno zistiť anomálie v správaní systému.

Tip na hodnotenie: Pri tomto druhu útokov môže hodnotiteľ zvážiť znalosti systému potrebné na vykonanie takýchto perturbácií. Napríklad, ak má systém teplotný snímač pevne nastavený na určitú hodnotu, musí sa zvážiť úsilie na získanie tejto hodnoty z hľadiska: dostupného zdrojového kódu (open source), metód reverzného inžinierstva, ...

Hlavné vplyvy sú:

- Zverejnenie akýchkoľvek kritických bezpečnostných informácií.

3.3 Fyzická bezpečnosť neinvazívne útoky

3.3.1 Reverzné inžinierstvo

3.3.1.1 Zobrazovacie technológie

Nasledujúce útoky obchádzajú akýkoľvek systém proti spätnému inžinierstvu s cieľom odhaliť kritické informácie o návrhu alebo tajné údaje (údaje uložené v otvorenom texte):

- Vizuálne/optické rozpoznávanie: Útočník sa pokúsi rozpoznať štruktúru bezpečnostnej skrinky vizuálnym rozpoznaním, napr. pohľadom cez otvor pomocou baterky.
- Röntgenový snímok: Röntgenové rozpoznanie pomôže útočníkovi odhadnúť štruktúru vnútorných častí chránených skrinkou, napr. zhotovenie röntgenového snímku bezpečnostnej skrinky niekedy odhalí konštrukciu vnútorných častí.
- Ultrazvukové útoky: Ultrazvukové zobrazovanie sa vykonáva pomocou zvukových vĺn s frekvenciou nad 20 000 Hz. Táto technika je užitočná na zobrazenie vodičov, hardvérových komponentov, chemických ochranných prostriedkov atď. a na zistenie porušení a medzier v povrchoch.
- Tomografické útoky: Útočník môže získať veľmi dôležité informácie o rôznych úrovniach vnútornej konštrukcie systému, napr. útočník urobí tomogram viacvrstvovej dosky plošných spojov, čo mu umožní odhadnúť vnútornú štruktúru dosky plošných spojov.
- Termoelektrické útoky: Útočník urobí termovíznu snímku, ktorá môže byť použitá na odhadnutie vnútornej štruktúry, napr. útočník urobí termovíznu snímku v snahe zistiť rozmiestnenie hlavných integrovaných obvodov.

Tip na hodnotenie: Pri každej vyššie opísanej metóde musí hodnotiteľ zohľadniť opatrenia prijaté pri návrhu systému. Niektoré mechanizmy ochrany proti reverznému inžinierstvu zakryjú rozloženie komponentov, čím sa výrazne zvýši identifikácia integrovaných obvodov použitých v implementácii. Na druhej strane, ak je systém chránený proti röntgenovému, tomografickému alebo inému druhu 2D/3D skenovania, hodnotiteľ musí zohľadniť aj potrebné úsilie, ktoré treba vynaložiť v prípade obídenia alebo deaktivácie takýchto mechanizmov.

Hlavné vplyvy sú:

- Zverejnenie vnútorných častí PCB.
- Zverejnenie uložených údajov v otvorenom texte.

3.3.2 Analýza spotreby energie

Nasledujúci útok bol navrhnutý tak, aby sa pokúsil odhaliť kritické tajné údaje (zašifrované kľúčové údaje):

- Analýza spotreby energie: merania spotreby energie sa zbierajú z napájacieho vedenia počas kryptografických operácií, napr. útočník vloží do série s napájacím vstupom akýkoľvek malý odpor, potom rozdiel napätia na odpore vydelený hodnotou odporu dáva hodnotu prúdu.

Tip na hodnotenie: hodnotiteľ môže tento druh analýzy považovať za veľmi náročný. Počet vzoriek, ktoré sa majú odobrať, a štúdia, ktorá sa má realizovať po vykonaní meraní, sú založené na komplexnej diferenciálnej analýze. Hodnotiteľ by mal zvážiť odborné znalosti potrebné pre útočníka, aby získal niektoré cenné informácie, napríklad kľúč použitý pri výpočtoch.

Na druhej strane, keďže bezpečnostná skrinky riadne chráni prístup k vnútorným častiam, analýza spotreby energie sa vykonáva pomocou externého rozhrania TOE.

Hlavné vplyvy sú:

- Zverejnenie uložených zašifrovaných údajov.
- Zverejnenie tajných kľúčov.

3.3.3 Analýza vyžarovania

Nasledujúci útok bol navrhnutý tak, aby sa pokúsil odhaliť kritické tajné údaje (tajné kľúče alebo zašifrované údaje):

- Analýza vyžarovania: anténa umiestnená v blízkosti čipu bude snímať zmeny elektromagnetického poľa indukované v okolí zariadenia, napr. útočník pripevní anténu v blízkosti integrovaného obvodu a analyzuje tvar vlny zobrazený na osciloskope počas určitého času.

Tip na hodnotenie: hodnotiteľ môže tento druh analýzy považovať za veľmi náročný. Počet vzoriek, ktoré sa majú odobrať, a štúdia, ktorá sa má realizovať po vykonaní meraní, sú založené na komplexnej diferenciálnej analýze. Hodnotiteľ by mal zvážiť odborné znalosti potrebné pre útočníka, aby získal niektoré cenné informácie, napríklad kľúč použitý pri výpočtoch.

Na druhej strane, keďže bezpečnostná skrinka riadne chráni prístup k vnútorným častiam, analýza vyžarovania sa vykoná umiestnením antény mimo hranice bezpečnostnej skrinky.

Hlavné vplyvy sú:

- Zverejnenie tajných kľúčov.

3.3.4 Časová analýza

Nasledujúci útok bol navrhnutý tak, aby sa pokúsil odhaliť kritické tajné údaje (tajné kľúče alebo zašifrované údaje):

- Analýza času vykonávania: analýza zmien času vykonávania operácie v kryptografickom algoritme, ktorá môže odhaliť znalosť alebo informácie o kritickom bezpečnostnom parametri, ako je PIN alebo kryptografický kľúč, napr. útočník vykoná rôzne kryptografické funkcie, pričom meria strávený čas.

Tip na hodnotenie: tento druh analýzy možno zvyčajne vykonať pomocou externých rozhraní systému. Ak však kryptografické časovanie nie je dosiahnuteľné zvonku, je potrebné vziať do úvahy dodatočné úsilie, napríklad pokúsiť sa určiť čas, ktorý spotrebuje interná kryptografická knižnica vykonávajúca výpočty.

Hlavné vplyvy sú:

- Zverejnenie kritických bezpečnostných informácií.

DODATOK A: HARDVÉROVÝ BEZPEČNOSTNÝ MODUL (HSM)

A.1 Prehľad

V tomto dodatku sa definuje hodnotenie potenciálu útoku, ktoré sa má uplatňovať na HSM.

A.2 Elektromagnetická a zvuková analýza

Nasledujúci útok bol navrhnutý tak, aby sa pokúsil odhaliť kritické tajné údaje (tajné kľúče alebo zašifrované údaje):

- Zadávanie PIN-padu: tajné číslo PIN sa dá uhádnuť počas zadávania kódu, napr. útočník pripevní malý mikrofón v blízkosti PIN-padu, nahrá zvuk stlačených klávesov a neskôr uhádne tajné číslo.
- Analýza vyžarovania: anténa umiestnená v blízkosti čipu bude snímať zmeny elektromagnetického poľa indukované v okolí zariadenia, napr. útočník pripevní anténu v blízkosti integrovaného obvodu a analyzuje tvar vlny zobrazený na osciloskope počas určitého času.

Tip na hodnotenie: hodnotiteľ môže zvážiť námahu pri snahe skryť akékoľvek elektrické zariadenie v prípade nahrávania zvukov. Napríklad by mohlo byť jednoduché ukryť nano-mikrofón v PIN-pade. Tipy týkajúce sa analýzy vyžarovania sú uvedené v oddiele 3.3.3 tejto prílohy.

Hlavné vplyvy sú:

- Zverejnenie tajných kľúčov.

DODATOK B: TACHOGRAF

B.1 Prehľad

Tento dodatok definuje hodnotenie potenciálu útoku, ktoré sa má uplatňovať na tachografy.

B.2 Autentizácia pomocou kódu PIN (klávesnica)

B.2.1 Elektromagnetická a zvuková analýza

Nasledujúci útok bol navrhnutý tak, aby sa pokúsil odhaliť kritické tajné údaje (tajné kľúče alebo zašifrované údaje):

- Zadávanie PIN-padu: tajné číslo PIN sa dá uhádnuť počas zadávania kódu, napr. útočník pripevní malý mikrofón v blízkosti PIN-padu, nahrá zvuk stlačených klávesov a neskôr uhádne tajné číslo.
- Analýza vyžarovania: anténa umiestnená v blízkosti čipu bude snímať zmeny elektromagnetického poľa indukované v okolí zariadenia, napr. útočník pripevní anténu v blízkosti integrovaného obvodu a analyzuje tvar vlny zobrazený na osciloskope počas určitého času.

Tip na hodnotenie: hodnotiteľ môže zvážiť námahu pri snahe skryť akékoľvek elektrické zariadenie v prípade nahrávania zvukov. Je napríklad jednoduchšie ukryť nanomikrofón v PIN-pade. Tipy týkajúce sa analýzy vyžarovania sú uvedené v oddiele 3.3.3 tejto prílohy.

Hlavné vplyvy sú:

- Zverejnenie tajných kľúčov.

B.2.2 Zásuvka tlačiarne

Nasledujúci útok bol navrhnutý s cieľom pokúsiť sa odhaliť kritické údaje o konštrukcii:

- Výmena tlačového papiera: V prípade tachografov s tlačovým zariadením sa výmena papiera stáva problémom. V mnohých situáciách zostáva v zásuvke obsahujúcej vymeniteľný papier veľký otvor. Útočník môže cez tento otvor vložiť takmer akýkoľvek nástroj, čím sa dostane do vnútorných častí tlačiarne, napr. útočník preskúma vnútorné časti tachografu pomocou kamery s vláknovým sklom cez otvor v zásuvke tlačiarne.

Tip na hodnotenie: hodnotiteľ môže zvážiť, či je otvor po zásuvke tlačiarne ľahko prístupný alebo nie. Ak je otvor zásuvky vyplnený čiernym epoxidom, musia sa použiť iné metódy opracovania, preto je potrebné zvážiť ďalšie hodnotenie.

Hlavné vplyvy sú:

- Zverejnenie tajných informácií o dizajne.

36. PRÍLOHA 10: MINIMÁLNE POŽIADAVKY NA ITSEF PRE HODNOTENIA BEZPEČNOSTI HARDVÉROVÝCH ZARIADENÍ S BEZPEČNOSTNÝMI SKRINKAMI

ÚČEL

V tejto prílohe sa uvádzajú požiadavky týkajúce sa minimálnych schopností, ktoré musí mať akreditovaný ITSEF vo svojich priestoroch na vykonávanie rôznych typov útokov uvedených v prílohe 9, UPLATNENIE POTENCIÁLU ÚITOKU NA HARDWAROVÉ ZARIADENIA S BEZPEČNOSTNÝMI SKRINKAMI. Tieto kapacity zahŕňajú znalosti a zručnosti ich hodnotiteľov a potrebné vybavenie a opis metodiky hodnotenia, všetko potrebné na vykonanie uvedených útokov.

KONKRÉTNY STAV

Žiadne.

KRÍŽOVÝ ODKAZ NA KAPITOLU(-Y), V KTOREJ(-ÝCH) SÚ TIETO PRVKY VYHLÁSENÉ ZA UPLATNITEĽNÉ

Kapitola 6, ŠPECIFICKÉ POŽIADAVKY VZŤAHUJÚCE SA NA CAB Kapitola 8, ŠPECIFICKÉ KRITÉRIA A METÓDY HODNOTENIA.

1 POŽADOVANÉ SCHOPNOSTI NA FYZICKÉ HODNOTENIE HARDVÉROVÝCH ZARIADENÍ S BEZPEČNOSTNÝMI SKRINKAMI

1.1 Prehľad fyzického hodnotenia

Fyzické hodnotenie hardvérových zariadení s bezpečnostnými skrinkami (HDwSB) si vyžaduje rozvoj špecifických zručností a znalostí. Cieľom je poskytnúť technické usmernenie pre hodnotiteľov, ktorí vykonávajú hodnotenie, a odhaliť súvisiace minimálne požiadavky.

Na dosiahnutie tohto cieľa budú nasledujúce časti obsahovať:

- Poznanie bezpečnej fyzikálnej technológie, jej základných princípov a vývojových zariadení používaných výrobcami.
- Znalosti a skúsenosti s technikami fyzických útokov, ktoré by mohli ohroziť hardvér, a schopnosť používať súvisiace zariadenia na zaťaženie hardvérových vrstiev. To zahŕňa pochopenie základných fyzikálnych princípov.
- Schopnosť používať príslušné vybavenie na vykonávanie fyzických narušení a pochopenie súvisiacich fyzických účinkov na hardvér.
- Znalosti a skúsenosti v oblasti techník kryptografických útokov a schopnosť vykonávať analýzu (vrátane zachytávania údajov, postupov spracovania signálov, analýzy a hodnotenia).

Nástroje potrebné na vykonanie rôznych útočných techník možno rozdeliť na štandardné (základné), špecializované a na mieru.

1.2 Fyzikálna technológia

Hodnotitelia musia rozumieť typickému hardvéru HDwSB a základným princípom v rozsahu potrebnom na pochopenie konštrukčných rozhodnutí výrobcu.

Vyžaduje sa základná znalosť nasledujúcich informácií:

- elektrické správanie elektronických súčiastok, napr. rezistorov, kondenzátorov, tranzistorov, integrovaných obvodov, RAM, ROM, E2PROM atď.,
- princípy návrhu integrovaných obvodov,
- chemické vlastnosti typického hardvéru HDwSB. Okrem toho musia mať hodnotitelia podrobné znalosti o:
- architektúra, funkčnosť a balenie mikrokontroléra,
- architektúra a funkčnosť FPGA (Field Programmable Gate Array) a ASIC (Application Specific Integrated Circuit),
- fyzikálne správanie spínačov detekcie vybratia a otvorenia puzdra,
- fyzikálne správanie snímačov (teplota, napätie, ...),
- zásady usporiadania dosiek plošných spojov (PCB),
- fyzikálne princípy ochranných štítov (napr. mriežkové fólie, tlačené mriežky),
- realizácia štandardných obvodov používaných v mikrokontroléroch,
- dynamické správanie digitálnych a analógových obvodov,
- fyzikálne správanie mechanizmov zalievania.

Hodnotitelia musia byť schopní porozumieť schémam (blokové schémy, schémy).

Hodnotitelia musia mať znalosti o procese navrhovania a musia rozumieť procesu od schémy (logické zobrazenie hardvéru) až po skutočné rozloženie (fyzické zobrazenie). Musia rozumieť procesom technologickej kvalifikácie, funkčného testovania, charakterizácie a testovania spoľahlivosti.

Hodnotitelia musia rozumieť vývojovým zariadeniam, ktoré výrobcovia používajú pre softvér mikrokontrolérov. Patria sem simulátory, emulátory a špeciálne softvérové nástroje na vyhodnocovanie. Musia byť schopní čítať zdrojový kód mikrokontrolérov a vyvíjať softvér na penetračné testovanie a iné vyšetrovania. Preto musia hodnotitelia rozumieť inštrukčnej sade CPU, mape pamäte a používaniu ostatných periférnych jednotiek mikrokontroléra.

1.3 Fyzické špecifické útoky

Nasledujúci text poskytuje prehľad o špecifických útokoch HDwSB. Nejde o úplný zoznam, ale o niekoľko príkladov. Podrobné informácie o špecifických útokoch na HDwSB sa nachádzajú v prílohe 9, UPLATNENIE POTENCIÁLU ÚTOKU NA HARDWAROVÉ ZARIADENIA S BEZPEČNOSTNÝMI SKRINKAMI.

Hodnotitelia musia mať znalosti o štandardných scenároch útokov a v zásade musia byť schopní vyvíjať nové nápady pre takéto útoky.

Presnejšie povedané, hodnotitelia musia poznať scenáre útokov na HDwSB, ako je vniknutie do senzorov, prepínačov a filtrov, fyzická manipulácia a sondovanie, útoky na poruchy, vlastné a vynútené útoky na únik informácií, zneužitie testovacích funkcií a kryptografické útoky. Množstvo takýchto scenárov útokov - spolu s citáciami - je opísané v uvedenej prílohe.

Hodnotitelia musia byť schopní prispôsobiť a kombinovať tieto scenáre útoku pre jednotlivé HDwSB, ktoré sú predmetom hodnotenia. Počas analýzy zraniteľnosti musia byť schopní nájsť možné slabé miesta (v schémach a ich realizácii na HDwSB a ich kombinácii) a musia byť schopní použiť štandardné techniky na ich posúdenie.

Hodnotitelia musia mať znalosti a skúsenosti s inými útokmi HDwSB; s útokmi na bočné kanály (SCA), ako je analýza časovania, SCA založená na strojovom učení, jednoduchá výkonová analýza (SPA), diferenciálna výkonová analýza (DPA), diferenciálna analýza elektromagnetického vyžarovania (DEMA), útoky na šablóny (TA); útoky na zavádzanie chýb, ako je DFA a súvisiace útoky) a musia mať vybavenie (fyzické a analytické nástroje) potrebné na vykonávanie takýchto útokov. ITSEF musí vlastniť alebo mať neobmedzený prístup k zariadeniam (fyzickým a analytickým nástrojom) potrebným na vykonanie takýchto útokov podľa bodu 1.4. Musí byť schopný obsluhovať toto vybavenie (vrátane postupov zachytávania údajov) a vykonávať analýzu (matematiku). Vyžadujú sa znalosti a skúsenosti v oblasti kryptografie a štandardných techník kryptografických útokov.

Hodnotitelia musia rozumieť aspoň fyzikálnym princípom a použitiu (podľa potreby) zariadení klasifikovaných ako "štandardné", "špecializované" a "na mieru", ako sú definované v prílohe 7, UPLATNENIE POTENCIÁLU ÚTOKU NA SMART KARTY A PODOBNÉ ZARIADENIA.

1.4 Vybavenie pre fyzické hodnotenie HDwSB

Na vykonanie analýzy zraniteľnosti a zlyhania, fyzických manipulácií a scenárov útokov uvedených v oddiele 1.3 musí mať ITSEF neobmedzený prístup k väčšine nástrojov kategórie "štandard", musí ich vlastniť a musí byť schopný ich efektívne používať.

ITSEF musí mať neobmedzený prístup k nástrojom kategórie "špecializované" a musí ich vedieť efektívne používať.

Príklady týchto zariadení a ich kategorizácia sú uvedené v prílohe 9, UPLATNENIE POTENCIÁLU ÚTOKU NA HARDWAROVÉ ZARIADENIA S BEZPEČNOSTNÝMI SKRINKAMI.

ITSEF musí disponovať aspoň základným súborom nástrojov (neobmedzený prístup nestačí) na fyzickú manipuláciu, analýzu bočných kanálov, útoky rušivými vplyvmi a zásobovacie zariadenia. Zásobovacie zariadenie je potrebné na prevádzku TOE počas hodnotenia.

Základná sada pozostáva z týchto nástrojov:

- spájkovačka, spájkovacia pasta, teplovzdušné pištole, lepidlo, ihly, injekčné striekačky, nože, oceľové rezné čepele, skrutkovač, kladivo, štandardná vŕtačka, pílky, sada zubárskych nástrojov (zrkadlá), nástroje na chemické leptanie, nástroje na brúsenie,
- multimeter, digitálny osciloskop, analyzátor signálov/protokolov, PC alebo pracovná stanica, softvér na analýzu signálov, bočníky, vodiče a elektrické sondy, digitálna kamera, endoskop, mikrofóny, elektrická baterka, antény,
- zariadenia na napájanie napätím, generátory signálov a funkcií.

2 POŽADOVANÉ SCHOPNOSTI PRE LOGICKÉ HODNOTENIE HDWSB

2.1 Logický dizajn HDwSB

Hodnotitelia musia rozumieť typickým logickým architektúram HDwSB (napr. zavádzací proces, operačný systém, správa zdrojov a rozhrania) a základným princípom v rozsahu potrebnom na pochopenie rozhodnutí vývojára HDwSB. Musia poznať typické potenciálne zraniteľnosti HWSB a štandardné metódy testovania a útokov, najmä metódy útokov špecifické pre danú oblasť.

Hodnotitelia musia preukázať schopnosť vyhľadávať nové verejne známe zraniteľnosti.

2.1.1 Zdrojový kód

Typický HDwSB používa softvér na vyhradenom hardvéri. Preto je pre hodnotenie dôležitá znalosť softvéru, ako je navrhnutý, skompilovaný a spustený a ako využíva hardvér.

Na písanie softvéru v HWSB možno použiť širokú škálu programovacích jazykov. Možno ich rozdeliť do troch skupín:

- Nízka úroveň: špecifická pre procesor jazyka HWSB (ARM assembler, x86 assembler atď.),
- Stredne pokročilá úroveň: kompilovaný kód (C, C++, ADA, GO, Rust atď.),
- Vysoká úroveň: riadený kód, ktorý beží vo virtuálnom stroji alebo interpreteri (Java, Python, Shell, Perl, PHP atď.).

Zatiaľ čo assembler sa používa menej, s riadeným kódom sa naopak často stretávame, rovnako ako s kompilovaným kódom. Hodnotitelia musia dôkladne poznať používanie jazyka C/C++ alebo Java kontexte konkrétnej hardvérovej architektúry. Ak je hodnotený HDwSB alebo jeho časti naprogramované v iných jazykoch, hodnotitelia potrebujú dôkladnú znalosť aj týchto jazykov.

Okrem toho je na hĺbkovú bezpečnostnú analýzu potrebná znalosť asemblerového kódu a medzikódu (napríklad bajtového kódu karty Java). Najmä na úrovni vyšších jazykov, ako je C alebo Java, nie je možné pochopiť rôzne bezpečnostné vplyvy a chyby, pretože sa prejavia až v assemblerovom kóde alebo bajtovom kóde. Preto sa výslovne zdôrazňuje dôležitosť pochopenia asemblerového kódu vytvoreného kompilátorom a bezpečnostných vplyvov nástrojov na generovanie - v konečnom dôsledku procesor beží na asemblerovom (strojovom) kóde, nie na C, Jave alebo čomkoľvek inom.

Okrem toho musia hodnotitelia pochopiť vplyv kompilátorov, kompilátorových knižníc a interpretov na bezpečnostné správanie HDwSB pri hodnotení. Musia poznať význam rôznych nastavení kompilátora

vo vzťahu k bezpečnostným aspektom (napr. či príznak optimalizácie odstraňuje slučky potrebné na zabránenie časovým útokom).

2.1.2 Rozhrania

Hodnotitelia musia poznať rôzne druhy rozhraní, ktoré sa zvyčajne používajú v HDwSB, napr. univerzálna sériová zbernica (USB), sériový port, ethernetový port, komunikácia v blízkom poli (NFC), Wi-Fi a Bluetooth. Ak HDwSB používa iné druhy rozhraní, musia ich tiež poznať.

Musia vedieť, či rozhrania umožňujú potenciálne kritické správanie z hľadiska bezpečnosti, napr. priamy prístup do pamäte (DMA) alebo spôsoby operácií, ktoré vývojár nepredpokladá. Hodnotitelia musia vedieť, ako riešiť rozhrania HDwSB na rôznych vrstvách ISO OSI a ako testovať ich správnu funkciu.

Prostredníctvom softvéru musia byť tiež schopné využívať ladiace porty dostupné na doske plošných spojov, ako napríklad JTAG. Hodnotitelia musia mať znalosti o penetračných testoch týkajúcich sa uvedených rozhraní.

2.1.3 Protokoly transportnej vrstvy

Hodnotitelia musia poznať bezpečnostné princípy šifrovacích schém, ktoré sa majú použiť pre protokoly transportnej vrstvy, ako je bezpečný prenos správ na rozhraniach smart kariet alebo TLS alebo SSH cez rozhrania podrobne opísané vo vyššie uvedenej časti.

Tieto normy často umožňujú vysokú mieru flexibility pri konfigurácii možností zabezpečenia, čo si vyžaduje dôkladnú kontrolu pri hodnotení konkrétneho výberu na základe súboru nevyhnutných požiadaviek.

Hodnotitelia musia mať znalosti penetračných testov týkajúcich sa vyššie uvedených protokolov transportnej vrstvy.

2.1.4 Protokoly aplikačnej vrstvy

Hodnotitelia musia mať znalosti o bezpečnostnom správaní protokolov aplikačnej vrstvy, napr. v prípade POI znalosti o platobných protokoloch ako EPAS, IFSF (online) a EMV. Ďalšími príkladmi sú spracovanie údajov GNSS v prostredí digitálneho tachografu a používanie protokolu PACE v bránach smart meračov. Musia poznať stavové stroje týchto protokolov súvisiace s bezpečnosťou, ako aj základné kryptografické mechanizmy. Musia byť schopní používať testovacie súbory implementujúce takéto protokoly na testovanie bezpečnostných funkcií týchto protokolov.

Hodnotitelia musia poznať typické schémy šifrovania PIN.

Musia poznať bezpečnostné princípy správy kľúčov, protokoly správy HDwSB a mechanizmy sťahovania softvéru.

2.1.5 Operačný systém, správa obsahu a zdrojov

Určujúcou úlohou operačného systému je správa výpočtových prostriedkov (ako je trvalá a nestála pamäť, vnútorné vstupy a výstupy, komponenty vonkajšieho rozhrania, displej, klávesnica atď.) a správa prístupu (rozhrania) k týmto prostriedkom.

Zatiaľ čo predchádzajúce odseky sa zaoberali komunikáciou medzi HDwSB a vonkajším svetom, tu sa zameriame na správu zdrojov vo vnútri samotného HDwSB.

Hodnotitelia musia najprv pochopiť rôzne typy operačných systémov a ich špecifiká, napr. operačný systém reálneho času sa nebude správať rovnako ako štandardný desktopový operačný systém. Aj štruktúra súborov a správa prístupových práv k súborom v rámci týchto rôznych operačných systémov sa bude líšiť. Vyžaduje sa znalosť typov pamäte (EE, Flash, ROM, RAM), špeciálnej vyhradenej pamäte RAM (ako je Crypto-RAM, Buffer-RAM) a postupov správy pamäte (napr. obmedzenia prístupu).

Je potrebné dôkladne pochopiť koncept oddelenia domén a izolácie aplikácií. Je to dôležité najmä pre

správu aplikácií, ktorá sa týka bezpečného načítavania, správy a odstraňovania aplikácií, ako aj prístupových práv týchto aplikácií k prostriedkom HDwSB. Tejto koncepcii oddelenia zvyčajne napomáha základná hardvérová/firmvérová platforma, napríklad s dôveryhodným vykonávacím prostredím (Trusted Execution Environment - TEE). Je dôležité, aby mal hodnotiteľ znalosti v tejto špecifickej oblasti.

Je potrebné dôkladne pochopiť koncepciu procesov zavádzania vstavaných zariadení, napr. viacstupňových zavádzačov, a rôzne možnosti aktualizácie firmvéru a operačných systémov. Procesy zavádzania a aktualizácie sú potenciálnym cieľom útočníka.

Ďalšou potenciálnou cestou útoku môže byť spracovanie chýb, napr. v prípade neočakávaného alebo nesprávne zarovnaného výrazu ako vstupu. Vyhodnocovateľ musí byť schopný analyzovať spracovanie chýb a vykonať príslušné testy.

2.1.6 Generátor náhodných čísel

Hodnotiteľ musí mať znalosti a skúsenosti s metodikami hodnotenia generátorov náhodných čísel, najmä podľa normy ISO/IEC 20543[65]65.

Na vyhodnotenie fyzikálnych RNG musí mať hodnotiteľ dostatočné znalosti z teórie pravdepodobnosti a princípov návrhu fyzikálnych RNG. Hodnotiteľ musí byť schopný identifikovať a analyzovať tie vlastnosti systému alebo procesu, ktoré majú významný vplyv na rozdelenie náhodných čísel, a posúdiť náhodnosť generovania čísel.

Táto analýza sa kvantifikuje pomocou stochastického modelu. Stochastický model umožní overiť dolnú hranicu entropie na náhodný bit. Stochastický model zahŕňa najmä skupinu rozdelení, ktorá obsahuje skutočné (ale neznáme) rozdelenie(-a) nespracovaných náhodných čísel (alebo aspoň náhodných čísel v počiatočnej fáze procesu generovania) počas životnosti fyzického RNG, a to aj pre chybné stavy, napr. neprijateľné výstupy. Stochastický model sa musí odôvodniť technickými argumentmi. Okrem toho sa na základe stochastického modelu overuje aj účinnosť online testov (známych aj ako "testy stavu").

2.2 Vybavenie pre logické hodnotenie HDwSB

Na vykonanie analýzy zraniteľnosti a zlyhania a scenárov útokov uvedených v časti 1.3 musí mať ITSEF neobmedzený prístup k nasledujúcim kategóriám nástrojov potrebných na vykonanie týchto analýz
a útokov:

- Zariadenie na kontrolu prostredia (napr. na kontrolu komunikácie, napätia, hodín a teploty);
- chemické a mechanické laboratórne vybavenie (napr. na prípravu a analýzu vzoriek);
- Zobrazovacie zariadenia (napr. kamery, mikroskopy);
- Logické testovacie nástroje (napr. na testovanie rozhraní, skenovanie zraniteľností, testovanie operačných systémov, analýzu náhodnosti, analýzu zdrojového kódu, analýzu rozloženia obvodov, nástroje na fuzzing).

Hodnotitelia musia byť schopní obsluhovať zariadenie na vykonávanie nezávislých testov a útokov.

3 ORGANIZÁCIA ITSEF

3.1 Životný cyklus

Hodnotitelia musia poznať hlavné fázy životného cyklu, ktorými sú: Vývoj a výroba, prvé načítanie softvéru, dodávka, inštalácia a prevádzka (vrátane načítania aktualizácií softvéru a dodatočného softvéru) a ukončenie životnosti (napr. kontrolované vymazanie kľúčov a zničenie alebo opätovné použitie hardvéru).

[65] ISO/IEC 20543:2019: Bezpečnosť informácií - Bezpečnostné techniky - Metódy testovania a analýzy generátorov náhodných bitov v rámci noriem ISO/IEC 19790 a ISO/IEC 15408.

3.2 Subdodávky, zariadenia a vybavenie tretích strán

Všeobecné podmienky subdodávok a používania zariadení a vybavenia tretích strán sú definované kapitole 7, NOTIFIKÁCIA A AUTORIZÁCIA CAB, FUNGOVANIE CAB A SUBDODÁVATEĽOV.

Niektoré metódy útoku na HDwSB si môžu vyžadovať špecifické know-how a špeciálne čipové vybavenie. V takom prípade je možné tento druh práce zadať subdodávateľovi ITSEF, ktorý je kompetentný pre technickú doménu týkajúcu sa smart kariet a podobných zariadení.

4 AKRONYMY

EMV	Europay, MasterCard a Visa
EPAS	Aplikačný softvér pre elektronické protokoly
HDwSB	Hardvérové zariadenie s bezpečnostnou skrinkou
IFSF	Medzinárodné fórum pre štandardy pre predvýdajné miesta
OSI	Prepojenie otvorených systémov
PIN	Osobné identifikačné číslo
SSH	Zabezpečený Shell
TLS	Zabezpečenie transportnej vrstvy

37. PRÍLOHA 11: KONTINUITA ZÁRUKY

ÚČEL

Táto príloha definuje minimálne požiadavky na kontinuitu záruky súvisiacu s údržbou certifikátov.

KONKRÉTNY STAV

Žiadne.

KRÍŽOVÝ ODKAZ NA KAPITOLU(-Y), V KTOREJ(-ÝCH) SÚ TIETO PRVKY VYHLÁSENÉ ZA UPLATNITEĽNÉ

Kapitola 12, PODMIENKY VYDÁVANIA, UDRŽIAVANIA, POKRAČOVANIA A OBNOVOVANIA CERTIFIKÁTOV Kapitola 14, PRAVIDLÁ TÝKAJÚCE SA RIEŠENIA ZRANITEĽNOSTÍ

1 ÚVOD

Táto príloha definuje minimálne požiadavky na kontinuitu záruky a súvisiace činnosti údržby týkajúce sa:

- opätovné posúdenie, či nezmenený certifikovaný produkt IKT stále spĺňa bezpečnostné požiadavky;
- hodnotenie vplyvu zmien certifikovaného produktu IKT na jeho certifikát.

Táto príloha sa zaoberá týmito aspektmi kontinuity záruky:

- Opis technických koncepcií, na ktorých je založená paradigma kontinuity záruky, vrátane opisu procesov zapojených do predtým opísaných činností údržby.
- Kritériá na charakterizáciu zmien.
- Usmernenie k vykonaniu analýzy vplyvu.
- Požiadavky na obsah a prezentáciu správy o analýze vplyvu.

2 TECHNICKÉ KONCEPTY

2.1 Účel kontinuity záruky

Účelom kontinuity záruky je umožniť vývojárom podporovať činnosti údržby súvisiace s certifikovanými produktmi IKT, ako je definované v kapitole 12, PODMIENKY VYDÁVANIA, UDRŽIAVANIA, POKRAČOVANIA A OBNOVOVANIA CERTIFIKÁTOV, a prípadne s manipuláciou so zraniteľnosťami, ako je definované v kapitole 14, PRAVIDLÁ TÝKAJÚCE SA RIEŠENIA ZRANITEĽNOSTÍ.

Udelenie hodnotiaceho certifikátu Common Criteria znamená, že boli vykonané všetky potrebné hodnotiace práce, ktoré presvedčili certifikačný orgán, že TOE spĺňa všetky definované požiadavky bezpečnostných záruk ako dôvod na dôveru, že produkt alebo systém IKT spĺňa svoje bezpečnostné ciele.

Kontinuita záruky podporuje činnosti na udržanie dôvery v certifikovaný produkt, ktorého platnosť certifikátu čoskoro vyprší alebo ktorý podlieha zmenám TOE alebo jeho prostredia, a umožňuje, aby sa predtým vykonaná hodnotiaca práca nemusela za každých okolností opakovať. Kontinuita záruky preto definuje prístup k minimalizácii redundancie pri hodnotení bezpečnosti IKT, ktorý umožňuje určiť, či je potrebné opätovne vykonať nezávislé hodnotiace činnosti.

2.2 Terminológia

V tomto popise sa kvôli prehľadnosti používajú tieto pojmy.

Certifikované TOE sa vzťahuje na verziu TOE, ktorá bola hodnotená a pre ktorú bol vydaný certifikát.

Zmenené TOE sa vzťahuje na verziu, ktorá sa v určitom ohľade líši od certifikovaného TOE; môže to byť napríklad:

- novú verziu TOE alebo produktu, v ktorom TOE predstavuje podmnožinu funkcií.
- certifikovaný TOE s opravami aplikovanými na odstránenie objavených chýb.
- rovnakú základnú verziu certifikovaného TOE, ale v novom prevádzkovom prostredí (napr. na inej hardvérovej alebo softvérovej platforme), ako je uvedené v novom bezpečnostnom zámere.

Zmenené TOE sa vzťahuje na upravené TOE, ktoré prešlo procesom údržby a na ktoré sa vzťahujú aj podmienky certifikátu pre pôvodne certifikované TOE. To znamená, že bezpečnostná záruka získaná v certifikovanom TOE sa vzťahuje aj na udržiavaný TOE.

Opätovne hodnotené TOE sa vzťahuje na predtým certifikované TOE, ktoré prešlo opätovným hodnotením.

Dodatok o údržbe certifikátu sa vzťahuje na poznámku, napríklad v zozname hodnotených produktov, ktorá slúži ako dodatok pridaný k certifikátu pre certifikovaný TOE. V dodatku o údržbe sú uvedené zmenené verzie TOE, ktoré sa môžu poskytnúť v aktualizovanej verzii certifikátu.

Správa o analýze vplyvu (IAR) sa vzťahuje na správu, ktorá zaznamenáva analýzu vplyvu zmien certifikovaného TOE. IAR vytvára vývojár, ktorý žiada o údržbu certifikovaného produktu IKT.

Správa o udržiavaní sa vzťahuje na verejne dostupnú správu, ktorá opisuje zmeny vykonané v certifikovanom TOE a výsledky činností potrebných na certifikáciu zmeneného produktu.

Základná línia záruky sa vzťahuje na vyvrcholenie činností vykonaných hodnotiteľom aj vývojárom, ktorých výsledkom je certifikovaná TOE, zaznamenaná alebo predložená ako dôkaz a merateľná zmenou tohto dôkazu.

Dôkazy vývojára sa vzťahujú na všetky položky, ktoré sú hodnotiteľom k dispozícii na podporu hodnotenia TOE.

Udržiavanie certifikácie sa vzťahuje na proces uznania, že súbor jednej alebo viacerých zmien vykonaných v certifikovanom TOE (alebo v aspektoch rozvojového prostredia) nemal nepriaznivý vplyv na bezpečnostnú záruku v tomto TOE, čo zodpovedá opätovne vydanému (novému) certifikátu pre zmenené TOE.

Prehodnotenie sa vzťahuje na proces uznania, že zmeny vykonané v certifikovanom TOE (alebo v iných opatreniach bezpečnostných záruk) si vyžadujú vykonanie činností nezávislého hodnotiteľa s cieľom stanoviť novú základnú líniu záruky. Cieľom prehodnotenia je opätovné použitie výsledkov predchádzajúceho hodnotenia. Pozitívny výsledok opätovného hodnotenia by mal viesť k vydaniu nového certifikátu s prípadným predĺženým obdobím platnosti v porovnaní s pôvodným certifikátom.

Opätovné posúdenie sa vzťahuje na proces aktualizácie analýzy zraniteľnosti pôvodne certifikovaného produktu na rovnakej úrovni, aká bola pôvodne požadovaná v rámci bezpečnostného zámeru, v prípade potreby vrátane súvisiacich penetračných testov. Opätovné posúdenie sa môže vykonávať ad hoc alebo pravidelne. Možno ho považovať za osobitný prípad opätovného hodnotenia, keď sa TOE nezmenil, ale keď je potrebné posúdiť zmeny v prostredí hrozieb, aby sa potvrdilo, že TOE stále dosahuje rovnakú úroveň odolnosti ako pôvodne certifikovaný. Pozitívny výsledok opätovného hodnotenia vedie obnoveniu certifikátu s predĺženou dobou platnosti v porovnaní s pôvodným.

Rozvojové prostredie rieši všetky postupy týkajúce sa vývoja, dodania, spustenia a odstraňovania chýb TOE. Zahŕňa všetky koncepty, na ktoré sa vzťahuje trieda ALC, spolu so skupinou AGD_PRE.

Hodnotenie podskupiny sa uplatňuje v prípade, že menej významné zmeny TOE zahŕňajú zmeny rozvojového prostredia. ITSEF identifikuje tie komponenty záruk, ktoré sú ovplyvnené zmenami rozvojového prostredia, a prehodnocuje len tieto komponenty záruk vzhľadom na zmeny, čím sa vytvorí čiastočné ETR.

Čiastočný ETR je výstupom z hodnotenia podskupiny. Vytvára ho hodnotiace pracovisko, ktoré vykonalo hodnotenie podskupiny, a pre ovplyvnené komponenty záruk poskytuje úroveň podrobnosti, ktorá je porovnateľná s príslušnými časťami ETR pre pôvodný certifikovaný TOE.

2.3 Paradigma kontinuity záruky

Kontinuita záruky sa snaží využiť skutočnosť, že pri zmenách v certifikovanom TOE alebo jeho prostredí nie je potrebné za každých okolností opakovať predtým vykonanú hodnotiacu prácu.

Paradigma kontinuity záruky preto definuje procesy udržiavania certifikácie prostredníctvom opätovného hodnotenia a opätovného posudzovania tak, že každý z nich sa snaží uznať predchádzajúcu hodnotiacu prácu.

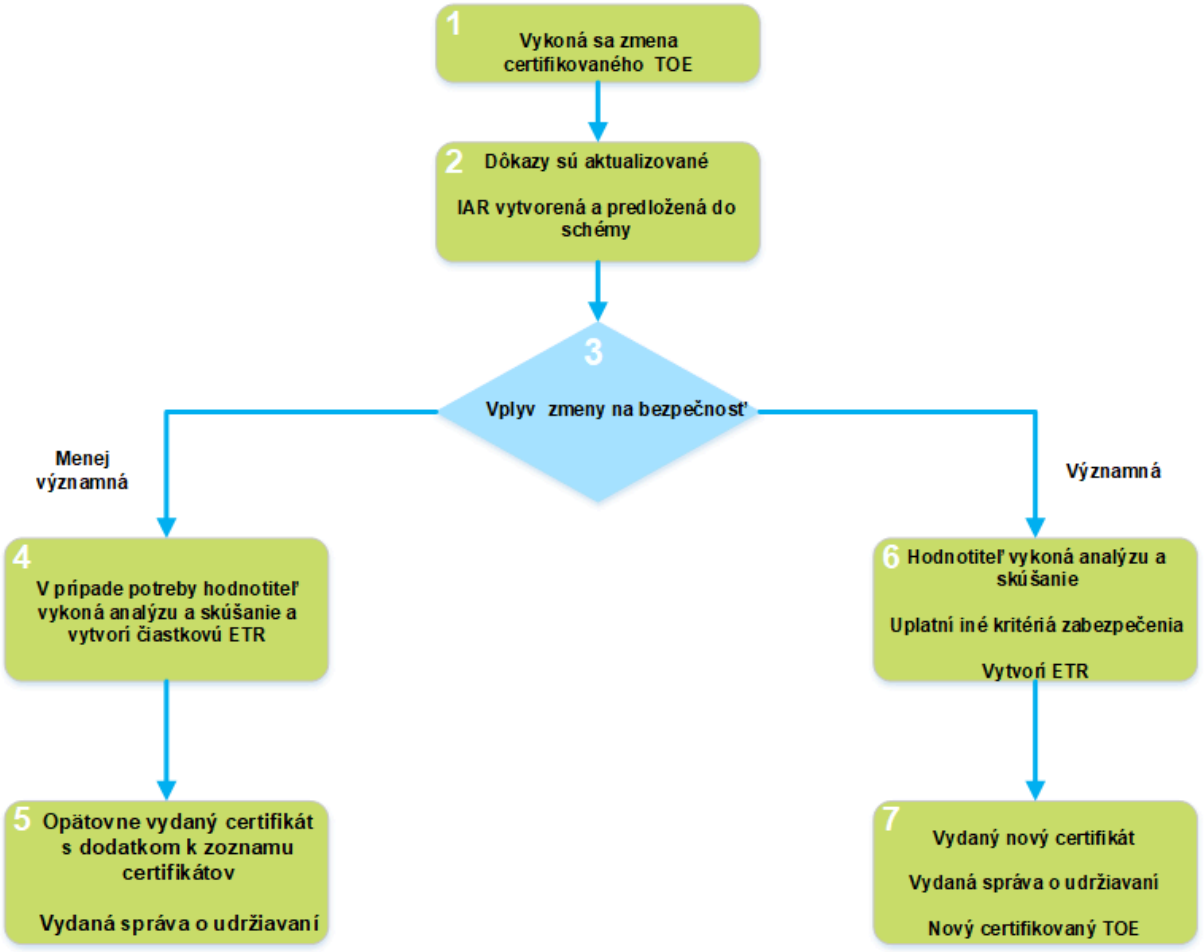
Činnosti udržiavania certifikácie sa vzťahujú na proces, ktorý vykonáva vývojár, aby mal TOE, uvedené v dodatku o údržbe pre daný TOE. Musí sa preukázať, že zmeny TOE, IT prostredia a/alebo rozvojového prostredia nemajú nepriaznivý vplyv na základnú líniu záruky.

Prehodnotenie sa vzťahuje na hodnotenie zmeneného TOE, keď vývojár nemohol (alebo sa rozhodol nepreukázať), že zmeny certifikovaného TOE nemajú nepriaznivý vplyv na základnú líniu záruky.

Opätovné posúdenie sa vzťahuje na hodnotenie predtým certifikovaného TOE na základe zmeneného prostredia hrozieb.

Na obrázkoch 2.1 a 2.2 sú znázornené primárne cesty cez kontinuitu záruky. Východiskovým bodom je vykonanie zmeny v certifikovanom TOE [rámček 1]. Touto zmenou môže byť záplata určená na opravu objavenej chyby, vylepšenie funkcie, pridanie novej funkcie, objasnenie v riadiacej dokumentácii alebo akákoľvek iná zmena certifikovaného TOE. V špecifickom prípade opätovného posúdenia sa
v certifikovanom TOE nevykonala žiadna zmena, ale berú sa do úvahy nové hrozby alebo techniky útoku.

Obrázok 1: *Všeobecný proces kontinuity záruky*



V dôsledku tejto zmeny je potrebné posúdiť jej výsledný vplyv na bezpečnostnú záruku [rámček 2]. To zahŕňa analýzu dôkazov o hodnotení, ktoré by sa museli aktualizovať, aby odrážali zmenu, a regresné testovanie kódu, aby sa zabezpečilo, že bude fungovať po začlenení do TOE. Základom pre toto posúdenie je tzv. analýza vplyvu, ktorú vykonáva vývojár TOE a zaznamenáva ju v správe o analýze vplyvu (IAR); podrobnejšie informácie o obsahu IAR sú uvedené v časti 5.

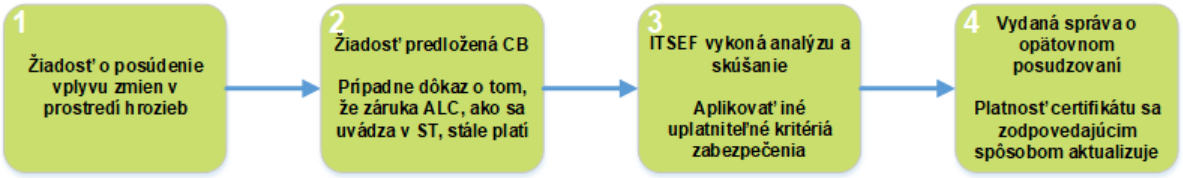
Certifikačný orgán (CB) používa IAR na určenie, či [rámček 3] má každá zo zmien menej významný alebo významný vplyv na bezpečnostnú záruku, a preto sa považuje za zmenu, ktorá si vyžaduje

alebo nevyžaduje prehodnotenie. Je potrebné poznamenať, že CB môže použiť aj iné faktory ako to, či sú zmeny významné alebo menej významné (napr. uplynulý čas od certifikácie).

Ak CB súhlasí s tým, že zmeny TOE majú menej významný vplyv, potom môže byť potrebné (ak došlo k zmenám opatrení bezpečnostných záruk v rozvojovom prostredí), aby ITSEF [rámček 4] vykonal čiastkové hodnotenie týchto opatrení bezpečnostných záruk a poskytol certifikačnému orgánu čiastkovú ETR, ktorá sa vzťahuje na tie komponenty záruk, ktoré boli ovplyvnené. Keď CB súhlasí s tým, že základná línia záruky nebola nepriaznivo ovplyvnená, potom [rámček 5] sa vytvorí dodatok k certifikačnému zoznamu a z IAR sa vypracuje správa o udržiavaní, ktorá sa zverejní a bude slúžiť ako dodatok k správe o certifikácii pôvodného certifikovaného TOE a poskytne sa v opätovne vydanom certifikáte pre zmenený produkt IKT.

Ak CB zistí, že zmena má významný vplyv na základnú líniu záruky, zmenená TOE sa musí podrobiť opätovnému hodnoteniu, aby mohla mať súvisiacu certifikáciu. Pri tomto hodnotení [rámček 6] sa v maximálnej miere využívajú predtým vytvorené dôkazy, ako aj IAR, výsledkom čoho je [rámček 7] nový ETR, a teda správa o udržiavaní skutočne novou správou o certifikácii; okrem toho certifikačný orgán vydáva nový certifikát. Tento nový certifikovaný TOE potom bude slúžiť ako základná úroveň, s ktorou sa budú porovnávať budúce zmeny [späť do rámčeka 1].

Obrázok 2: *Opätovné posúdenie*



V prípade požiadavky na posúdenie vplyvu zmien v prostredí hrozieb na certifikované TOE sa certifikačnému orgánu predloží žiadosť o opätovné posúdenie [rámček 2]. Nie je potrebný žiadny IAR, ale v tejto fáze by sa mal poskytnúť dôkaz, že záruka o rozvojovom prostredí je stále platná, ak je k dispozícii, aby sa predišlo zbytočnej hodnotiacej práci. TOE potom prechádza analýzou a testovaním hodnotiteľom [rámček 3]. Opätovne sa otvoria len činnosti bezpečnostných záruk ovplyvnené vývojom prostredia hrozieb, konkrétne skupina AVA_VAN, a ak nebolo možné poskytnúť dostatočné dôkazy, aj trieda ALC.

2.3.1 Popis procesu

Proces kontinuity záruky možno definovať z hľadiska potrebných vstupov, činností a výstupov, ktoré vedú k aktualizácii zoznamu certifikovaných produktov, aby odrážali:

1. bezpečnostnú záruku získanú pre zmenené TOE alebo,
2. vplyv na platnosť certifikátu pre pôvodne certifikovaný TOE.

Na dosiahnutie cieľa 1 poskytuje mechanizmus kontinuity záruky, ktorý umožňuje vývojárom analyzovať účinok zmien a prezentovať svoje zistenia CB. To znamená, že keď nastane zmena, vývojári musia vykonať príslušné kroky, aby zistili, či bola základná línia záruky nepriaznivo ovplyvnená. Tento proces ukladá vývojárovi povinnosť uchovávať všetky vývojárske dôkazy (zaznamenanie dostatočných informácií v IAR o zmenách dokumentárnych dôkazov by sa považovalo za uchovávanie týchto dôkazov), vykonať a zaznamenať príslušné testovanie a potvrdiť, že predchádzajúce výsledky analýzy neboli ovplyvnené zmenami TOE. V časti 4: Vykonávanie analýzy vplyvu sa tieto typy činností ďalej opisujú. Proces kontinuity záruky je opísaný ďalej.

Aby CB mohla preskúmať analýzu navrhovateľa a začať proces, navrhovateľ musí zabezpečiť, aby CB mala k dispozícii nasledujúce vstupy (niektoré z týchto vstupov už orgán pravdepodobne má):

- Certifikát pre TOE (vrátane existujúceho dodatku o údržbe)
- Správa o certifikácii
- Technická správa hodnotenia
- Bezpečnostný zámer pre certifikovaný TOE
- Správa o analýze vplyvu (IAR)

Keď sa CB uistí, že má požadované vstupy, pristúpi k preskúmaniu IAR a ďalších relevantných vstupov s cieľom určiť, aký vplyv majú zmeny opísané v IAR na základnú líniu záruky.

Proces preskúmania, ktorý vykonáva CB, bude s najväčšou pravdepodobnosťou zahŕňať konzultácie s navrhovateľom a výsledkom týchto konzultácií by mala byť úplná a konzistentná správa hodnotenia vplyvu. To znamená, že zaznamenaná analýza je úplná a IAR spĺňa všetky požiadavky na obsah a prezentáciu (pozri kapitolu 5) k spokojnosti CB.

Preskúmanie IAR sa vykonáva v súlade s touto prílohou a so všetkými relevantnými usmerneniami, ktoré môže vydať CB, a kľúčovým cieľom tohto preskúmania je určiť, či zmeny (TOE, IKT prostredia a/alebo rozvojového prostredia) možno považovať za významné alebo menej významné na základe ich zjavného vplyvu na základnú líniu záruky.

Z preskúmania IAR môžu vyplynúť dva možné výsledky:

i. CB rozhodne, že vplyv zmien na základnú líniu záruky sa považuje za zanedbateľný, a dodatok o udržiavaní certifikácie sa následne aktualizuje tak, aby bolo zrejmé, že certifikát sa vzťahuje aj na udržiavané TOE. V časti 2.3.2 sa uvádzajú ďalšie podrobnosti týkajúce sa procesu udržiavania certifikácie.

ii. CB rozhodne, že vplyv zmien na základnú líniu záruky sa považuje za závažný a dodatok o udržiavaní certifikácie sa nebude aktualizovať. Takéto zmeny by bolo potrebné zohľadniť pri opätovnom hodnotení. V časti 2.3.3 sa uvádzajú ďalšie podrobnosti týkajúce sa procesu opätovného hodnotenia.

Po prijatí tohto rozhodnutia CB informuje navrhovateľa o výsledku. V oboch prípadoch, či už ide o závažné alebo menej závažné rozhodnutie, CB zaznamená základné odôvodnenie svojho rozhodnutia v súlade s procesmi zabezpečenia kvality. Tieto záznamy môžu byť v prípade potreby sprístupnené aj pre proces vzájomného posudzovania

2.3.2 Spracovanie menej významných zmien

Účelom kontinuity záruky - zaobchádzanie s menej významnými zmenami je umožniť vykonanie menej významných zmien (tých, ktoré môžu mať malý alebo žiadny vplyv na bezpečnostnú záruku) v certifikovanom TOE, prostredí IKT a/alebo rozvojovom prostredí, pričom výsledná verzia TOE bude uznaná ako zachovávajúca rovnakú úroveň záruky ako certifikovaný TOE.

Ak sa vplyv zmien TOE považuje za menej významný, CB musí tiež určiť, že rozsah akýchkoľvek zmien vývojového prostredia nemá následný vplyv na žiadne komponenty záruk mimo rozvojového prostredia. V prípade akýchkoľvek zmien opatrení bezpečnostných záruk rozvojového prostredia je potrebné, aby ITSEF vykonal čiastočné hodnotenie (pozri časť 2.3.2.1) príslušných komponentov záruk
v bezpečnostnom zámere. Po úspešnom ukončení každého takéhoto čiastočného hodnotenia sa v zozname certifikovaných produktov hodnotiaceho orgánu uverejní aktualizovaný dodatok o údržbe (pozri oddiel 2.3.2.2) a správa o udržiavaní (pozri oddiel 2.4.2.3). Úplný IAR sa považuje za výstup, ktorý sa zdieľa len medzi vývojárom a CB.

2.3.2.1 Vyhodnotenie zmien rozvojového prostredia

ITSEF vykonáva čiastočné hodnotenie, pričom sa zameriava len na tie komponenty záruk rozvojového prostredia, pre ktoré boli opatrenia bezpečnostnej záruky upravené. ITSEF vykonáva toto hodnotenie rovnakým spôsobom, ako by bežne vykonával hodnotenie CC pre danú funkcionalitu, a vypracuje čiastočný ETR, ktorý hodnotiacemu orgánu poskytne dostatočný dôkaz o tom, že základná línia záruky bola zachovaná pre tieto zmeny rozvojového prostredia.

ITSEF sa vyberie v súlade s úrovňou záruky spojenou s hodnotením.

2.3.2.2 Dodatok k udržiavaniu certifikácie

Dodatok o udržiavanie certifikácie slúži ako dodatok k certifikátu pre certifikovaný TOE, ktorý obsahuje zoznam zmenených TOE odvodených od tohto certifikovaného TOE.

V dodatku sa vyžadujú tieto informácie:

- Jedinečný identifikátor TOE pre každý zmenený TOE súvisiacu s certifikovanou TOE.
- Odkaz na bezpečnostný zámer spojený s zmeneným TOE (upozorňujeme, že ak jedinou zmenou

bezpečnostného zámeru je verzia TOE, potom sa môže odkazovať na pôvodný bezpečnostný zámer).
- Odkaz na správu o udržiavaní, ktorá by mala byť verejne dostupná.

2.3.2.3 Správa o udržiavaní

V prípade udržiavania certifikácie sa správa o udržiavaní považuje za dodatok k správe o certifikácii pre certifikovaný TOE. Poskytuje podrobné informácie o zmenách vykonaných v certifikovanom TOE, ktoré boli akceptované.

Informácie obsiahnuté v správe o udržiavaní sú v podstate podmnožinou obsahu IAR. V správe udržiavaní by mali byť zahrnuté tieto oddiely IAR:

1) Úvod
2) Opis zmien
3) Dôkazy dotknutého vývojára

Obsah každého z týchto oddielov je opísaný v časti 5 Správa o analýze vplyvu. Tieto oddiely sa môžu pri reprodukcii v správe o udržiavaní v prípade potreby upraviť anonymizovaním alebo parafrázovaním chránených technických informácií.

Správa o udržiavaní by mala obsahovať aj odkaz na správu o certifikácii, ku ktorej je dodatkom.

CB môžu chcieť poskytnúť používateľom užitočné informácie týkajúce sa zmenenej TOE. Takéto informácie by mohli byť zahrnuté aj do správy o udržiavaní.

2.3.3 Prehodnotenie

Ak sa zistí, že zmena certifikovaného TOE má veľký vplyv, je potrebné, aby nezávislí hodnotitelia vykonali podrobnejšiu analýzu s cieľom posúdiť bezpečnostnú záruku zmenenej TOE. Opätovné hodnotenie sa vykonáva v kontexte predchádzajúceho hodnotenia, pričom sa opätovne použijú všetky výsledky predchádzajúceho hodnotenia, ktoré stále platia.

Je možné, že sa vývojár rozhodne pre opätovné hodnotenie priamo bez vypracovania IAR (napríklad ak sú zmeny také podstatné, že zmenené TOE sa len minimálne podobá na hodnotené TOE).

Prípadne aj pri podstatných zmenách mohol vývojár vykonať analýzu bezpečnostného vplyvu rozdielov medzi zmeneným TOE a hodnoteným TOE.

Ak bol predložený IAR, použije sa ako základ na identifikáciu tých častí zmeneného TOE, ktoré sa oproti predtým hodnotenému TOE nezmenili. Tak ako pri všetkých hodnoteniach, analýza, ktorá sa už vykonala na častiach TOE, ktoré zostávajú nezmenené, sa nemusí vykonať znova, čím sa maximalizuje množstvo výsledkov predchádzajúceho úsilia, ktoré sa môžu znovu použiť. Na tento účel sa nový ETR odvodí z ETR pôvodného TOE.

Po ukončení hodnotenia zmeneného TOE sa vyhotoví nový ETR spolu so správou o certifikácii, ktorá predstavuje správu o udržiavaní, a certifikát pre zmenené TOE. Táto zmenená TOE sa stáva aktualizovaným základom pre všetky prípadné budúce zmeny.

2.3.4 Opätovné posudzovanie

Ak sa prostredie hrozieb od prvej certifikácie TOE zmenilo, držiteľ certifikátu môže chcieť, aby sa odolnosť TOE prehodnotila. Opätovné posudzovanie vykonáva ten istý hodnotiteľ, ktorý vykonal pôvodné posudzovanie, pričom sa opätovne použijú všetky výsledky z predchádzajúceho posudzovania, ktoré stále platia. Opätovne sa otvoria len úlohy týkajúce sa skupiny AVA_VAN, ako aj, ak je to relevantné, úlohy triedy ALC, pre ktoré nie je možné poskytnúť dostatočné dôkazy, že sú stále splnené.

Pri aktualizácii analýzy zraniteľnosti produktu môže ITSEF zvážiť nasledujúce skutočnosti:

- zoznam potenciálnych zraniteľností vytvorený počas počiatočného hodnotenia sa opätovne použije na aktualizáciu analýzy zraniteľností. Metódy a potenciál útoku sa môžu časom vyvíjať, preto sa hodnotenie útokov môže oproti pôvodnej certifikácii zmeniť. Môže sa vykonať aj nové penetračné testovanie s cieľom posúdiť zraniteľnosti pôvodne považované za reziduálne.

- nové potenciálne zraniteľnosti, ktoré neboli riešené počas pôvodnej certifikácie, a súvisiace metódy útoku sa identifikujú prostredníctvom preskúmania verejne dostupných zdrojov informácií (pozri pracovnú jednotku CEM AVA_VAN.*-3) a akýchkoľvek iných dôkazov hodnotenia (pozri pracovnú jednotku CEM AVA_VAN.2-4 a vyššie) Tieto nové potenciálne zraniteľnosti sa použijú na aktualizáciu analýzy zraniteľností v súlade s pôvodnou úrovňou AVA_VAN.

Keďže opätovné posudzovanie vychádza z pôvodného bezpečnostného zámeru, nie je možné vykonať žiadnu zmenu bezpečnostného problému a sú zahrnuté len nové alebo vyvinuté techniky útoku.

Po ukončení opätovného posudzovania TOE sa vypracuje nový ETR spolu so správou o opätovnom posudzovaní pre opätovne posudzovanú TOE.

Platnosť pôvodného certifikátu sa potom aktualizuje podľa nasledujúcej tabuľky:

Tabuľka 1: *Vplyv výsledkov opätovného posudzovania na certifikát*

Výsledky opätovného posudzovania	Vplyv na certifikát
Pozitívne[66]66	Platnosť pôvodného certifikátu sa predlžuje do obnoveného certifikátu.
Negatívne	Nová úroveň AVA_VAN, ktorú dosiahol prehodnotený TOE, sa uvedie do opätovne vydaného certifikátu a predchádzajúci certifikát sa archivuje.

Ak sa platnosť certifikátu predĺži, nové obdobie platnosti sa stanoví s ohľadom na platné pravidlo prijaté systémom.

3 CHARAKTERISTIKA ZMIEN

CB preskúma zmeny opísané v správe o analýze vplyvu s cieľom určiť ich vplyv na bezpečnostnú záruku certifikovanej TOE.

Menej významná zmena je taká, ktorej vplyv je dostatočne minimálny, aby neovplyvnila bezpečnostnú záruku do takej miery, že je potrebné opätovne nezávisle aplikovať činnosti hodnotiteľa (hoci sa očakáva, že vývojár otestoval zmeny v rámci svojho štandardného regresného testovania), alebo zmena rozvojového prostredia, pri ktorej možno preukázať, že zmena nemá žiadny následný vplyv na ostatné opatrenia bezpečnostných záruk, ktoré boli zavedené v čase pôvodného hodnotenia.

Naopak, zmena považovaná za významnú má dostatočne podstatný vplyv na to, aby ovplyvnila bezpečnostnú záruku (s výnimkou vyššie uvedeného rozvojového prostredia) a následne by si vyžadovala nezávislé opätovné uplatnenie činností hodnotiteľa.

Preto sa menej významné zmeny riešia v rámci udržiavania certifikácie, ktorú vykonáva výlučne vývojár, zatiaľ čo významné zmeny sa riešia v rámci opätovného hodnotenia, ktoré vykonáva hodnotiteľ.

Je dôležité si uvedomiť rozdiel medzi vplyvom zmeny na certifikovaný TOE a vplyvom zmeny bezpečnostnej záruky certifikovaného TOE. Daná zmena, ktorá je rozsiahla a ovplyvňuje mnohé časti TOE, nemusí mať žiadny vplyv na bezpečnostnú záruku TOE, alebo môže mať ďalekosiahle účinky na bezpečnostnú záruku TOE. Podobne daná zmena, ktorá ovplyvňuje len veľmi malú časť TOE, nemusí mať žiadny vplyv na bezpečnostnú záruku TOE alebo môže mať ďalekosiahle účinky na bezpečnostnú záruku TOE.

Nie je možné predvídať všetky možné zmeny všetkých možných TOE, a teda ani určiť vplyv všetkých možných zmien (a či je daná možná zmena menej významná alebo významná). V dôsledku toho neexistuje pevná metóda na určenie toho, či je bezpečnostný vplyv zmeny významný alebo menej významný. Nasledujúci text ponúka všeobecné usmernenie o rozdieloch medzi významnými a menej významnými zmenami a ponúka aj príklady výnimiek.

[66] Pozitívny výsledok tu znamená, že TOE je opätovne posúdený ako zhodný s tým istým komponetom AVA_VAN, ako sa pôvodne uvádzalo v bezpečnostnom zámere.

3.1 Typické menej významné zmeny

Menej významné zmeny zvyčajne pozostávajú zo zmien TOE, ktoré nemajú vplyv na žiadne tvrdenia o TOE. Príklady menej významných zmien, ktoré je preto vhodné riešiť v rámci udržiavania certifikácie, sú:

1) Zmeny IT prostredia, ktoré nemenia certifikované TOE. Napríklad zmena základného hardvéru (ak hardvér nie je súčasťou TOE) alebo softvérových častí produktu, ktoré sú mimo hranice TOE, bude pravdepodobne malá, ak sa rozhranie nezmení. Ak sa však zmení aj rozhranie, pôjde pravdepodobne o významnú zmenu.
2) Zmeny certifikovaného TOE, ktoré nemajú vplyv na dôkaz o bezpečnostnej záruke. Napríklad, ak bol TOE certifikovaný na EAL1, zmena zdrojového kódu a/alebo hardvérových schém nebude mať vplyv na dokumentáciu o bezpečnostnej záruke. Napriek tomu by vývojár tieto zmeny otestoval v rámci štandardného regresného testovania.
3) Redakčné zmeny (gramatické, typografické, formátovanie) v ktoromkoľvek z dôkazov o bezpečnostnej záruke. Napríklad redakčné zmeny vo funkčnej špecifikácii, ktoré poskytujú dodatočné objasnenie, by pravdepodobne boli menej významné. Ak by však PP špecifikoval presnú zhodu ako stupeň zhody, potom by aj redakčná zmena vo vyhláseniach o bezpečnostných cieľoch ST alebo v opise prostredia bola významná.
4) Zmeny rozvojového prostredia. Zmena rozvojového prostredia, pri ktorej sa dá preukázať, že nemá žiadny následný vplyv na iné opatrenia bezpečnostných záruk, je zvyčajne malou zmenou. Príkladom by to bolo v prípade, že vývojár prešiel certifikáciou, ktorá tvrdila, že ALC_CMC.2 a z nejakého dôvodu zmenil Configuration Management Tool. Ak vývojár dokáže v správe o analýze vplyvu presvedčivo zdôvodniť, že tento proces nemá následné účinky na ostatné opatrenia bezpečnostných záruk, ktoré boli zavedené pôvodne, potom by sa to mohlo považovať za menej významné.
5) Zmeny na prednej strane ST. Zmena identifikácie ST alebo identifikátora TOE (napr. zmena názvu produktu) by bola menej významná. Ak sa zmení niektoré z vyhlásení o hrozbách, OSP, predpokladoch alebo bezpečnostných cieľoch bez toho, aby to vyžadovalo zmenu bezpečnostných požiadaviek, pravdepodobne by išlo o menej významné zmeny. Ak sa však zmení niektoré z vyhlásení o požiadavkách, pôjde o významné zmeny.

3.2 Typické hlavné zmeny

Významné zmeny zvyčajne spočívajú v zmenách tvrdení o TOE a môžu (ale nemusia) viesť k zmenám TOE. Príklady významných zmien, ktoré je preto vhodné riešiť v rámci prehodnotenia, sú:

1) Zmeny v súbore deklarovaných požiadaviek bezpečnostných záruk. Patrí sem pridanie nových opatrení bezpečnostných záruk a zrušenie existujúcich opatrení bezpečnostných záruk.
2) Zmeny v súbore požadovaných požiadaviek funkcionalít. Tým by sa pravdepodobne zmenila hranica TOE, ktorej správnosť a spoľahlivosť by sa musela v rámci opätovného hodnotenia opätovne posúdiť.
3) Súbor menej významných zmien, ktoré majú spolu veľký vplyv na bezpečnosť. Hoci zmeny môžu mať samostatne malý vplyv, súbor menej významných zmien môže mať veľký vplyv na bezpečnosť. Ich kombinácia by sa musela prehodnotiť.

Je potrebné poznamenať, že oprava chyby nemá predvídateľný rozsah zmeny certifikovaného TOE ani predvídateľný vplyv na bezpečnostnú záruku certifikovaného TOE. Preto "oprava chyby" môže predstavovať buď významnú, alebo menej významnú zmenu.

4 VYKONANIE ANALÝZY VPLYVU

4.1 Vstup

Vstupy do procesu analýzy vplyvu sú tieto:

a) vývojárske dôkazy spojené s certifikovaným TOE;

b) popis zmeny (pravdepodobne vytvorený na základe procesov a postupov kvality životného cyklu).

4.2 Predbežná práca

Bezpečnostná kategorizácia TOE sa môže použiť ako nástroj, ktorý pomôže posúdiť, či zmena patrí do rozsahu údržby. Napríklad, keď je zmena opísaná v analýze vplyvu, je možné konzultovať bezpečnostnú kategorizáciu s cieľom identifikovať vplyv zmeny na dôkazy vývojára uvedené v základnej línii záruky.

Bezpečnostná kategorizácia môže zahŕňať všetky bezpečnostné vývojové nástroje, bezpečné postupy dodávania, bezpečnostné postupy vývojárov, činnosti životného cyklu vývoja alebo bezpečnostné postupy ovplyvňujúce používanie alebo správu systému riadenia konfigurácie.

Je potrebné poznamenať, že všetky dodatky k TOE budú musieť byť zaradené do bezpečnostnej kategórie podľa zvoleného prístupu a všetky modifikované časti môžu vyžadovať preskúmanie ich zaradenia do bezpečnostnej kategórie.

4.3 Kroky pri vykonávaní analýzy vplyvu

Počas údržby je zodpovednosťou vývojára potvrdiť, že obsah a verdikty prezentácie pre upravené dôkazy vývojára je možné stále splniť. Po identifikácii vplyvu zmeny na dôkaz vývojára je potom vývojár schopný vyvodiť bezpečnostný vplyv zmeny.

Krok 1 - Identifikácia certifikovaného TOE

Určite dôkazy vývojára poskytnuté pre základnú líniu záruky certifikovaného TOE vrátane certifikovaného TOE. Všetky zmeny sa uplatňujú na základe tejto základnej línie.

Krok 2 - Identifikujte a opíšte zmenu(-y)

Opíšte zmenu(-y) produktu vzhľadom na produkt spojený s certifikovaným TOE.

Identifikujte a opíšte zmenu(-y) rozvojového prostredia vzhľadom na rozvojové prostredie certifikovaného TOE.

Tieto zmeny sú uvedené na takej úrovni podrobnosti, ktorá je potrebná na pochopenie toho, čo bolo vykonané, ale nie nevyhnutne ako to bolo vykonané.

Krok 3 - Určenie dôkazov ovplyvnených vývojárov

Cieľom tohto kroku je vzhľadom na každú zmenu z predchádzajúceho kroku určiť, ktoré položky dôkazov vývojára je potrebné aktualizovať. Tento krok by sa mal vykonať systematickým spôsobom, pričom sa postupne zváži každý komponent záruk zahrnutá v balíku záruky pre certifikovaný TOE, vplyv zmeny na komponent záruk a dôkazy poskytnuté pre tento komponent. Na uľahčenie takéhoto prístupu možno použiť nasledujúci zoznam.

Pri zmene produktu by sa mali zohľadniť tieto aspekty:

a) Ovplyvnilo to bezpečnostný zámer?
b) Ovplyvnilo to referenciu na TOE?
c) Ovplyvnilo to zoznam konfiguračných položiek pre TOE?
d) Ovplyvnilo to niektorú z úrovní abstrakcie TSF, t. j. funkčnú špecifikáciu, návrh TOE alebo zobrazenie implementácie?
e) Ovplyvnilo to opis architektúry (ak základná línia bezpečnostnej záruky obsahuje komponent zo skupiny ADV_ARC)?
f) Ovplyvnilo to mapovanie z TSFI funkčnej špecifikácie na najnižšiu úroveň dekompozície dostupnú v návrhu TOE (ak základná línia bezpečnostnej záruky obsahuje komponent zo skupiny ADV_TDS) a na zobrazenie implementácie (ak základná línia bezpečnostnej záruky obsahuje komponent zo skupiny ADV_IMP)?
g) Ovplyvnilo to sprievodnú dokumentáciu (ak základná línia záruky obsahuje komponent

z triedy AGD)?
h) Ovplyvnilo to testovaciu dokumentáciu, t. j. analýzu pokrytia testov, analýzu hĺbky testovania alebo testovaciu dokumentáciu (ak základná línia záruky zahŕňa komponent z triedy ATE)?
i) Ovplyvnilo to analýzu zraniteľnosti?

Pri zmene rozvojového prostredia by sa mali zohľadniť tieto aspekty:

a) Ovplyvnilo to bezpečnostný zámer?
b) Ovplyvnilo to dokumentáciu CM?
c) Ovplyvnilo to postupy doručovania (ak základná línia záruky obsahuje komponent zo skupiny ALC_DEL)?
d) Ovplyvnila postupy potrebné na bezpečné prijatie dodaného TOE, bezpečnú inštaláciu TOE a bezpečnú prípravu prevádzkového prostredia?
e) Ovplyvnilo to bezpečnostné postupy vývojára (ak základná línia záruky obsahuje komponent zo skupiny ALC_DVS)?
f) Ovplyvnilo to postupy odstraňovania chýb (ak základná línia záruky obsahuje komponent zo skupiny ALC_FLR)?
g) Ovplyvnilo to model životného cyklu (ak základná línia záruky zahŕňa komponent zo skupiny ALC_LCD)?
h) Ovplyvnilo to vývojové nástroje (ak základná línia záruky obsahuje komponent zo skupiny ALC_TAT)?
i) Došlo k zmenám vo výrobnom procese (najmä v prípade hardvérových komponentov)?

Na základe opisu zmeny by sa mali zvážiť vplyvy na všetky dôkazy navrhovateľa, aby sa skontrolovalo, či boli identifikované všetky potenciálne vplyvy.

Upozorňujeme, že ST bude pravdepodobne ovplyvnený, aj keď je v podstate podobný pôvodnému ST. Ak sa TOE zmenil, bude to zahŕňať aspoň zmenu čísla verzie TOE.

Ako vstupné údaje pre túto analýzu možno použiť predchádzajúce verzie IAR.

V prípade niektorých prvkov činnosti vývojára môže byť toto určenie jednoduché (napr. nové grafické používateľské rozhranie pre zmenené TOE, ktoré sa má dodať rovnakým spôsobom, aký sa používa pre TOE, nebude mať nepriaznivý vplyv na ALC_DEL), zatiaľ čo v prípade iných požiadaviek to môže byť zložitejšie (napr. zmenil sa návrh TOE pre subsystém používateľského rozhrania zavedením nového grafického používateľského rozhrania a vplyv na materiál poskytovaný pre ADV_TDS?

Výstupom tohto kroku je zoznam dotknutých prvkov akcie vývojára.

Krok 4 - Vykonajte požadované úpravy dôkazov vývojára.

Cieľom tohto kroku je určiť, ako by sa mal upraviť každý z dotknutých dôkazov vývojára (identifikovaných počas predchádzajúceho kroku), aby sa riešil príslušný obsah a prezentácia prvkov dôkazov. Stačí spoločne zhromaždiť zmeny požadované v dôkazoch vývojára pred skutočným vykonaním týchto zmien.

Na aktualizáciu dôkazov by mohlo byť potrebné testovanie (regresné testovanie). Vývojár môže napríklad zopakovať vzorku testov vývojára dodaných na hodnotenie.

Pokiaľ ide o IAR, vyžadovali by sa dostatočné informácie o tom, ako bolo aktualizované testovanie vývojárov, úmerné testovacím komponentom v základnej línii záruky. Ak boli na riešenie zmeny napísané nové testy, tieto sú spolu s účelom testovania uvedené v správe o analýze vplyvu. Podrobnosti o teste v zmysle poskytnutia testovacích skriptov vrátane jednotlivých krokov testu sa však nevyžadujú.

Ak je zmena TSF "neviditeľná" na najnižšej dostupnej abstrakcii TSF (napr. najnižšiu úroveň dekompozície TSF predstavuje komponent ADV_TDS.2 a počas údržby sa zmení časť zdrojového kódu, ale zmeny si nevyžadujú úpravu subsystémov v návrhu TOE), potom stačí, ak vývojár uvedie, ako bola zmena testovaná, a poskytne súvisiace odôvodnenie v IAR.

Výstupom tohto kroku je zoznam aktualizovaných dôkazov (môže mať podobu zoznamu zmien dôkazoch - kde, prečo, čo).

Krok 5 - Záver

Určiť celkový vplyv identifikovaných zmien bezpečnostnej záruky certifikovaného TOE. Záver: malý

alebo veľký vplyv.

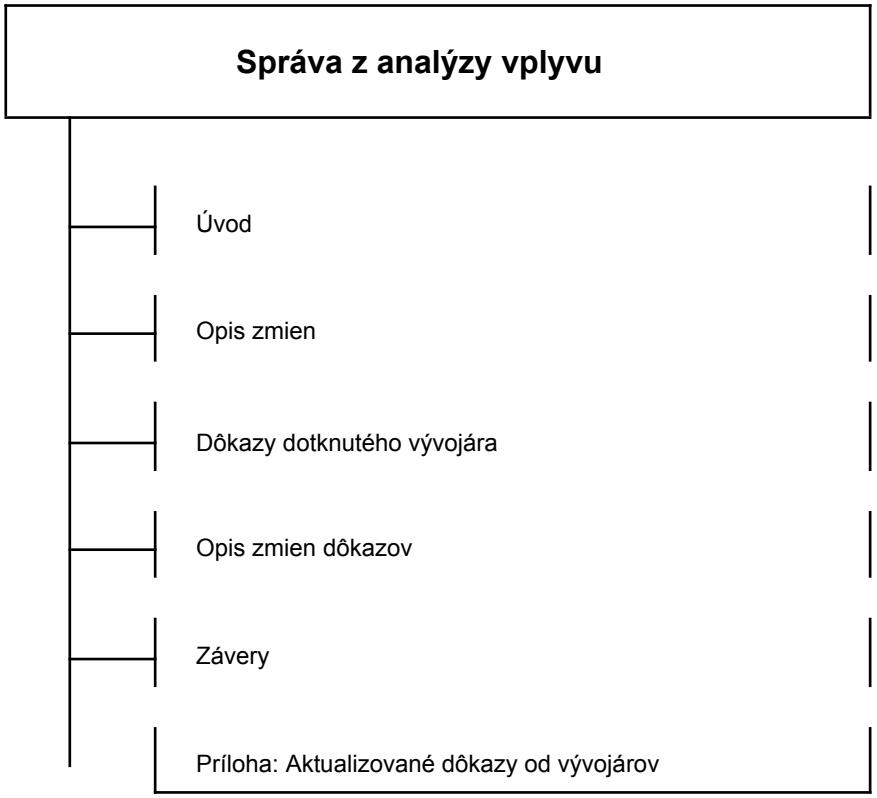
4.4 Výstupy

a) Správa z analýzy vplyvu (IAR);
b) Aktualizované dôkazy vývojárov.

5 SPRÁVA Z ANALÝZY VPLYVU (IAR)

V tejto časti sa opisuje minimálny obsah IAR. Obsah IAR je znázornený na obrázku 37-1; tento obrázok sa môže použiť ako pomôcka pri zostavovaní štrukturálneho náčrtu dokumentu IAR. IAR je požadovaným vstupom pre proces údržby.

Obrázok 2: *Správa z analýzy vplyvu*



5.1 Úvod

Vývojár nahlási identifikátory kontroly konfigurácie IAR. Identifikátory kontroly konfigurácie IAR obsahujú informácie, ktoré identifikujú IAR (napr. názov, dátum a číslo verzie).

Vývojár oznámi aktuálne identifikátory kontroly konfigurácie TOE.

Identifikátory kontroly konfigurácie TOE identifikujú aktuálnu verziu TOE, ktorá odráža zmeny certifikovaného TOE.

Vývojár nahlási identifikátory kontroly konfigurácie pre ETR, správu o certifikácii a certifikovaný TOE. Tieto identifikátory kontroly konfigurácie sú potrebné na identifikáciu základnej línie záruky a s ňou súvisiacej dokumentácie, ako aj všetkých ďalších zmien, ktoré mohli byť vykonané v tejto základnej línii.

Vývojár oznámi identifikátory kontroly konfigurácie pre verziu ST týkajúcu sa certifikovaného TOE.

Vývojár oznámi totožnosť vývojára. Totožnosť vývojára TOE sa vyžaduje na identifikáciu strany zodpovednej za výrobu TOE, vykonanie analýzy vplyvu a aktualizáciu dôkazov.

Vývojár môže zahrnúť informácie týkajúce sa právnych alebo zákonných aspektov, napríklad

v súvislosti s dôvernosťou dokumentu.

5.2 Opis zmeny (zmien)

Vývojár nahlási zmeny produktu. Identifikované zmeny sa týkajú produktu spojeného s certifikovaným TOE.

Vývojár nahlási zmeny do rozvojového prostredia. Identifikované zmeny sa týkajú rozvojového prostredia certifikovaného TOE.

5.3 Dôkazy dotknutého vývojára

Pri každej zmene vývojár nahlási zoznam dotknutých položiek vývojárskej evidencie. Pri každej zmene produktu spojeného s certifikovaným TOE alebo rozvojového prostredia certifikovaného TOE sa uvedú všetky položky vývojárskych dôkazov, ktoré je potrebné upraviť, aby sa riešili prvky činnosti vývojára.

5.4 Opis úprav dôkazov vývojára

Vývojár stručne opíše požadované úpravy dotknutých položiek vývojárskej evidencie. Pre každú dotknutú položku vývojového dôkazu sa stručne opíšu úpravy potrebné na riešenie príslušného obsahu a prezentácie prvkov dôkazu.

5.5 Závery

Pri každej zmene vývojár oznámi, či sa vplyv na bezpečnostnú záruku považuje za menej významný alebo významný. Pre každú zmenu by mal vývojár poskytnúť podporné zdôvodnenie uvádzaného vplyvu. V prípade, že sa zmena týka rozvojového prostredia, zdôvodnenie preukáže, že nemá následný vplyv na iné opatrenia bezpečnostných záruk.

Investor oznámi, či sa celkový vplyv považuje za malý alebo veľký.

Vývojár by mal uviesť podporné odôvodnenie, pričom by mal zohľadniť kulmináciu zmien.

5.6 Príloha: Aktualizované dôkazy od vývojárov

Vývojár nahlási pre každú aktualizovanú položku vývojárskeho dôkazu tieto informácie:

- názov;
- jedinečný odkaz (napr. dátum vydania a číslo verzie).

Je potrebné uviesť len tie položky dôkazov, ktoré sa výrazne zmenili; ak jedinou aktualizáciou položky dôkazu je zohľadnenie novej identifikácie TOE, potom ju nie je potrebné zahrnúť.

38. PRÍLOHA 12: POSTUP PRI VYKONÁVANÍ VZÁJOMNÉHO POSUDZOVANIA

ÚČEL

V tejto prílohe je opísaný platný postup vzájomného posudzovania.

KONKRÉTNY STAV

Žiadne.

KRÍŽOVÝ ODKAZ NA KAPITOLU(-Y), V KTOREJ(-ÝCH) SÚ PRVKY VYHLÁSENÉ ZA UPLATNITEĽNÉ

Kapitola 22, VZÁJOMNÉ POSUDZOVANIE.

1 OBSAH

V tejto prílohe je opísaný platný postup vzájomného posudzovania. Postup pozostáva zo štyroch fáz: príprava, návšteva na mieste, podávanie správ a prijatie správy.

Postup definuje len postup, ktorý sa má dodržať. Aby bol postup čo najkomplexnejší a najobjektívnejší, v spolupráci s ECCG sa ďalej vypracujú kontrolné zoznamy, ktoré budú pomáhať tímu vzájomného posudzovania. Tieto kontrolné zoznamy budú obsahovať spoločné chápanie „state of the art“[67]
a prevádzkových postupov.

Tento postup sa vzťahuje na tri typy vzájomného posudzovania:

1. Typ 1: Ak certifikačný orgán (CB) vykonáva certifikačné činnosti na úrovni AVA_VAN.3;
2. Typ 2: Keď CB vykonáva certifikačné činnosti týkajúce sa technickej domény;
3. Typ 3: Ak CB vykonáva certifikačné činnosti nad úrovňou AVA_VAN.3 podľa ochranného profilu definovaného osobitne pre toto použitie a pripojeného k schéme EUCC.

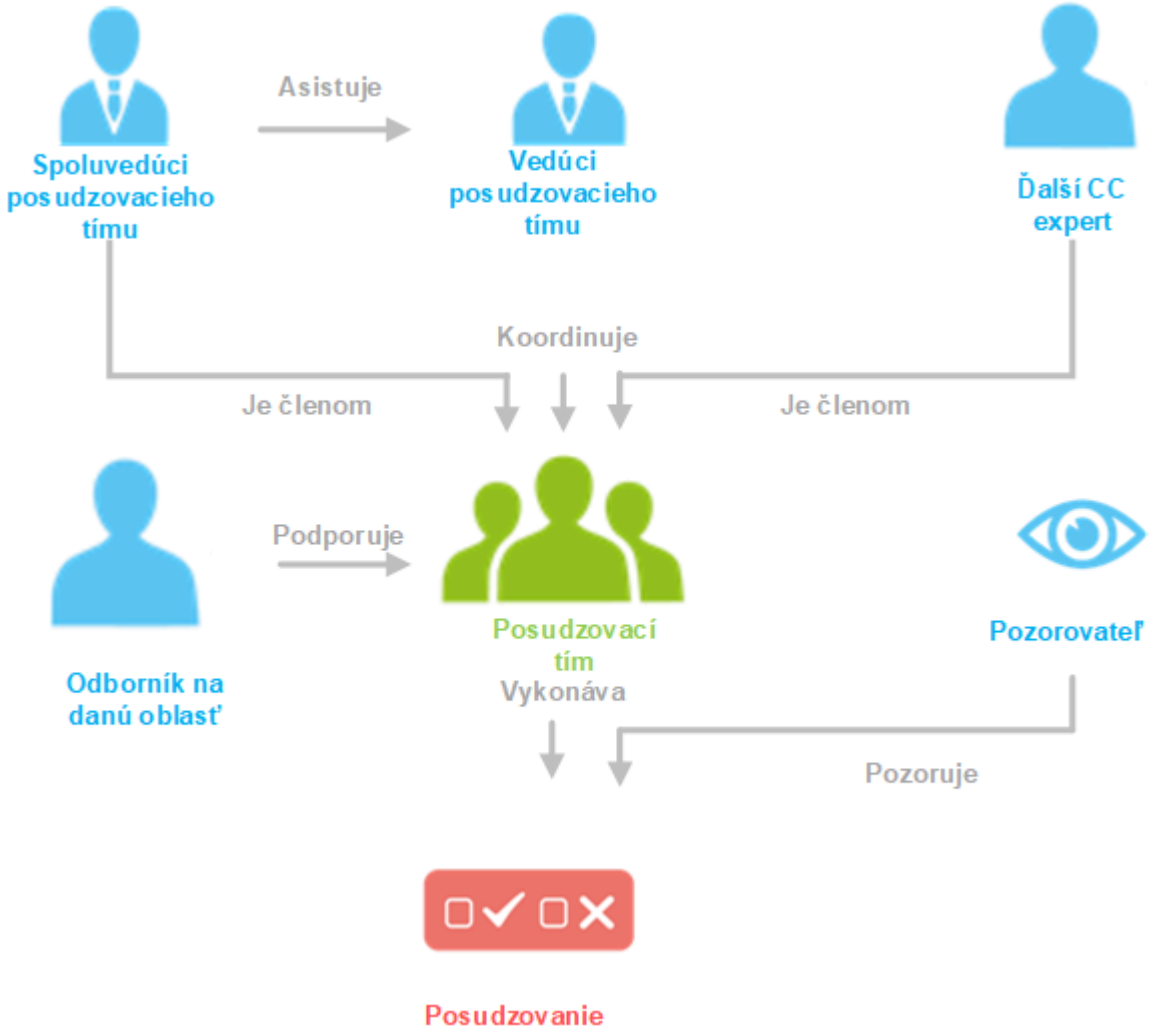
Všetky rozdiely medzi typmi 1 a 2 sú uvedené v tomto postupe. Typ 3 si bude vyžadovať ďalší vývoj, keď budú vypracované takéto ochranné profily.

2 PREHĽAD

Primárny posudzovací tím pozostáva z dvoch odborníkov na spoločné kritériá (CC) (vedúci a spoluvedúci) vybraných z dvoch certifikačných orgánov (CB), ktoré vydávajú certifikáty na úrovni záruky „vysoká“ CSA.

Tento primárny posudzovací tím môže byť rozšírený o ďalších expertov z iných alebo tých istých CB a v prípade delegovania vydávania certifikátov alebo predchádzajúceho schvaľovania certifikátov môže byť k vybranému expertovi z CB do tímu pridaný expert z príslušného NCCA.

[67] Ako bolo prerokované v spolupráci s ECCG a/alebo príslušnými podskupinami.



Obrázok 1: *Organizácia hodnotiaceho tímu*

Pri vzájomnom posudzovaní typu 2 sa primárny posudzovací tím vyberie z CB pôsobiacich v príslušnej technickej doméne.

Každý expert na CC v posudzovacom tíme musí mať minimálne tieto zručnosti/skúsenosti:

1. dva roky ako certifikátor v CB, prípadne pôsobiaci v príslušnej technickej doméne (doménach);
2. účasť na hodnotení spôsobilostí ITSEF, ktorý vykonáva hodnotenie pre CB na podporu autorizácie CB, ako je definované v kapitole 7, NOTIFIKÁCIA A AUTORIZÁCIA CAB, FUNGOVANIE CAB A SUBDODÁVATEĽOV.

Pri vzájomnom posudzovaní typu 2 môžu tímu pre vzájomného posudzovanie pomáhať odborníci na danú technickú doménu (domény). Títo odborníci môžu byť sami certifikátormi, ale nie je to nevyhnutné.

Dôrazne sa tiež odporúča, aby sa členovia tímu vzájomného posudzovania zúčastnili na predchádzajúcich vzájomných posudzovaniach buď ako pozorovatelia, alebo ako členovia tímu.
V ideálnom prípade by malo ísť o vzájomné posudzovania vykonané v rámci schémy EUCC, ale prínosom sú aj skúsenosti s vzájomným posudzovaním v rámci iných dohôd o vzájomnom uznávaní, ako je SOG-IS MRA alebo CCRA.

Vzájomné posudzovanie môžu pozorovať pozorovatelia navrhnutí inými NCCA.

Vzájomne posudzovaná CB môže ECCG predložiť akékoľvek obavy týkajúce sa výberu členov tímu vzájomného posudzovania a pozorovateľov, napríklad v prípade konfliktu záujmov.

Vzájomné posudzovanie sa uskutoční v štyroch fázach.

Prípravná fáza zahŕňa preskúmanie dokumentácie CB členmi tímu vzájomného posudzovania s cieľom oboznámiť sa s politikami a postupmi CB.

Fáza návštevy na mieste bude pozostávať z dvojtýždňovej návštevy tímu vzájomného posudzovania v CB s cieľom posúdiť odbornú kompetentnosť CB a prípadne ITSEF vykonávajúcich hodnotenia. Presné trvanie návštevy na mieste bude závisieť od možného opätovného použitia existujúcich dôkazov
a výsledkov vzájomného posudzovania a v prípade posudzovania typu 2 od počtu ITSEF a od počtu technických domén, pre ktoré CB vydáva certifikáty.

Vzájomné posudzovanie bude zahŕňať fázu podávania správ: posudzovací tím zdokumentuje svoje zistenia v správe o vzájomnom posudzovaní, ktorú doručí ECCG.

Vzájomné posudzovanie sa ukončí prijatím stanoviska ECCG k výsledku vzájomného posudzovania.

3 PLÁNOVANIE ČINNOSTÍ VZÁJOMNÉHO POSUDZOVANIA

V súlade s plánovaním stanoveným ECCG a s prihliadnutím na možné priority uvedené v kapitole 22, VZÁJOMNÉ POSUDZOVANIE, ECCG oznámi CB vzájomné posudzovanie a poverí tím pre vzájomné posudzovanie, aby vykonal vzájomné posudzovanie.

Vzájomne posudzovaná CB predloží požadovaný počet kandidátskych produktov, pri ktorých CB postupovala podľa projektov hodnotenia, na preskúmanie tímu vzájomného posudzovania. Kandidátske produkty vo všeobecnosti pokrývajú všetky technické aspekty auditu.

Ak bola certifikácia nad úrovňou AVA_VAN.3 pre produkty IKT, na ktoré sa nevzťahuje technická doména, zavedená podľa osobitných ochranných profilov certifikovaných v rámci tejto schémy na tento účel, do zoznamu kandidátskych produktov sa zahrnie aspoň jeden produkt IKT certifikovaný podľa týchto ochranných profilov.

Pri vzájomnom posudzovaní typu 2 CB predloží posudzovaciemu tímu na posúdenie aspoň jeden produkt za technickú doménu na každý posudzovaný ITSEF, pre ktorý CB sledovala projekt hodnotenia, a poskytne podrobnosti o každom ITSEF, ktorý považuje za spôsobilý na hodnotenie na vyššej úrovni v danej technickej doméne.

Požiadavky na minimálny počet produktov sú zhrnuté v nasledujúcej tabuľke.

***Tabuľka 1:** Minimálny počet produktov*

Hodnotené produkty	Typ 1	Typ 2
Minimálny počet produktov	2	Min. 1 za technickú doménu a za každý ITSEF*

* PRÍKLAD:

1. počet požadovaných technických domén: 2
2. počet ITSEF žiadajúcich o vyššiu úroveň hodnotenia v 2 technických doménach: 2
3. minimálny počet produktov hodnotených v rámci tieňovej certifikácie: 2 x 2 = 4

Požadované informácie a zoznam kandidátskych produktov (a ITSEF) poskytne vzájomne posudzovaná CB tímu pre vzájomné posudzovanie jedného mesiaca od oznámenia zo strany ECCG.

Posudzovací tím dohodne termíny vzájomného posudzovania CB a prípadne návštevy ITSEF na mieste.

4 POVINNOSTI VZÁJOMNE POSUDZOVANÉHO CB

Vzájomne posudzovaná CB poskytne túto dokumentáciu:

- úplný opis jej rozsahu, organizácie a fungovania vrátane:
  - názov, adresu a hlavné kontaktný bod;
  - svoju úlohu podľa článku 56;
  - rozhodnutie o akreditácii CB;

- postupy certifikácie;
- prípadne postupy predchádzajúceho schválenia pre každé jednotlivý certifikát alebo požiadavky vyplývajúce zo všeobecného poverenia;
- pravidlá, ktoré sa uplatňujú v rámci vzájomne posudzovanej CB a jej interných alebo externých testovacích zariadení (ITSEF) na ochranu chránených iných citlivých informácií;
- názvy a adresy ITSEF, ktoré sa zúčastňujú na činnostiach, a ich štatút (komerčné alebo vládne);
- postupy, ktorými vzájomné posudzovanie CB zabezpečuje, aby ITSEF správne a dôsledne uplatňovali kritériá a metódy hodnotenia a chránili dôvernosť príslušných citlivých informácií;

- najnovší zoznam certifikátov vydaných vzájomne posudzovanou CB za posledných päť rokov;
- dva alebo viac vydaných certifikátov a správ o certifikácii, ktoré vyberie tím vzájomného posudzovania;
- ak sa navrhuje opätovné použitie výsledkov predchádzajúceho vzájomného posudzovania, súvisiace výsledky za podmienok uvedených v kapitole 22, VZÁJOMNÉ POSUDZOVANIE.

Okrem toho sa poskytnú všetky relevantné informácie o systéme riadenia kvality, ktorý CB zaviedla s cieľom získať akreditáciu od svojho NAB. Je potrebné poznamenať, že tieto informácie sa poskytujú pre informatívne účely a že obsah týchto informácií nie je predmetom vzájomného posudzovania. Všetky zistené odchýlky od postupov opísaných v týchto dokumentoch sa však musia nahlásiť.

Všetka písomná dokumentácia a komunikácia pre činnosti vzájomného posudzovania musí byť poskytnutá v angličtine najmenej 4 týždne pred dátumom auditu.

V prípade vzájomného posudzovania typu 2 CB poskytne zoznam všetkých ITSEF, ktoré vykonávajú hodnotenia pre danú doménu, a opis dôkazov použitých pri posudzovaní kompetencií týchto ITSEF.

Počas návštevy na mieste sa bude hovoriť anglicky, pokiaľ sa CB a tím pre vzájomné posudzovanie jednomyseľne nedohodnú na inom jazyku.

Súčasťou činností vzájomného posudzovania počas návštevy na mieste bude preskúmanie aspoň jedného hodnotenia, ktoré bolo v rámci CB ukončené alebo sa blíži k ukončeniu. (V prípade žiadosti o vyššiu úroveň v technickej doméne (typ 2 definovaný vyššie) sa hodnotenie musí týkať produktu v rámci tejto domény a zahŕňať príslušné metódy útoku/vyhľadávania zraniteľností na príslušnej úrovni).

Hoci hodnotenia vybraných produktov predložených na posúdenie nemusia byť úplne úplné, musia existovať záznamy preukazujúce, že sa vykonali významné hodnotiace analýzy a certifikačné činnosti a že väčšina správy z hodnotenia (vrátane aspoň jedného kola analýzy zraniteľnosti) bola doručená certifikačnému tímu a analyzovaná ním.

Okrem vybraných produktov môže CB poskytnúť tímu pre vzájomné posudzovanie aj informácie o (najviac) dvoch ďalších hodnoteniach, ktoré boli ukončené v priebehu 12 mesiacov pred začatím činností vzájomného posudzovania. Ak má tím vzájomného posudzovania dostatok času a zdrojov, preskúma tieto hodnotenia počas svojej návštevy na mieste a v prípade, že sa zistí, že sú v súlade s požiadavkami schémy EUCC, zohľadní ich v správe o vzájomnom posudzovaní.

CB je zodpovedný za prípravu, dokumentáciu a poskytovanie všeobecných informácií o produktoch, ktoré sú predmetom žiadosti. Tieto informácie sa poskytnú tímu vzájomného posudzovania na účely ich preskúmania a výberu a musia obsahovať:

- stručný prehľad produktu,
- stav hodnotenia (ak nie je ukončené, uveďte, ktoré časti hodnotenia boli ukončené a ktoré ešte treba vykonať),
- cieľové úrovne EAL a AVA_VAN (a prípadné rozšírenie),
- akékoľvek nároky na súlad s ochranným profilom.

Tím pre vzájomné posudzovanie vyberie aspoň jedno hodnotenie kandidátov, ktoré sa bude posudzovať počas návštevy na mieste CB a prípadne ITSEF.

CB určí kontaktnú osobu, ktorá bude zodpovedná za uľahčenie činností vzájomného posudzovania a za interakciu s vedúcim posudzovacieho tímu.

Kontaktná osoba CB je zodpovedné za:

- Koordinácia termínov a miesta(-ov) návštevy na mieste s tímom pre vzájomné posudzovanie,
- doručenie materiálov CB tímu pre vzájomné posudzovanie počas prípravnej fázy najmenej 4 týždne pred dátumom auditu,

- Koordinácia všetkých požadovaných návštev ITSEF(ov) s tímom pre vzájomného posudzovania,
- Zabezpečenie všetkých potrebných povolení, aby tím pre vzájomné posudzovanie mohol vykonať návštevy na mieste CB a ITSEF(-ov) a mal prístup ku všetkým informáciám potrebným na dokončenie činností vzájomného posudzovania,
- Koordinácia programu vzájomného posudzovania pre CB vrátane plánovania rozhovorov a brífingov certifikačného tímu pre vzájomné posudzovanie, zabezpečenie dostupnosti materiálov, ktoré sa majú preskúmať počas návštevy na mieste, atď.,
- Poskytnutie možnosti vyhotovenia kópií a výtlačkov pre tím vzájomného posudzovania na použitie počas návštevy na mieste;
- v prípade potreby zabezpečiť bezpečné uloženie dokumentov tímu vzájomného posudzovania (napr. v čase obeda, cez noc);
- byť všeobecne k dispozícii na zodpovedanie otázok a riešenie problémov, ktoré sa môžu vyskytnúť počas návštevy na mieste,
- Koordinácia preskúmania správy o vzájomnom posudzovaní zástupcami CB,
- Poskytovanie spätnej väzby vedúcemu tímu vzájomného posudzovania k návrhu správy o vzájomnom posudzovaní.

CB musí mať k dispozícii súkromnú(-é) miestnosť(-ti), ktorá(-é) je(sú) dostatočne veľká(-é) na to, aby sa do nej(nich) počas návštevy(-y) na mieste zmestil tím pre vzájomné posudzovanie a zamestnanci CB. Takáto miestnosť (miestnosti) bude slúžiť ako rokovacia miestnosť počas celej návštevy na mieste.

Počas celej návštevy na mieste bude v rokovacej miestnosti potrebný prístup k záznamom a pracovníkom CB.

5 POVINNOSTI VEDÚCEHO TÍMU VZÁJOMNÉHO POSUDZOVANIA

Jeden člen tímu vzájomného posudzovania bude určený za vedúceho tímu. Vedúci tímu je zodpovedný za tieto úlohy:

- Koordinácia prijímania materiálov od CB,
- Koordinácia rozhodnutia o výbere kandidátskych produktov (a ITSEF) a oznámenie rozhodnutia vzájomného posudzovania CB,
- Vypracovanie programu návštevy na mieste (a na účely prijatia za výrobcu certifikátu na vyššej úrovni v technickej domény (typ 2) vybraného(-ých) ITSEF-u(-ov) na návštevu) a jeho koordinácia s CB,
- Koordinácia a vyplnenie návrhu správy o vzájomnom posudzovaní na konci návštevy na mieste,
- Predloženie záverečnej správy z vzájomného posudzovania ECCG, ,
- v prípade potreby monitorovanie riešenia nevyriešených otázok vyplývajúcich zo vzájomného posudzovania zo strany CB.

6 PRÍPRAVNÁ FÁZA

Tím pre vzájomné posudzovanie by sa mal začať pripravovať približne štyri týždne pred návštevou na mieste. Vzájomne posudzovaná CB poskytne tímu vzájomného posudzovania štyri týždne pred návštevou na mieste prístup ku všetkým písomným zásadám a dokumentom o prevádzkových postupoch. V závislosti od preferencií členov tímu vzájomného posudzovania a povahy potrebnej dokumentácie je potrebné poskytnúť elektronickú a/alebo tlačenú dokumentáciu. Tím vzájomného posudzovania by sa mal pri preskúmaní dokumentácie zamerať na získanie prehľadu o štandardných prevádzkových postupoch CB.

Vedúci tímu vzájomného posudzovania bude koordinovať preskúmanie materiálov počas prípravnej fázy. Ak je potrebné preskúmať veľké množstvo materiálov, tím si ich môže rozdeliť tak, aby členovia preskúmali rôzne časti dokumentácie. Vedúci tímu tiež na záver prípravnej fázy vypracuje a dokončí program návštevy (návštev) na mieste, pričom doň vloží podnety od členov tímu. Program návštevy(-y) na mieste musí byť zaslaný vzájomne posudzovanej CB najneskôr týždeň pred návštevou(-ami) na mieste. Odporúča sa, aby vedúci tímu vzájomného posudzovania udržiaval počas prípravnej fázy úzky kontakt s kontaktnou osobou CB, aby ju informoval o oblastiach, ktoré si počas návštevy na mieste budú vyžadovať ďalšie skúmanie.

CB môže navrhnúť predchádzajúce výsledky vzájomného posudzovania so súvisiacimi výsledkami, aby ich posúdil tím pre vzájomné posudzovanie.

7 FÁZA NÁVŠTEVY NA MIESTE

7.1 Určiť, že stanovy a postupy CB sú v súlade so všeobecnými požiadavkami schémy EUCC

Kontrolný zoznam sa použije na určenie, či procesy, ktoré CB používa na poskytovanie svojich certifikačných služieb, sú dostatočné na zabezpečenie účinného dohľadu nad hodnoteniami a na zabezpečenie toho, aby úspešné certifikácie boli v súlade so spoločnými kritériami a spoločnou metodikou hodnotenia.

CB poskytne všetky relevantné informácie súvisiace s jej akreditáciou na podporu tohto rozhodnutia.

Ak sa tím pre vzájomné posudzovanie rozhodne skontrolovať niektoré postupy CB, malo by sa tak stať pred začatím procesu hodnotenia. Tím vzájomného posudzovania by však mal skontrolovať, či CB uplatňuje svoje postupy. To sa môže uskutočniť počas návštevy na mieste (pozri nižšie) v súvislosti
s konkrétnymi hodnotenými certifikátmi.

7.2 Vykonajte vzájomné posudzovanie

Pri vzájomnom posudzovaní typu 1 by mal tím pre vzájomné posudzovanie vyhradiť na návštevu miesta jeden celý týždeň (5 pracovných dní). Ak sa vzájomné posudzovanie dokončí v kratšom čase, tím nemusí zostať celý týždeň.

V prípade vzájomného posudzovania typu 2 by mal tím pre vzájomné posudzovanie vyhradiť na návštevu(-y) na mieste celé dva týždne. Ak sa vzájomné posudzovanie dokončí v kratšom čase, tím nemusí zostať celé dva týždne.

Tím vzájomného posudzovania má prístup ku všetkej hodnotiacej a certifikačnej dokumentácii, ktorú CB použila počas procesu certifikácie, a najmä pri preskúmavaní hodnotiacej dokumentácie, a je mu umožnené pozorovať všetky činnosti vykonávané počas takéhoto preskúmania. Ak sa počas návštevy na mieste uskutoční zasadnutie hodnotiaceho tímu/certifikačného orgánu, tím vzájomného posudzovania by mal toto zasadnutie sledovať.

Tím vzájomného posudzovania by nemal úplne preskúmať prácu ITSEF, na ktorú sa môže vzťahovať jeho akreditácia podľa normy ISO/IEC 17025. Tím vzájomného posudzovania by však mal posúdiť, či sú výstupy, ktoré má CB k dispozícii, dostatočne kvalitné na to, aby CB mohla určiť, že hodnotenie bolo vykonané v súlade s príslušnou metodikou.

Pri vzájomnom posudzovaní typu 2 tím vzájomného posudzovania určí odbornú kompetentnosť ITSEF tak, že:

- návšteva technického laboratória v areáli ITSEF,
- rozhovory s hodnotiteľmi o technických položkách týkajúcich sa technickej doméne a jej špecifických metód útoku.

Zistenia zodpovedajú buď

- nezhody, ktoré súvisia s požiadavkou z platného kontrolného zoznamu alebo so spoločným chápaním „state of the art“ a operatívnych postupov, ktoré nie sú splnené (alebo nie sú splnené). Posledné uvedené budú prerokované s ECCG a v prípade potreby by mohli byť začlenené ako nová položka do zoznamov na použitie pri budúcich vzájomných posudzovaniach.
- alebo pripomienky, ktoré zodpovedajú návrhom na zlepšenie predloženým tímom vzájomného posudzovania, ktoré nie sú priamo spojené s požiadavkami z kontrolného zoznamu.

Nezhoda môže byť kritická alebo nekritická. Kritická nezhoda spochybňuje spoľahlivosť výsledkov zistených posudzovanou CB. Tím vzájomného posudzovania analyzuje a opisuje vplyv každej kritickej nezhody.

Na konci návštevy na mieste by mal tím pre vzájomné posudzovanie predložiť zoznam zistení (aspoň návrh zoznamu nezhôd v súvislosti s ich úrovňou kritickosti) vzájomne posudzovanej CB, aby posudzovaná CB mohla vypracovať návrh akčného plánu na pokrytie zistení. Tím vzájomného posudzovania by mal najneskôr do štyroch týždňov po návšteve na mieste poskytnúť posudzovanej CB konečný zoznam nezhôd (priradený k ich úrovni kritickosti).

Ak sa zistia nezrovnalosti, CB môže požiadať tím pre vzájomné posudzovanie o podporu pri vypracovaní akčného plánu spojeného s časovým harmonogramom na vykonanie príslušných opatrení.

8 SPRÁVY

Tím vzájomného posudzovania vypracuje správu, v ktorej zhrnie a vysvetlí svoje zistenia.

Správa by mala byť interne odsúhlasená v rámci tímu vzájomného posudzovania. Ak sa tím vzájomného posudzovania nemôže interne dohodnúť, v správe sa uvedú väčšinové a menšinové názory.

Nesúhlas CB so zisteniami možno do správy zapracovať najneskôr do jedného mesiaca od vypracovania správy.

V správe sa uvedie aj stanovisko tímu vzájomného posudzovania k relevantnosti navrhovaného akčného plánu na pokrytie zistení, ak bol tento plán predložený tímu pred doručením správy ECCG. Ak sa pred vydaním správy predložia dôkazy, ktoré pokrývajú kritickú nezhodu, tím môže prehodnotiť kritickosť nezhody a túto zmenu zdokumentuje v správe.

Posudzovací tím môže do svojej správy zahrnúť relevantné výsledky a zistenia z iných vzájomných posudzovaní, ktoré opätovne použil.

Zistenia tímu vzájomného posudzovania zahrnuté do správy musia byť jasne označené jedinečným a jednoznačným identifikátorom.

Záverečná správa sa vypracuje do troch mesiacov po návšteve na mieste a pred jej zaslaním ECCG ju preskúma vzájomne posudzovaný CB.

Pri príprave záverečnej správy sa budú dodržiavať tieto kroky:

1. tím pre vzájomné posudzovanie vypracuje návrh správy, ktorý obsahuje všetky zistenia, nevyriešené menej závažné a závažné nezrovnalosti zistené počas vzájomného posudzovania vo fáze prípravy a vo fáze návštevy na mieste, a doručí ho posudzovanej CB na pripomienkovanie (jeden mesiac).
2. posudzovaná CB pripomienkuje návrh správy, pričom upozorní na všetky sporné body a navrhne zmeny v správe (jeden mesiac).
3. tím pre vzájomné posudzovanie zváži pripomienky, ktoré CB dostal, a vypracuje záverečnú správu s prípadnými revíziami (jeden mesiac).

Všetky tri dokumenty v bodoch 1 až 3 doručí tím pre vzájomné posudzovanie ECCG ako dôkaz záverečnej fázy podávania správ o vzájomnom posudzovaní.

Ak sa zistia odchýlky, ktoré sú pre NAB relevantné, NAB sa o tom informuje. Správa obsahuje jeden z troch možných verdiktov:

Vyhovuje: CB splnil všetky požiadavky a nevyžaduje sa žiadne opatrenie.

Vyhovuje s kontrolovanými (menej závažnými) nezhodami: CB nesplnila všetky požiadavky, ale predložila príslušný akčný plán a prijateľný časový harmonogram na odstránenie nezhôd zistených tímom vzájomného posudzovania. V správe nie je identifikovaná žiadna zostávajúca kritická nezhoda.

Zlyhanie: CB nesplnila požiadavky a nepredložila príslušný akčný plán a prijateľný časový harmonogram na nápravu nezhôd zistených tímom vzájomného posudzovania

Vedúci tímu vzájomného posudzovania (alebo vhodný zástupca, ktorý je plne oboznámený s hodnotením) predloží ECCG správu vrátane prípadných nezhôd v rámci tímu so vzájomne posudzovanou CB. Predstaví zistenia tímu a jeho hodnotenie toho, ako opatrenia navrhnuté CB vyriešia problémy.

V prípade potreby sa do kontrolného zoznamu posudzovania doplnia vhodné dodatky, ktoré pomôžu budúcim tímom vzájomného posudzovania.

9 PRIJATIE SPRÁVY O VZÁJOMNOM POSUDZOVANÍ

Nasledujúci postup je určený na zaručenie primeraného zapojenia posudzovanej CB s cieľom preukázať rýchle riešenie nezhôd. Tento postup tiež pomáha obmedziť čas na prijatie vzájomného posudzovania.

1. ECCG požiada podskupinu ECCG, ktorá sa venuje údržbe schémy EUCC, aby pripravila stanovisko, ktoré ECCG prijme k vykonanému vzájomnému posudzovaniu.
2. Podskupina ECCG sa stretne, aby prediskutovala výsledok vzájomného posudzovania (na základe dokumentov 1 - 3) a pozve na stretnutie tím pre vzájomné posudzovanie a hodnotené CB. Po zasadnutí podskupina ECCG vydá jeden z nasledujúcich návrhov stanoviska:

   - záverečná správa posudzovacieho tímu sa navrhuje prijať v tejto podobe;
   - navrhuje sa prijať zmenenú a doplnenú záverečnú správu posudzovacieho tímu.

   V prípade nezrovnalostí bude stanovisko, ktoré prijme ECCG, obsahovať odporúčanie pre posudzovanú CB, aby tieto nezrovnalosti vyriešila, s uvedením lehoty, ktorá je na toto riešenie určená. Toto trvanie by malo byť vo všeobecnom prípade obmedzené na 2 mesiace a nemalo by presiahnuť 6 mesiacov.
3. podskupina ECCG poskytne ECCG:

   - zápisnicu zo zasadnutia;
   - navrhované stanovisko, ktoré má prijať ECCG.

   Podskupina ECCG zabezpečí, aby sa ECCG postúpila akákoľvek spätná väzba o nezhodách alebo odporúčaniach, ktoré CB, ktorá prešla vzájomným posudzovaním alebo NAB, dostala.
4. ECCG poskytne svoje stanovisko k návrhu stanoviska. V prípade kladného stanoviska posudzovaná CB:

   a. buď prejsť vzájomným posudzovaním (ak návrh stanoviska uvádza pozitívny verdikt vzájomného posudzovania). Pozitívny verdikt bude zverejnený na webovej stránke agentúry ENISA priamo so sprievodnými zisteniami vzájomného posudzovania.

   b. alebo sa odporúča prijať potrebné opatrenia na vyriešenie nezhôd v stanovenej lehote. Odporúčanie nebude zverejnené na webovej stránke agentúry ENISA.

   ECCG by tiež mohla požiadať podskupinu ECCG o opätovné preskúmanie vzájomného posudzovania (opäť prejdite k bodu 2.) len jedenkrát.
5. Ak ECCG požiada CB o nápravné opatrenia, po ich vykonaní vydá posudzovaná CB do 2 mesiacov správu podskupine ECCG.
6. Podskupina ECCG sa do 2 mesiacov stretne s posudzovanou CB a posudzovacím tímom, aby prediskutovala stav riešenia nezhôd. Nedostatok správy od posudzovanej CB nebude brániť podskupine ECCG v uskutočnení stretnutia.
7. Podskupina ECCG pripraví stanovisko, ktoré má ECCG prijať a ktoré bude obsahovať buď kladné (úspešná náprava nezhôd), alebo záporné (pretrvávajúce nezhody), a doručí navrhované stanovisko a zápisnicu zo zasadnutia ECCG.
8. ECCG vypracuje svoje stanovisko na základe návrhu stanoviska a prijme konečný výsledok (vrátane zvyškového odporúčania alebo bez odporúčania pre CB). ECCG prijme navrhované stanovisko alebo prijme svoje vlastné stanovisko bez toho, aby sa opakovali ďalšie iterácie s podskupinou ECCG. Stanovisko prijaté ECCG sa uverejní spolu so všetkými príslušnými dokumentmi na webovej stránke agentúry ENISA.

39. PRÍLOHA 13: OBSAH SPRÁVY O CERTIFIKÁCII

ÚČEL

Táto príloha podrobne opisuje obsah správy o certifikácii.

Správa o certifikácii je zdrojom podrobných informácií o bezpečnosti produktu IKT alebo ochranného profilu pre všetky zainteresované strany. Jej cieľom je poskytnúť spotrebiteľom praktické informácie o produkte IKT alebo ochrannom profile. Správa o certifikácii nemusí a ani by nemala obsahovať chránené informácie.

KONKRÉTNY STAV

Žiadne.

KRÍŽOVÝ ODKAZ NA KAPITOLU(-Y), V KTOREJ(-ÝCH) SÚ TIETO PRVKY VYHLÁSENÉ ZA UPLATNITEĽNÉ

Kapitola 17, OBSAH A FORMÁT CERTIFIKÁTOV.

Na základe technickej správy hodnotenia (ETR) vypracovanej ITSEF vydavateľ certifikátu vypracuje ku každému certifikátu správu o certifikácii.

Správa o certifikácii je zdrojom podrobných informácií o produkte IKT a o tom, ako ho bezpečne zaviesť, a preto poskytuje praktické a verejne zdieľateľné informácie o produkte IKT pre koncových používateľov a zainteresované strany. Správa o certifikácii obsahuje aspoň tieto časti:

1 ZHRNUTIE

Zhrnutie je stručným zhrnutím celej správy. Informácie obsiahnuté v tejto časti poskytujú publiku jasný a stručný prehľad výsledkov hodnotenia a obsahujú tieto informácie:

- názov hodnoteného produktu IKT, zoznam komponentov produktu, ktoré sú súčasťou hodnotenia, a výrobca alebo poskytovateľ verzie;
- názov ITSEF, ktorý pristúpil k hodnoteniu, a prípadne subdodávateľov;
- dátum ukončenia hodnotenia;
- odkaz na hodnotiacu technickú správu vypracovanú ITSEF;
- stručný opis výsledkov správy vrátane:
  - Verzia/release CC použitá na hodnotenie;
  - Dosiahnutá úroveň záruky CSA, balík záruky CC vrátane dosiahnutej úrovne AVA_VAN;
  - funkčnosť;
  - prehľad hrozieb a politík organizačnej bezpečnosti (OSP), ktoré hodnotený produkt IKT rieši;
  - špeciálne požiadavky na konfiguráciu;
  - predpoklady o prevádzkovom prostredí;
  - prípadne prítomnosť schváleného mechanizmu správy záplat;
  - zrieknutie sa zodpovednosti.

2 IDENTIFIKÁCIA

Hodnotený produkt IKT sa jasne identifikuje uvedením týchto informácií:

- názov hodnoteného produktu IKT;
- výpočet komponentov produktu, ktoré sú súčasťou hodnotenia;
- číslo verzie softvéru;
- identifikáciu všetkých príslušných softvérových záplat;
- číslo verzie hardvéru vrátane prípadných periférnych zariadení;

- názov a kontaktné údaje výrobcu alebo poskytovateľa;
- prípadne použiteľný mechanizmus správy záplat;
- odkaz na webové sídlo výrobcu alebo poskytovateľa na prístup k doplnkovým informáciám o kybernetickej bezpečnosti certifikovaného produktu IKT v súlade s článkom 55 CSA.

Informácie uvedené v tejto časti musia byť čo najpresnejšie, aby sa zabezpečilo, že bude možné obnoviť celé a presné zobrazenie produktu IKT na účely jeho používania alebo budúcich hodnotení.

3 BEZPEČNOSTNÉ POLITIKY

Tento oddiel obsahuje opis bezpečnostnej politiky produktu IKT a politiky alebo pravidlá, ktoré musí hodnotený produkt IKT dodržiavať a/alebo presadzovať. Musí obsahovať odkaz a stručný opis:

- zásady zaobchádzania so zraniteľnosťou výrobcu alebo poskytovateľa;
- zásady kontinuity záruky výrobcu alebo poskytovateľa.

V prípade potreby môže takáto politika zahŕňať podmienky týkajúce sa používania mechanizmu riadenia záplat a v tomto oddiele sa potom uvedie, že počas platnosti certifikátu je možné uplatňovať mechanizmy záplat v súlade s touto politikou.

4 PREDPOKLADY A OBJASNENIE ROZSAHU PÔSOBNOSTI

Tento oddiel obsahuje informácie týkajúce sa aspektov prostredia/konfigurácie, v ktorom sa očakáva používanie produktu IKT. Informácie musia obsahovať:

- predpoklady používania, ktoré poskytujú základnú úroveň produktu počas hodnotenia, ako napríklad správna inštalácia a konfigurácia a splnenie minimálnych požiadaviek na hardvér;
- predpoklady prostredia týkajúce sa produktu IKT počas hodnotenia;
- zoznam a opisy hrozieb pre produkt IKT, ktoré neboli zahrnuté do hodnotenia.

Informácie uvedené v tomto oddiele musia byť čo najpresnejšie, aby koncoví používatelia mohli prijímať informované rozhodnutia o rizikách spojených s používaním produktu IKT.

5 ARCHITEKTONICKÉ INFORMÁCIE

Tento oddiel obsahuje opis produktu IKT a jeho hlavných komponentov na vysokej úrovni na základe návrhu subsystémov ADV_TDS.

6 DOPLŇUJÚCE INFORMÁCIE O KYBERNETICKEJ BEZPEČNOSTI

Úplný zoznam doplňujúcich informácií o kybernetickej bezpečnosti produktov IKT sa poskytuje v súvislosti s článkom 55 CSA. Všetka príslušná dokumentácia sa uvedie s číslami verzií.

7 TESTOVANIE PRODUKTOV IKT

Tento oddiel obsahuje tieto informácie:

- skúšobné zariadenie, ktoré vykonalo hodnotenie
- názov a kontaktný bod orgánu alebo inštitúcie, ktorá vydala certifikát, vrátane zodpovednej NCCA
- názov ITSEF, ktorý vykonal hodnotenie, ak sa líši od certifikačného orgánu
- identifikáciu typu úrovne záruky od CSA (buď "významná", alebo "vysoká") a (ak je k dispozícii) príslušnú značku/štítok
- identifikáciu použitých komponentov záruk z časti 3 CC
- použité kritériá a metodika hodnotenia bezpečnosti a ich verzia
- úplné a presné nastavenia a konfiguráciu IT produktu počas hodnotenia vrátane prevádzkových poznámok a pozorovaní, ak sú k dispozícii;
- každý použitý ochranný profil vrátane nasledujúcich informácií:
    - Vývojár ochranného profilu
    - Názov/identifikátor ochranného profilu
    - číslo certifikátu
    - názov vydavateľa certifikátu a ITSEF
    - Balík záruky požadovaný pre produkt, ktorý je v súlade s ochranným profilom

8 VÝSLEDKY HODNOTENIA A INFORMÁCIE TÝKAJÚCE SA CERTIFIKÁTU

Tento oddiel obsahuje tieto informácie:

- dosiahnutá úroveň záruky z CSA (buď "významná", alebo "vysoká");
- požiadavky bezpečnostných záruk z časti 3 CC, ktoré produkt IKT spĺňa, vrátane úrovne AVA_VAN;
- podrobný opis požiadaviek bezpečnostných záruk, ako aj podrobnosti o tom, ako produkt spĺňa každú z nich;
- dátum vydania a obdobie platnosti certifikátu
- Unikátne-ID certifikátu.

9 ZHRNUTIE BEZPEČNOSTNÉHO ZÁMERU

Bezpečnostný zámer je:

- zahrnutý v správe o certifikácii;
- alebo na ktoré sa odkazuje a ktoré sú zhrnuté v správe o certifikácii a ktoré sa poskytujú spolu so správou o certifikácii na uverejnenie v súvislosti s ňou.

Môže byť anonymizovaná odstránením alebo parafrázovaním chránených technických informácií: Príloha 14: ANONYMIZOVANIE BEZPEČNOSTNÉHO ZÁMERU PRED ZVEREJNENÍM definuje pravidlá anonymizácie bezpečnostného zámeru a opisuje minimálny obsah výsledného dokumentu.

10 AK JE K DISPOZÍCII, ZNAČKA ALEBO ŠTÍTOK PRIRADENÝ K SCHÉME

Ak je k dispozícii, môže sa vložiť značka alebo štítok súvisiaci so schémou, ako je definované v kapitole 10, ZNAČKY A ŠTÍTKY.

11 BIBLIOGRAFIA

V časti Bibliografia sa uvedie všetka dokumentácia, na ktorú sa odkazuje a ktorá bola použitá ako zdrojový materiál pri zostavovaní správe o certifikácii. Tieto informácie zahŕňajú a neobmedzujú sa na:

- odkaz na použité kritériá bezpečnostného hodnotenia, metodiku a podporné dokumenty a ich verziu;
- technickú správu hodnotenia;
- technickú správu hodnotenia pre zložené hodnotenie (ak sa uplatňuje);
- technickú referenčnú dokumentáciu;
- dokumentácia vývojára použitá pri hodnotení.

S cieľom zaručiť reprodukovateľnosť hodnotenia musí byť všetka dokumentácia jednoznačne označená správnym dátumom vydania a správnym číslom verzie.

40. PRÍLOHA 14: ANONYMIZOVANIE BEZPEČNOSTNÉHO ZÁMERU PRED ZVEREJNENÍM

ÚČEL

Bezpečnostný zámer, ktorý má byť zahrnutý do správy o certifikácii alebo na ktorý sa má v nej odkazovať, ako sa vyžaduje v prílohe 13: OBSAH SPRÁVY O CERTIFIKÁCII, môže byť anonymizovaný odstránením alebo parafrázovaním chránených technických informácií. V tejto prílohe sa vymedzujú pravidlá na anonymizovanie bezpečnostného zámeru a opisuje sa minimálny obsah výsledného dokumentu, ktorý sa nazýva ST- lite.

KONKRÉTNY STAV

Žiadne.

KRÍŽOVÝ ODKAZ NA KAPITOLU(-Y), V KTOREJ(-ÝCH) SÚ TIETO PRVKY VYHLÁSENÉ ZA UPLATNITEĽNÉ

Príloha 13: OBSAH SPRÁVY O CERTIFIKÁCII.

1 ÚVOD

Správa o certifikácii je zdrojom podrobných informácií o bezpečnosti produktu IKT alebo ochranného profilu pre všetky zainteresované strany. Jej cieľom je poskytnúť spotrebiteľom praktické informácie o produktu IKT alebo ochrannom profile. Bezpečnostný zámer, ktorý sa má zahrnúť do správy o certifikácii alebo na ktorý sa v nej má odkazovať, ako sa vyžaduje v prílohe 13: OBSAH SPRÁVY O CERTIFIKÁCII môže byť anonymizovaný odstránením alebo parafrázovaním chránených technických informácií. Výsledný dokument sa nazýva ST-lite. ST-lite musí byť skutočným zobrazením celého ST. To znamená, že ST-lite nesmie vynechať informácie, ktoré sú potrebné na pochopenie bezpečnostných vlastností TOE a rozsahu hodnotenia.

2 MINIMÁLNY OBSAH

Na základe štrukturálneho náčrtu spoločných kritérií (CC časť 1, príloha C) sa ďalej opisuje minimálny obsah ST-lite:

- Úvod ST vo všeobecnosti neobsahuje žiadne vlastnícke informácie. Preto nie je potrebné úvod ďalej anonymizovať. ST-lite potrebuje jedinečný identifikátor, aby sa odlišoval od úplného ST.
- Opis TOE by sa mohol zredukovať. Môže obsahovať vlastnícke a podrobné informácie o konštrukcii TOE, ktoré by sa nemali zverejňovať.
- Opis bezpečnostného prostredia TOE (predpoklady, hrozby, organizačné bezpečnostné politiky) nemožno redukovať. Všetky tieto informácie sú potrebné na pochopenie rozsahu hodnotenia.
- Bezpečnostné ciele sa nemôžu znížiť, všetky informácie musia byť zverejnené, aby bolo možné pochopiť zámer hodnotenia ST a TOE.
- Všetky bezpečnostné požiadavky musia byť zverejnené. Poznámky k aplikácii by mohli poskytnúť informácie o tom, ako boli použité komponenty CC časť 2 na pochopenie ST. Upresnenia a aplikačné poznámky by však mohli byť anonymizované tak, aby sa z nich odstránili vlastnícke informácie (napr. o návrhu).
- Súhrnná špecifikácia TOE môže byť upravená tak, aby sa z nej anonymizovali vlastnícke informácie (napr. o dizajne). Minimálne musia byť zahrnuté všetky bezpečnostné funkcie TOE.
- Zahŕňajú sa tvrdenia o PP.
- Odôvodnenie môže byť anonymizované tak, aby sa odstránili informácie, ktoré sú predmetom vlastníctva.

3 HODNOTENIE

Hodnotenie TOE musí byť založené na úplnom bezpečnostnom zámere, ako je uvedené v kritériách.

ST-lite sa nebude formálne hodnotiť podľa kritérií. Kontrolu zhody ST-lite s kompletným bezpečnostným zámerom môže vykonať hodnotiteľ alebo certifikačný orgán. Správa o certifikácii musí odkazovať na kompletný ST aj na ST-lite. CB musí schváliť ST-lite na zverejnenie.

41. PRÍLOHA 15: SPRÁVA ZÁPLAT

ÚČEL

Táto príloha na skúšobné použitie[68] zavádza proces správy záplat na podporu požiadaviek súvisiacich s manipuláciou so zraniteľnosťami, ktoré sú definované v kapitole 14, PRAVIDLÁ TÝKAJÚCE SA RIEŠENIE ZRANIOTEĽNOSTÍ, a ktoré sa môžu použiť aj na činnosti udržiavania certifikácie , ako je definované v kapitole 12, PODMIENKY VYDÁVANIA, UDRŽIAVANIA, POKRAČOVANIA A OBNOVOVANIA CERTIFIKÁTOV.

KONKRÉTNY STAV

Na skúšobné použitie[69]. Obdobie skúšobného používania by malo byť 2 roky, ale udržiavajúca organizácia schémy môže navrhnúť skrátenie tohto obdobia, ak sa skôr zistí významný pokrok v jeho celosvetovom prijatí.

KRÍŽOVÝ ODKAZ NA KAPITOLU(-Y), V KTOREJ(-ÝCH) SÚ PRVKY VYHLÁSENÉ ZA UPLATNITEĽNÉ

Kapitola 12, PODMIENKY VYDÁVANIA, UDRŽIAVANIA, POKRAČOVANIA A OBNOVOVANIA CERTIFIKÁTOV. Kapitola 14, PRAVIDLÁ TÝKAJÚCE SA RIEŠENIE ZRANITEĽNOSTÍ.

1 ÚVOD

Produkt môže obsahovať mechanizmus správy záplat posúdený v rámci jeho certifikácie za týchto podmienok. Obsah tejto prílohy dopĺňa obsah prílohy 11, KONTINUITA ZÁRUKY. V prípade certifikovaného produktu IKT sa môžu uplatniť oba prístupy, ale ak bol zvolený prístup správy záplat, uplatňujú sa tieto požiadavky.

2 PLATNÉ POŽIADAVKY

Takýto mechanizmus správy záplat môže byť založený na:

- na základe podmienok definovaných v technickej správe ISO SC27 WG3 "Rozšírenie pre správu záplat pre 15408 a 18045", ako je definované na https://www.jtsec.es/papers/Technical/Report_Patch_Management.pdf;
- alebo o návrhu pracovnej skupiny ISCI WG1 pre nové komponenty a balíky SAR v CC pre správu záplat, ako je definované na stránke https://cclab.com/isci-workgroup.

Pri uplatnení ktorejkoľvek z uvedených možností musí výrobca alebo poskytovateľ IKT produktu počas počiatočnej certifikácie:

- podrobne popísať procesy záplat v súlade s požiadavkami na obsah a prezentáciu prijatého procesu správy záplat;
- definovať hranice TOE, ak je zahrnutý ADV_ARC, a ak nie, opis hraníc TOE sa vloží do bezpečnostného zámeru.
- podrobne popísať mechanizmy záplat pomocou príslušných pracovných jednotiek vybraného prístupu.

ITSEF počas počiatočnej certifikácie overí, či:

- vývojár implementoval požiadavky prijatého procesu riadenia záplat pomocou príslušných pracovných jednotiek SAR;
- Hranice TOE sú oddelené tak, aby zmeny vykonané v oddelených procesoch neovplyvnili bezpečnosť TOE;
- Mechanizmy záplat fungujú v súlade s tvrdeniami.

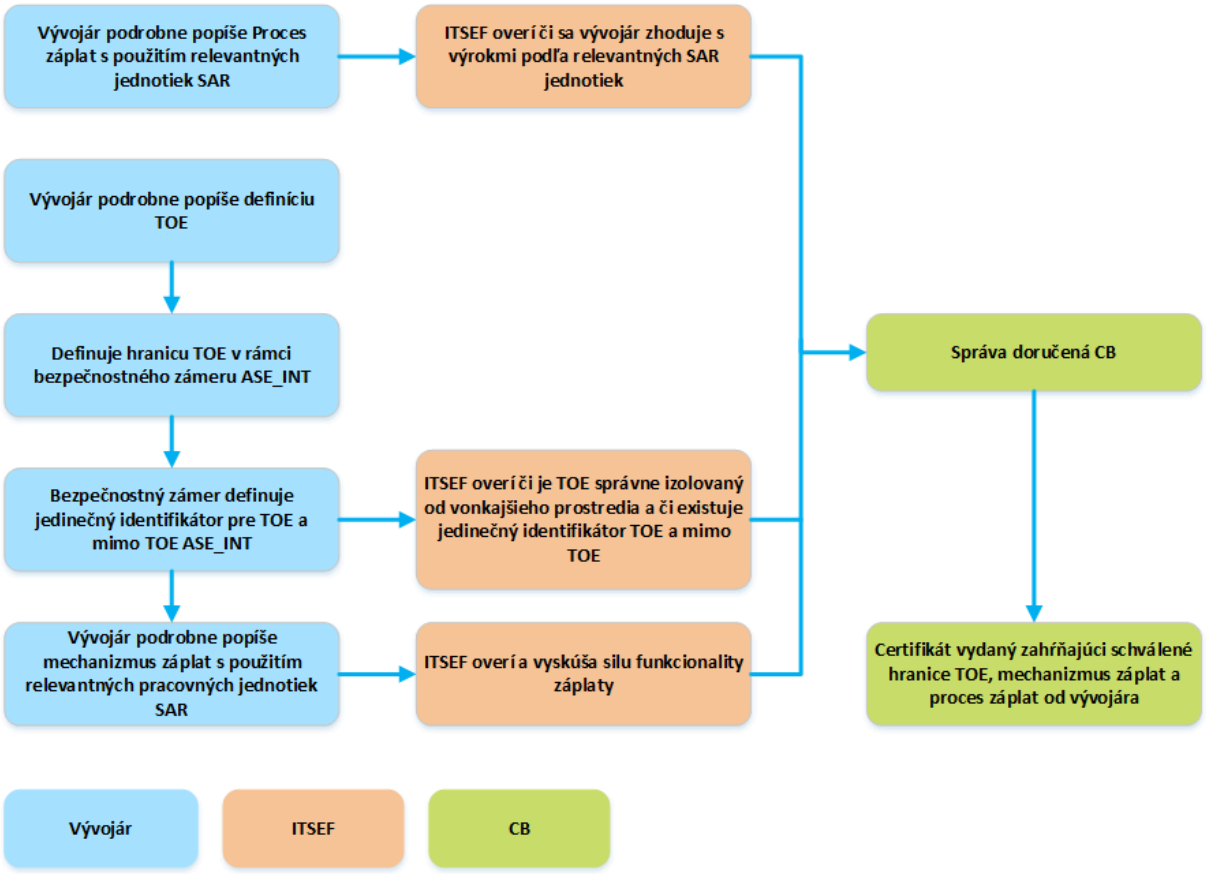
CB zahrnie do správy o certifikácii použitý mechanizmus správy záplat a uvedie, že počas platnosti

[68] Ako je definované v kapitole 8, ŠPECIFICKÉ KRITÉRIA A METÓDY HODNOTENIA

[69] Ako je definované v kapitole 8, ŠPECIFICKÉ KRITÉRIA A METÓDY HODNOTENIA.

certifikátu je možné použiť ďalej opísané mechanizmy záplat.

Obrázok 1: *Proces správy záplat*



Počas fázy *vývoja nápravy* spracovania zraniteľnosti sa určí oprávnená úroveň záplaty na základe prvkov uvedených v analýze zraniteľnosti a v súlade s nasledujúcou tabuľkou:

Tabuľka 1: *Uplatniteľné úrovne záplat*

Blízkosť alebo dostupnosť možného útoku	Úroveň zmeny, ktorú je potrebné uplatniť	Uplatniteľné úrovne záplat
Útok je k dispozícii a môže byť zneužitý (zneužiteľná zraniteľnosť)	Mimo TOE	Úroveň 1
	Menej významná	Kritický aktualizačný tok/úroveň 2
	Významná	Kritický aktualizačný tok/úroveň 3
Zraniteľnosť, ktorú možno použiť na vytvorenie útoku (zneužiteľná alebo potenciálna zraniteľnosť)	Mimo TOE	Úroveň 1
	Menej významná	Úroveň 2 s potenciálne kritickým aktualizačným tokom
	Významná	Úroveň 3 s potenciálne kritickým aktualizačným tokom
Zraniteľnosť, pri ktorej útok nie je pravdepodobný alebo ju nemožno použiť na vytvorenie potenciálu útoku alebo zvyškovej zraniteľnosti)	Mimo TOE	Úroveň 1
	Menej významná	Úroveň 2
	Významná	Úroveň 3

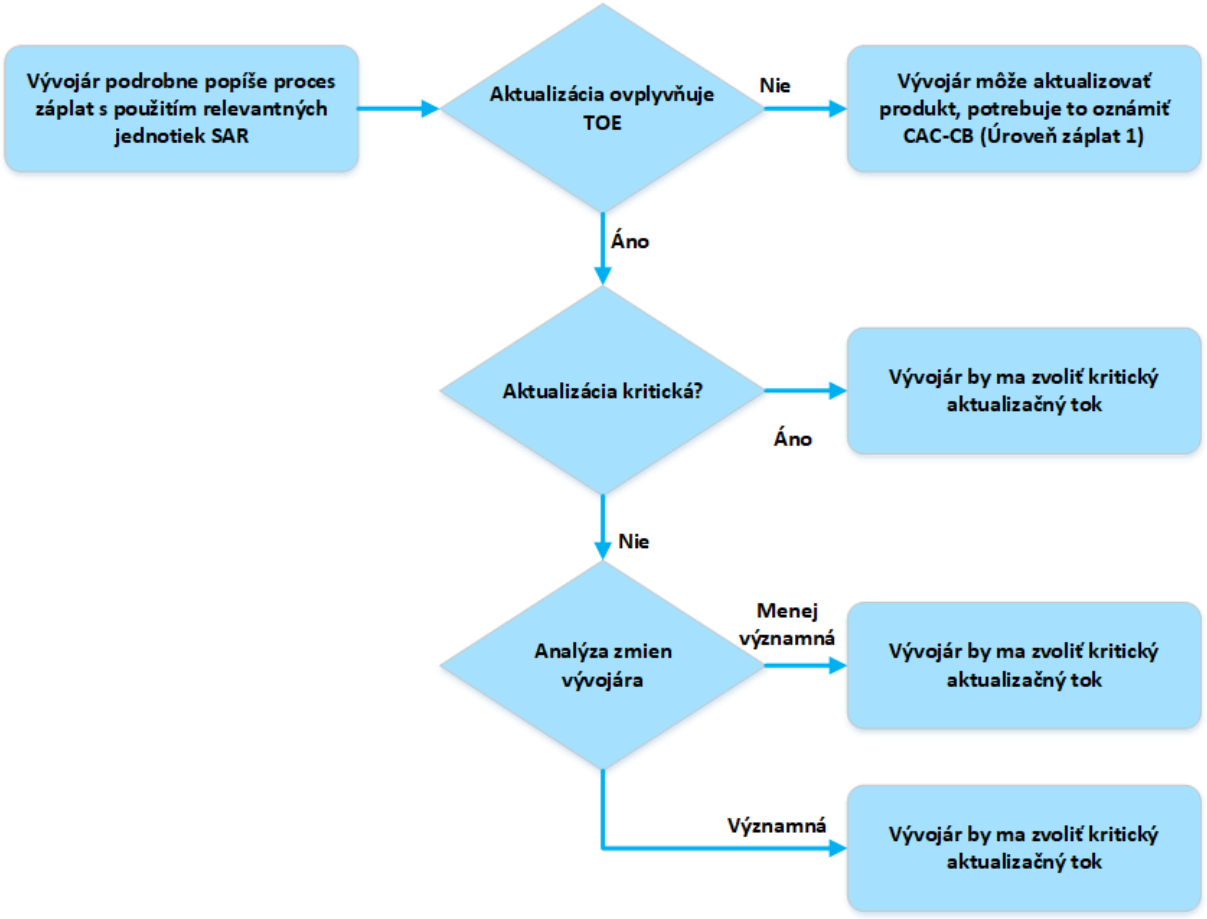
Menej významné/významné zmeny sa vzťahujú na definície uvedené v prílohe 11, KONTINUITA

ZÁRUKY, a v časti Usmernenia na uplatňovanie uvedené nižšie.

Úrovne záplat sa definujú za týchto podmienok.

Úroveň záplaty 1 sa uplatňuje v prípade, že TOE je súčasťou väčšieho produktu IKT, a časti produktu, ktoré nemajú vplyv na TOE, môžu byť opravené vždy, keď je to potrebné. Počiatočné hodnotenie podľa spoločných kritérií jasne definuje rozsah TOE a preukáže, že zmeny mimo rozsahu TOE nemôžu ovplyvniť bezpečnosť certifikovaného TOE, ako je uvedené vyššie. Výsledok tohto vymedzenia
a preukázania sa uvedie v správe o certifikácii, v ktorej sa podrobne uvedie, čo sa môže zmeniť podľa procesu úrovne záplaty 1.

Obrázok 2: *Zobrazenie procesu aktualizácie z pohľadu vývojára*



Zmeny produktu v rámci úrovne záplaty 1 sa vykonávajú na základe rozhodnutia a na zodpovednosť vývojára. Vývojár do piatich pracovných dní informuje CAB o všetkých takto uplatnených zmenách
a CAB môže rozhodnúť o uplatnení rozhodnutia CB o údržbe alebo iného príslušného rozhodnutia CB.

Na menej významné zmeny sa vzťahuje úroveň záplaty 2. Aby bol tento prístup k záplatám možný, musí sa počas prvotnej certifikácie posúdiť a certifikovať možnosť uplatnenia záplaty a počas zmien sa musia uplatňovať dohodnuté metódy.

Výrobca alebo poskytovateľ po analýze uplatniteľnosti zraniteľnosti vypracuje a otestuje opravnú záplatu v súlade s použitým prijatým prístupom.

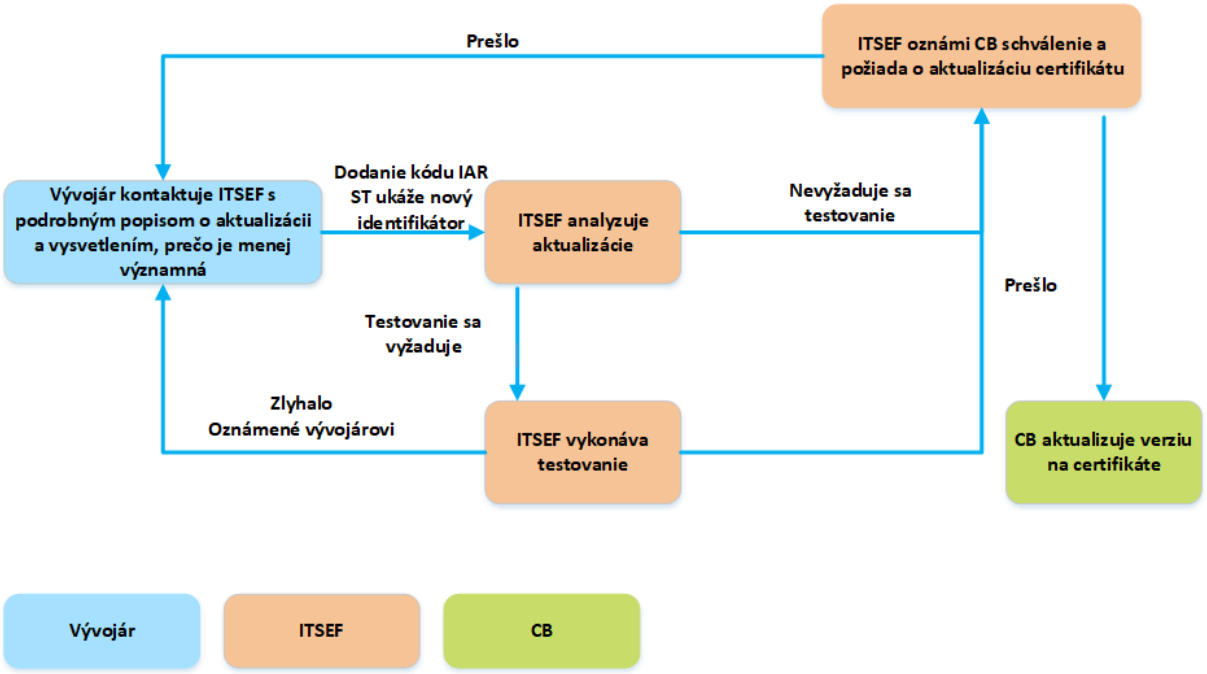
Vypracuje sa IAR spolu so zmenenými dôkazmi/dokumentáciou a zašle sa ITSEF na preskúmanie.
V prípade, že zmeny majú vplyv aj na kód a ADV_IMP je súčasťou procesu hodnotenia, ITSEF preskúma aj zmeny kódu. ITSEF pristúpi k akémukoľvek požadovanému testovaniu.

Pri tomto prístupe úrovne záplaty 2 sa pred opravou produktu pristúpi k hodnoteniu ITSEF. Časový limit pre hodnotenie sa môže dohodnúť medzi zainteresovanými stranami procesu na základe možných škôd, ktoré by zneužitá zraniteľnosť predstavovala.

Výsledky hodnotenia určia, či výrobca alebo poskytovateľ vyhlási záplatu za vhodnú na ďalšie nasadenie alebo uvoľnenie.

ITSEF oznámi CB takéto výsledky a poskytne hodnotiacu dokumentáciu tak CB, ako aj vývojárovi. Vývojár môže začať záplatu certifikovaného produktu IKT len vtedy, ak výsledky hodnotenia vyhlásili záplatu za prijateľnú na vydanie. Za záplatu je zodpovedný vývojár produktu IKT. Na základe poskytnutej dokumentácie CB v prípade potreby rozhodne o aktualizácii verzie v certifikáte alebo prijme rozhodnutie na základe certifikačného procesu. Žiadosť o záplatu tu nemusí čakať na výsledky certifikačného procesu.

Obrázok 3: *Úroveň záplaty 2*



Úroveň záplaty 3 pozostáva z uplatnenia už existujúcich ustanovení definovaných v prílohe 11, KONTINUITA ZÁRUKY, pre významnú zmenu.

Proces kritického toku aktualizácií: táto dodatočná úroveň záplat sa uplatňuje na zmeny, pri ktorých je už možné zneužiť útok alebo je aktualizácia kritická a musí sa urýchlene vydať. Zamýšľané prípady použitia môžu zahŕňať:

- Zraniteľnosti, ktoré sú verejne známe a zneužiteľné;
- Produkt sa používa v rámci kritickej infraštruktúry;
- Uplatňujú sa otázky zodpovednosti;
- Bezpečnosť je ohrozená.

Proces toku kritických aktualizácií nenahrádza úroveň záplat 2 alebo 3 a používa sa ako spôsob, ktorým výrobca alebo poskytovateľ rýchlo nasadí alebo vydá kritickú aktualizáciu a neskôr nasleduje úroveň záplat 2 alebo 3.

Kritický aktualizačný tok sa môže použiť len na TOE, na ktorých boli certifikované príslušné opravné mechanizmy. Za uplatnenie kritického aktualizačného toku zodpovedá výrobca alebo poskytovateľ produktu IKT.

Výrobca alebo poskytovateľ po overení uplatniteľnosti zraniteľnosti a posúdení, že táto oprava je kritickej povahy, vypracuje a otestuje opravnú záplatu v súlade s použitým prijatým prístupom.

Toto je jediný prípad, keď je oprava nasadená alebo vydaná pred preskúmaním. ITSEF a CB sú o zmenách informované do piatich pracovných dní a vykonajú potrebné hodnotiace a certifikačné činnosti. Tento proces sa môže začať súbežne so zmenou, ale aplikácia opravy nemusí čakať na výsledky procesu hodnotenia a certifikácie.

ITSEF vyhodnotí už nasadenú záplatu s najvyššou prioritou, aby vyhodnotil zmeny a vytvoril príslušnú dokumentáciu vo vopred dohodnutom čase podľa dohody s výrobcom alebo poskytovateľom.

Výsledky hodnotenia sa zašlú CB.

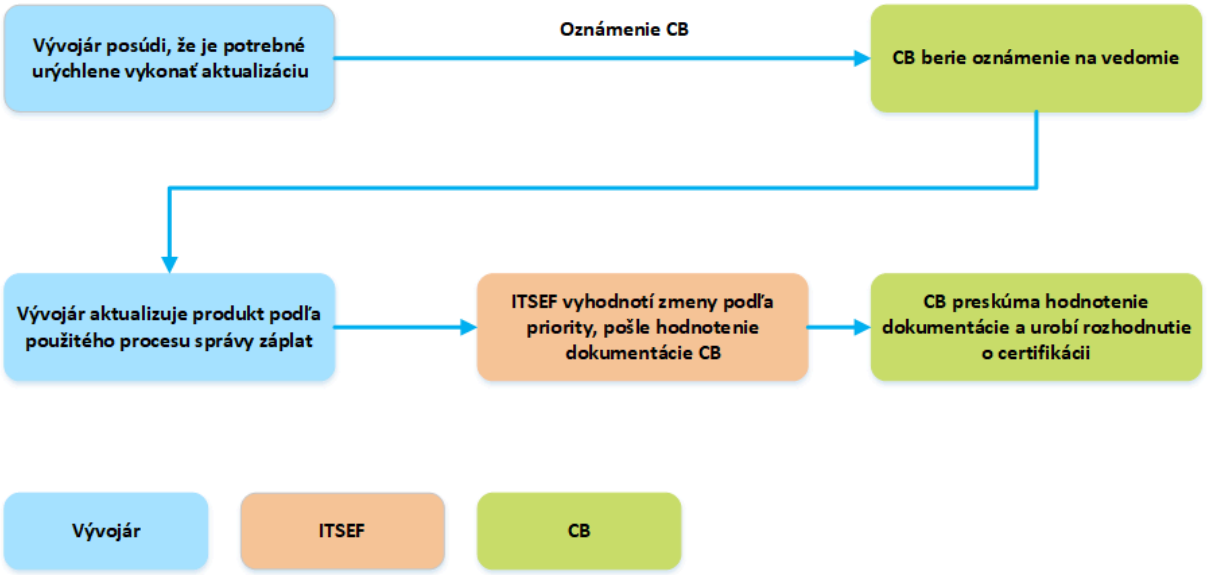
Na základe poskytnutej dokumentácie CB v prípade potreby rozhodne o aktualizácii verzie v certifikáte alebo prijme rozhodnutie na základe certifikačného procesu.

Dostupnosť opravy sa oznámi prostriedkami definovanými výrobcom alebo poskytovateľom produktu IKT, ktoré sú opísané v usmernení podľa článku 55 CSA. Používatelia produktu IKT musia byť zahrnutí medzi príjemcov informácií o možnosti záplaty certifikovaného TOE, ktoré výrobca alebo poskytovateľ produktu IKT

Produkt IKT chce zahrnúť do rozsahu certifikátu. Vo všetkých prípadoch, keď bol úspešne uplatnený opravný mechanizmus, sa vydá nový certifikát, ktorého platnosť nepresiahne platnosť pôvodného certifikovaného produktu IKT.

Poznámka: Systém správy záplat môže používať aj výrobca alebo poskytovateľ pre funkčné záplaty svojich produktov IKT. Platí to len za podmienky, že sa použije prístup záplaty 1. úrovne alebo že je spojený so záplatami zraniteľností a nemá priamy ani nepriamy vplyv na TSFI a tiež nemení bezpečnostné funkcionality spĺňajúce funkčné bezpečnostné požiadavky.

Obrázok 4: *Kritický aktualizačný tok*



3 USMERNENIA PRE PODÁVANIE ŽIADOSTÍ

Tabuľka 2: *Uplatniteľné činnosti úrovní záplat*

Akcie/úrovne záplat	Akcia 1	Akcia 2	Akcia 3	Komentár
Úroveň záplaty 1	Zmeny produktu v rámci úrovne záplat 1 sa vykonávajú na základe rozhodnutia výrobcu.	Výrobca informuje CAB do piatich pracovných dní o všetkých takto uplatnených zmenách.	CAB môže rozhodnúť o uplatnení výživného alebo iného príslušného rozhodnutia CB.	Zmeny produktu v rámci úrovne záplaty 1 sa vykonávajú na základe rozhodnutia výrobcu.
Úroveň záplaty 2	Výrobca vyvíja a testuje opravnú záplatu podľa použitého prijatého prístupu. (Nie je stanovená žiadna požadovaná lehota).	Pred opravou produktu sa ITSEF podrobí hodnoteniu. Toto je zdokumentované ITSEF. Časový limit pre hodnotenie sa môže dohodnúť medzi	Ak to výsledok hodnotenia umožňuje, výrobca môže produkt opraviť.	Na základe poskytnutej dokumentácie CB v prípade potreby rozhodne o aktualizácii verzie v certifikáte alebo prijme rozhodnutie na

Akcie/úrovne záplat	Akcia 1	Akcia 2	Akcia 3	Komentár
		zainteresovanými stranami procesu.		základe certifikačného procesu.
Úroveň záplaty 3	Príloha 11, KONTINUITA ZÁRUKY, pre významnú zmenu.			
Kritický aktualizačný tok	Výrobca/poskytovateľ vypracuje nápravnú záplatu (bez časového obmedzenia).	ITSEF a CB sú o zmenách informované do piatich pracovných dní a vykonajú potrebné hodnotiace a certifikačné činnosti. Žiadosť o záplatu nemusí čakať na výsledky certifikačného procesu.	ITSEF vyhodnotí už nasadenú záplatu s najvyššou prioritou, aby vyhodnotil zmeny a vytvoril príslušnú dokumentáciu vo vopred dohodnutom čase podľa dohody s výrobcom alebo poskytovateľom.	Na základe poskytnutej dokumentácie CB v prípade potreby rozhodne o aktualizácii verzie v certifikáte alebo prijme rozhodnutie na základe certifikačného procesu.

Prístup k správe záplat v rámci schémy EUCC sa môže uplatniť len vtedy, ak produkt IKT spĺňa príslušné požiadavky počas počiatočnej certifikácie. Patrí medzi ne ISCI WG1 "Návrh nových komponentov
a balíkov SAR v CC pre správu záplat" a technická správa ISO SC27 WG3 "Rozšírenie pre správu záplat pre 15408 a 18045". Ak produkt IKT nie je v súlade s jednou z nich, potom sa uplatňujú požiadavky na kontinuitu záruky definované v prílohe 11.

Cieľom oboch (2) prijatých procesov je zabezpečiť proces vývoja a nasadenia opráv.

Návrh pracovnej skupiny ISCI WG1 pre nové komponenty a balíky SAR v CC pre správu záplat má v úmysle použiť asynchrónny proces hodnotenia a certifikácie za predpokladu dôvery v už vyhodnotený vývoj a nasadenie záplat a poskytuje potrebné SAR a pracovné jednotky.

Technická správa ISO SC27 WG3 "Extension for Patch Management for 15408 and 18045" definuje stavebné bloky (t. j. SFR pre funkcionalitu záplat a jednu ďalšiu skupinu ALC), ktoré možno integrovať do PP a ST s cieľom poskytnúť dodatočnú bezpečnostnú záruku pre funkcionalitu záplat TOE a proces riadenia záplat vývojárom.

Všimnite si, že oba prístupy poskytujú potrebnú bezpečnostnú záruku na zvládnutie problémov s aktualizáciou certifikovaných produktov a môžu byť zvolené na použitie v ich poslednej platnej verzii. Návrh pracovnej skupiny ISCI WG1 bol vytvorený na použitie pre technickú doménu smart kariet a podobných zariadení. Technická správa ISO predstavuje všeobecnejší prístup. Oba sa môžu použiť na všetky produkty, ktorých cieľom je dosiahnuť významnú a vysokú úroveň záruky. Oba prístupy sú stále predmetom ďalších zlepšení.

Existujú štyri (4) prijateľné úrovne správy záplat: 1,2,3 a kritický aktualizačný tok.

Prístup k správe záplat v rámci schémy EUCC sa začína objavením predtým nezistenej zraniteľnosti v oblasti kybernetickej bezpečnosti týkajúcej sa certifikovaného produktu IKT.

Druhým krokom je potvrdenie, že výrobca alebo poskytovateľ vykoná analýzu produktu a oznámi CB dátum, kedy odpovie na otázku, či sa zraniteľnosť vzťahuje na produkt. Keď sa zraniteľnosť vyvráti, je potrebné uchovávať príslušnú dokumentáciu, ale proces sa končí. Analýza musí obsahovať aj overenie ITSEF a CB o výpočte potenciálu útoku, pričom sa zohľadní aj to, či sa predtým vypočítaný potenciál útoku zraniteľnosti odvtedy nezmenil.

Ak sa zraniteľnosť vzťahuje na certifikovaný produkt IKT, ďalším krokom je triedenie s cieľom zvážiť možné riziká a oprávnené úrovne záplat.

V procese triedenia sa zohľadňujú tieto opatrenia:

1. blízkosť alebo dostupnosť možného útoku;
2. úroveň zmeny, ktorú musí výrobca alebo poskytovateľ použiť na proces správy záplat. Zmeny menej významného a významného rozsahu sú úrovne definované v procese JIL AC.

Menej významné/významné úrovne zmien sa môžu ďalej spresniť pomocou príkladov počas počiatočnej certifikácie, aby sa urýchlil rozhodovací proces, ale toto spresnenie sa musí riadiť definíciami uvedenými v prílohe 11, KONTINUITA ZÁRUKY.

V prístupe k správe záplat EUCC sú dva (2) dodatky ku kontinuite záruky:

1. Opravy chýb sa tu považujú za typické menej významné zmeny;
2. zmeny v prostredí IKT, ktoré nemenia certifikované TOE, sa považujú za použiteľné na úrovni záplaty 1.

Tento zoznam by mali rozšíriť skupiny odborníkov zodpovedné za udržiavanie schémy EUCC.

Výrobca alebo poskytovateľ by mal zdokumentovať podrobnosti o zmenách a možných účinkoch použitia/nepoužitia záplat a zaslať tento dokument používateľom produktu, ako aj ITSEF a CB. Takto môžu používatelia certifikátu posúdiť možné riziká aj na základe údajov poskytnutých výrobcami alebo poskytovateľmi. Dobrou praxou môže byť aj zdokumentovanie posudzovania rizík pre používateľov, ITSEF a CB.

Výrobca sa dohodne s CB a ITSEF na podmienkach budúcich procesov správy záplat. Taktiež je potrebné poznamenať, že bez ohľadu na cestu, ktorú naznačila analýza, môže výrobca z akéhokoľvek dôvodu produkt nezáplatovať. Tabuľka identifikuje možný aplikovateľný postup pre každý prípad, ale nič nerobenie je vždy možnosťou (ktorá má dôsledky na ovplyvnené certifikáty, ako je uvedené v kapitole 13).

Asynchrónny prístup, ktorý možno opísať ako možnosť, že bezpečnostnú analýzu opravy posudzuje ITSEF a CAB po aplikácii alebo vydaní záplaty, sa má akceptovať len pre proces kritického toku aktualizácií. Pre ostatné úrovne sa uplatňuje:

- pri úrovni záplaty 1 je CB informovaná a môže uplatniť proces údržby, ak to považuje za potrebné;
- v úrovni záplaty 2 sa ITSEF vyhodnocuje synchrónne a CB je opäť informovaná a môže sa rozhodnúť, či aktualizuje verziu v certifikáte;
- v úrovni záplat 3 je proces plne synchrónny.

V budúcej aktualizácii schémy EUCC sa môže zvážiť širšie uplatňovanie asynchrónneho prístupu.

O AGENTÚRE ENISA

Poslaním Agentúry Európskej únie pre kybernetickú bezpečnosť (ENISA) je dosiahnuť vysokú spoločnú úroveň kybernetickej bezpečnosti v celej Únii aktívnou podporou členských štátov, inštitúcií, orgánov, úradov a agentúr Únie pri zlepšovaní kybernetickej bezpečnosti. Prispievame k tvorbe a implementácii politík, podporujeme budovanie kapacít a pripravenosť, uľahčujeme operačnú spoluprácu na úrovni Únie, zvyšujeme dôveryhodnosť produktov, služieb a procesov IKT zavádzaním systémov certifikácie kybernetickej bezpečnosti, umožňujeme výmenu poznatkov, výskum, inovácie a budovanie povedomia a zároveň rozvíjame cezhraničné komunity. Naším cieľom je posilniť dôveru v prepojené hospodárstvo, zvýšiť odolnosť infraštruktúry a služieb Únie a udržať našu spoločnosť v kybernetickej bezpečnosti.
Viac informácií o agentúre ENISA a jej práci nájdete na adrese www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu