CONFIRMATE

Posudzovanie zhody, metrika a automatizácia dodržiavania predpisov pre Nariadenie o kybernetickej odolnosti

Metodika Penetračného Testovania

Dátum vydania: 2025-09-04

Stav: Skontrolované

Verzia: 0.3.1

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Projekt financovaný na základe grantovej dohody **č. 101190193** je podporovaný Európskym centrom pre kybernetickú bezpečnosť. Názory a stanoviská vyjadrené v tomto dokumente sú však výlučne názormi autora(-ov) a nemusia odzrkadľovať názory Európskej únie alebo Európskeho centra pre kybernetickú bezpečnosť. Európska únia ani poskytovateľ grantu nenesú za ne žiadnu zodpovednosť.

Zoznam zmien

Verzia	Dátum	Popis	Autor(i)
0.1	21/03/25	Počiatočný návrh metodiky bol zaslaný partnerom na posúdenie a pripomienkovanie.	Cyen
0.2	08/04/25	Revízie zapracované na základe spätnej väzby od partnerov	Cyen
0.3	05/08/25	Revízie zapracované na základe spätnej väzby od kolegov	Cyen
0.3.1	04/09/25	Preklad do SVK	Motúz

Úprimne ďakujeme recenzentom, najmä Krasenovi Parvanovovi (QRTECH), Stijnovi Horemansovi (Refracted), Aymanovi Khalilovi a Romainovi Muguetovi (Red Alert Labs), Petrovi Kuzminovi (Kikimora) a Dominikovi Holzapfelovi (Nviso) za ich kritické postrehy a odbornú spätnú väzbu, čím významne prispeli ku kvalite, jednoznačnostii a zrozumiteľnosti tejto metodiky.

Preklad do slovenského jazyka Ľuboš Motúz.

Metodika penetračného testovania súladu s CRA pre malé a stredné podniky

Obsah

1. Referencie

- Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách na kybernetickú bezpečnosť produktov s digitálnymi prvkami a o zmene a doplnení nariadení (EÚ) č. 168/2013 a (EÚ) č. 2019/1020 a smernice (EÚ) 2020/1828 (Nariadenie o kybernetickej odolnosti), dostupný tu: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

- Inštitút pre bezpečnosť a otvorené metodiky (ISECOM). (2010). Manuál metodiky testovania bezpečnosti otvoreného zdrojového kódu (OSSTMM) verzia 3.0, dostupný tu: https://www.isecom.org/OSSTMM.3.pdf

- Penetration Testing Execution Standard (PTES) PTES Organization. (n.d.). Penetration Testing Execution Standard (PTES), dostupný tu:

  https://www.pentest-standard.org/index.php/Main_Page

- Scarfone, K., & Mell, P. (2008). Technická príručka pre testovanie a hodnotenie informačnej bezpečnosti (NIST SP 800-115), dostupná tu: https://csrc.nist.gov/pubs/sp/800/115/final

- OWASP Foundation. (n.d.). OWASP Web Security Testing Guide (WSTG), dostupné tu: https://owasp.org/www-project-web-security-testing-guide/

- MITRE Corporation. (n.d.). MITRE ATT&CK® Framework, dostupné tu: https://attack.mitre.org/

- Skupina pre bezpečnosť otvorených informačných systémov (OISSG). (2005). Rámec pre hodnotenie bezpečnosti informačných systémov (ISSAF) Návrh 0.2, dostupný tu: https://untrustednetwork.net/files/issaf0.2.1.pdf

- Etické červené tímy založené na informáciách o hrozbách (TIBER-EU) Európska centrálna banka. (2023). Rámec TIBER-EU: Etické červené tímy založené na informáciách o hrozbách, dostupné tu: https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

- ETSI TS 103 701 V1.1.1 (2021-08): Kybernetická bezpečnosť pre spotrebiteľský internet vecí: Posudzovanie zhody so základnými požiadavkami. Dostupné tu: https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf

2. Slovník pojmov: Skratky a pojmy

Skratky

OSSTMM:	**Príručka metodiky testovania bezpečnosti s otvoreným zdrojovým kódom**
OWASP:	**Projekt bezpečnosti otvorených webových aplikácií**
PTES:	**Štandard vykonávania penetračných testov**
NIST:	**Národný inštitút pre štandardy a technológie**
SIEM:	**Správa bezpečnostných informácií a udalostí**
IAM:	**Správa identít a prístupov (odvodené z kontextu)**
API:	**Rozhranie pre programovanie aplikácií**
VPN:	**Virtuálna súkromná sieť**
SSO:	**Jednotné prihlásenie**
IoT:	**Internet vecí**
GDPR:	**Všeobecné nariadenie o ochrane údajov**
ISO:	**Medzinárodná organizácia pre normalizáciu**
IEC:	**Medzinárodná elektrotechnická komisia**
CIS:	**Centrum pre internetovú bezpečnosť**
CMMC:	**Certifikácia modelu zrelosti kybernetickej bezpečnosti**
PSD2:	**Revidovaná smernica o platobných službách**
SWIFT CSP:	**Spoločnosť pre celosvetovú medzibankovú finančnú telekomunikáciu Program bezpečnosti zákazníkov**

Pojmy

Penetračné testovanie (alebo pen testovanie):	Bezpečnostné cvičenie, pri ktorom odborník na kybernetickú bezpečnosť snaží nájsť a využiť zraniteľné miesta v produkte a jeho prostredí, vrátane hardvéru, softvéru, rozhraní a povrchov interakcie s používateľom.
Zraniteľnosť:	Slabá stránka alebo chyba v systéme, aplikácii alebo sieti, ktorú možno využiť na ohrozenie bezpečnosti.
Zneužitie:	Kúsok kódu, technika alebo proces, ktorý využíva zraniteľnosť na spôsobenie nežiaduceho správania v systéme.
Hrozba:	Jednotlivec alebo skupina, ktorá predstavuje potenciálne riziko pre kybernetickú bezpečnosť organizácie, môže byť hacker, insider alebo konkurent.
Hodnotenie rizík:	Proces identifikácie rizík, ktoré by mohli negatívne ovplyvniť schopnosť organizácie vykonávať svoju činnosť.
Bezpečnostný audit:	Systematické hodnotenie bezpečnostného stavu produktu s digitálnymi prvkami, meranie jeho súladu s vopred definovanými technickými a regulačnými požiadavkami, ako je CRA.
Plán reakcie na incidenty:	Súbor pokynov, ktoré pomáhajú organizáciám detekovať, reagovať na incidenty v oblasti bezpečnosti počítačových sietí a obnovovať ich po incidente.
Šifrovanie:	Metóda, pomocou ktorej sa informácie prevádzajú na tajný kód, ktorý skryje ich skutočný význam.
Výrobca:	Fyzická alebo právnická osoba, ktorá vyvíja alebo vyrába produkty s digitálnymi prvkami alebo má produkty s digitálnymi prvkami navrhnuté, vyvinuté alebo vyrobené a uvádza ich na trh pod svojím menom alebo ochrannou známkou, či už za úhradu, za účelom zisku alebo bezplatne.
Viacfaktorová autentizácia (MFA):	Metóda autentizácie, ktorá vyžaduje, aby používateľ poskytol dva alebo viac overovacích faktorov, aby získal prístup k zdroju, ako je aplikácia, online účet alebo VPN.

Sociálne inžinierstvo:	Taktika manipulácie, ovplyvňovania alebo podvádzania obete s cieľom získať kontrolu nad počítačovým systémom alebo ukradnúť osobné a finančné informácie.
Taktiky, techniky a postupy (TTP):	Popisuje správanie aktéra hrozby a štruktúrovaný rámec na vykonanie kybernetického útoku.
CIA triáda (dôvernosť, integrita, dostupnosť):	Model informačnej bezpečnosti navrhnutý na ochranu citlivých informácií pred porušením bezpečnosti údajov.
Produkt s digitálnymi prvkami (PDE):	Produkt, ktorý obsahuje alebo je prepojený so softvérom alebo firmvérom a je schopný zhromažďovať, prenášať alebo spracúvať údaje. PDE zahŕňajú fyzické zariadenia aj softvérovo definované produkty, ktoré sú uvedené na trh alebo uvedené do prevádzky.

Preklady názvov dokumentov

Planning & Requirements Document (D1)	**Dokument plánovania a požiadaviek (D1)**
Pre-test Risk Assessment and Stakeholder Alignment (D2)	**Predbežné posúdenie rizík a zosúladenie zainteresovaných strán (D2)**
First version of Vulnerabilities Report (D3)	**Prvá verzia správy o zraniteľnosti (D3)**
Vulnerabilities Report (D3)	**Správa o zraniteľnosti (D3)**
Recommendations & Remediation Roadmap (D4)	**Odporúčania a plán nápravných opatrení (D4)**
Pentesting Report (D5)	**Správa o penetračných testoch (D5)**

3. Úvod

3.1 Účel a ciele

Tento dokument opisuje, ako spravovať a vykonávať penetračné testy produktov s digitálnymi prvkami (PDE) s cieľom podporiť overenie súladu s nariadením o kybernetickej odolnosti (CRA). Táto metodika vypĺňa praktickú medzeru tým, že definuje pracovný postup penetračného testovania v súlade s CRA, prispôsobený rizikovej expozícii na úrovni produktu, so zameraním na to, ako takéto testovanie podporuje vyhlásenie o zhode. Hoci CRA neodkazuje na penetračné testovanie ani ho nepredpisuje, naďalej zostáva jednou z najúčinnejších techník na určenie miery, do akej môže útočník potenciálne zraniteľnosti využiť. Úspešné vykonanie penetračného testovania môže preto posilniť dôkazovú základňu pre vyhlásenie o zhode.

Počas vývoja tejto metodiky bola pozornosť venovaná súboru produktov uvedených v prílohe A. Tieto produkty pokrývajú rôzne úrovne kritickosti definované v nariadení o kybernetickej odolnosti (CRA). Tieto produkty boli vybrané s cieľom zabezpečiť, aby bola metodika použiteľná a praktická v rôznych prípadoch použitia. Uvedené príklady produktov nás budú sprevádzať vo všetkých nástrojoch Confirmate.

Prístup je založený na uznávanej metodike (OSSTMM3), ktorá bola vyvinutá v otvorenej komunite a podrobená peer a interdisciplinárnemu preskúmaniu. OSSTMM3 ponúka štruktúrovaný prístup k identifikácii zraniteľností a ich priraďovaniu k možným kybernetickým útokom, čo umožňuje presnejšie posúdenie potenciálnych bezpečnostných rizík.

Ciele navrhovaného prístupu sú nasledovné:

- Poskytnúť štruktúrovanú metódu penetračného testovania produktov s digitálnymi prvkami a zároveň ponúknuť flexibilitu v používaných technikách.
- Definovať štandardný súbor výstupov, ktoré možno použiť na podporu tvrdenia výrobcu o súlade s CRA.
- Ilustrovať použitie prístupu vysvetlením, ako by sa dal uplatniť na viaceré produkty vybrané z dôležitých produktov (trieda I a trieda II) a kritických produktov podľa definície CRA.
- Táto metodika sa nevzťahuje na všeobecné hodnotenia podnikových IT systémov ani na samostatné penetračné testovanie webových aplikácií, ktoré nepredstavujú PDE podľa definície CRA. Metodiky Web-o a OWASP sa často

vzťahujú na aktíva, ktoré existujú iba na webe, čo nie je v súlade s produktovo orientovaným regulačným rozsahom požadovaným v tomto prípade.

3.2 Cieľová skupina

Cieľovou skupinou tohto dokumentu sú výrobcovia produktov s digitálnymi prvkami, ako sú definované v CRA.

4. Rozsah

4.1 Uplatniteľnosť na malé a stredné podniky

Prístup k penetračnému testovaniu navrhnutý v tomto dokumente je určený na použitie malými a strednými podnikani (MSP). Bolo vynaložené maximálne úsilie, aby bol tento prístup jednoduchý a ľahko zrozumiteľný a aby sa minimalizoval zbytočný žargón, aby navrhované metódy boli dostupné aj pre menšie spoločnosti.

Táto metodika je použiteľná na samostatné aj integrované digitálne produkty v rámci CRA, vrátane spotrebiteľských zariadení, priemyselných regulátorov, inteligentných brán a komponentov kritických z hľadiska bezpečnosti. Hoci je primárne určená na testovanie pred uvedením na trh a počas prevádzky, môže sa použiť aj v skorších fázach vývoja na identifikáciu slabých miest v kybernetickej bezpečnosti pred uvedením produktu na trh.

4.2 Hranice a obmedzenia

Tento dokument opisuje, ako spravovať a vykonávať penetračné testy s cieľom podporiť vyhlásenie o zhode v kontexte požiadaviek CRA. Nezahŕňa stratégie nápravy, mitigácie, kontrolné opatrenia na zmiernenie rizík ani nápravné bezpečnostné opatrenia, ktoré môžu byť potrebné po zistení slabých miest počas testovania.

Na rozdiel od klasických penetračných testov, ktoré sú zamerané na prostredie, testy uvedené v tomto dokumente sú zamerané na produkt. To však má zmysel len vtedy, ak je produkt umiestnený vo vhodnom prostredí. V tomto zmysle bude prostredie používané na hosťovanie produktu počas testov hrať úlohu pri určovaní platnosti konečných výsledkov. Penetračné testovanie v tomto kontexte sa zvyčajne vykonáva v kontrolovanom laboratórnom prostredí. Testovací tím by mal buď zabezpečiť alebo schváliť testovacie prostredie a zabezpečiť, aby odrážalo reálne prevádzkové podmienky bez oslabenia bezpečnostných predpokladov.

4.3 Predpoklady a obmedzenia

Hlavné predpoklady použité v prezentovanom prístupe sú nasledovné:

- Produkt bude testovaný v „laboratórnych podmienkach“ a nie v teréne.
- Prostredie, v ktorom bude produkt testovaný, bude čo najviac zodpovedať cieľovému prostrediu (t. j. prostredia, v ktorom bude produkt používaný).

Hoci sa v tomto prístupe navrhujú príkladové testovacie scenáre, predpokladá sa, že výrobcovia tieto scenáre prispôsobia tak, aby odrážali povahu testovaného produktu.

Obmedzenia procesu budú identifikované v rámci činností fázy 1. Hlavným obmedzením je, že testy by mali byť navrhnuté tak, aby nemali negatívny vplyv na činnosť testovacej organizácie.

5. Priemyselné normy pre testovanie

5.1 ETSI EN 303 645

Norma je doplnená špecifikáciou skúšok (TS 103 701) a implementačnou príručkou (TR 103 621)
https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf.

ETSI TS 103 701 poskytuje štruktúrované testovacie skupiny a posudzovanie zhody prispôsobené spotrebiteľským zariadeniam IoT. Testovacie prípady zahŕňajú funkčné požiadavky, požiadavky na odolnosť, rozhranie a ochranu údajov. V tejto metodike sa relevantné testovacie skupiny z TS 103 701 selektívne uplatňujú na kategórie produktov uvedené v prílohe A.

ETSI EN 303 645 je základná európska norma pre kybernetickú bezpečnosť spotrebiteľských zariadení internetu vecí (IoT). Stanovuje ustanovenia na riešenie najbežnejších a najvplyvnejších vektorov útokov. Cieľom normy je zabezpečiť minimálnu základnú úroveň kybernetickej bezpečnosti a slúžiť ako referenčný dokument pre vnútroštátne predpisy a posudzovanie zhody.

5.2 OSSTMM3

Audit OSSTMM je presné meranie kybernetickej bezpečnosti na prevádzkovej úrovni, ktoré neobsahuje žiadne predpoklady ani neoficiálne dôkazy. Ako metodika je navrhnutá tak, aby bola konzistentná a opakovateľná. Ako projekt s otvoreným zdrojovým kódom umožňuje akémukoľvek testerovi kybernetickej bezpečnosti prispieť svojimi nápadmi na vykonávanie presnejších, realizovateľnejších a efektívnejších bezpečnostných testov. Ďalej umožňuje voľné šírenie informácií a duševného vlastníctva.

V porovnaní s normami založenými na dodržiavaní predpisov sa OSSTMM 3 zameriava na overovanie kybernetickej bezpečnosti v reálnom svete a to vo viacerých oblastiach, vrátane:

- **Dátové siete**: smerovače, brány firewall, SIEM, inteligentné meracie zariadenia a zariadenia IoT.
- **Telekomunikácie**: Bezpečnosť vzdialeného prístupu, konfigurácie VPN.

- **Bezdrôtová bezpečnosť**: Zraniteľnosti Wi-Fi, šifrovacie štandardy.

Zaviedol tiež hodnoty posudzovania rizík (RAV), ktoré umožňujú kybernetickо bezpečnostným tímom kvantifikovať kybernetickо bezpečnostné riziká a sledovať zraniteľnosti v čase, čím sa zlepšuje riadenie rizík a rozhodovanie.

5.3 Príručka testovania OWASP

Príručka OWASP Testing Guide je vyvíjaná v rámci projektu OWASP Testing Project organizácie Open Web Application Security Project (OWASP). Nie je to kompletná metodika pokrývajúca celý penetračný test, zameriava sa iba na základné fázy testovania kybernetickej bezpečnosti webových aplikácií.

Sprievodca obsahuje podrobnú diskusiu o hodnotení kybernetickej bezpečnosti webových aplikácií, ako aj o ich variáciách nasadzovania, vrátane konfigurácie webového servera. Postupuje podľa prístupu pentestovania typu black-box a komplexne popisuje „čo“ a „kedy“. Obsahuje aj niektoré pokyny týkajúce sa „ako“, hlavne vo forme zoznamu nástrojov, ktoré možno použiť v jednotlivých krokoch alebo úlohách.

5.4 PTES

Penetration Testing Execution Standard (PTES) je najnovšia metodika penetračného testovania. Bola vyvinutá tímom odborníkov v oblasti kybernetickej bezpečnosti s cieľom vyriešiť potrebu komplexného a aktuálneho štandardu v oblasti penetračného testovania.

Okrem usmerňovania odborníkov v oblasti kybernetickej bezpečnosti sa snaží informovať podniky o tom, čo môžu očakávať od penetračného testovania, a usmerňovať ich pri vymedzovaní rozsahu a rokovaní o úspešných projektoch. Pokrýva „čo“ a „kedy“, ale ide oveľa hlbšie do „ako“.

PTES sa skladá z dvoch hlavných častí, ktoré sa navzájom dopĺňajú. Pokyny pre penetračné testovanie opisujú hlavné časti a body penetračného testovania, zatiaľ čo technické pokyny sa zaoberajú konkrétnymi nástrojmi a technikami, ktoré sa majú použiť v jednotlivých krokoch.

5.5 NIST SP 800-15

NIST 800-115 s názvom „Technická príručka pre testovanie a hodnotenie informačnej bezpečnosti“ je publikácia vypracovaná s cieľom poskytnúť usmernenia a odporúčania pre vykonávanie hodnotení informačnej bezpečnosti s cieľom posúdiť stav kybernetickej bezpečnosti informačných systémov a sietí.

Jej cieľom je pomôcť organizáciám porozumieť rôznym typom hodnotení bezpečnosti, vybrať vhodné techniky hodnotenia a navrhnúť komplexné programy hodnotenia. Usmernenia možno uplatniť na viaceré organizácie, vrátane verejnej správy, organizácií súkromného sektora a vzdelávacích inštitúcií.

Ďalšie podrobnosti o iných metodikách pentestingu a ich porovnaní sú k dispozícii v prílohe D: Porovnanie metodík. Okrem toho sú v prílohe E uvedené ďalšie usmernenia v oblasti bezpečnosti a osvedčené postupy.

6. Primárna metodika

Príručka metodiky testovania kybernetickej bezpečnosti otvoreného zdrojového kódu (OSSTMM 3) je primárnou metodikou používanou v tomto prístupe k penetračnému testovaniu. Poskytuje návod pre dôkladné kyberneticko bezpečnostné testovanie, ktoré sa v tomto dokumente označuje ako audit OSSTMM.

Hoci OSSTMM 3 je primárnou metodikou, tento rámec penetračného testovania zahŕňa aj prvky z:

- **ETSI TS 103 701 –** Relevantné testovacie prípady z tejto normy na testovanie zhody sú začlenené do nášho procesu vykonávania testov, najmä pre IoT a spotrebiteľské PDE.
- **OWASP Testing Guide** – Testovacie prípady OWASP sme integrovali do fáz prieskumu a zneužitia pre webové aplikácie a API. To zahŕňa dodržiavanie usmernení OWASP na identifikáciu zraniteľností, ako sú SQL injection, cross-site scripting a nezabezpečené riadenie relácií.
- **PTES** (Penetration Testing Execution Standard) – PTES definuje štruktúrovaný životný cyklus zapojenia, ktorý sme integrovali do metodiky. Aby sme zabezpečili, že každá fáza má jasné ciele, výstupy a komunikačné protokoly, zosúladili sme fázy OSSTMM3 s PTES, čím sme dosiahli konzistentný a opakovateľný proces testovania.

NIST SP 800-115 – NIST SP 800-115 poskytuje solídny rámec pre testovanie kybernetickej bezpečnosti založené na rizikách. Fázy zneužitia a analýzy dopadu boli zosúladené s jeho smernicami, aby sa zabezpečila systematická identifikácia zraniteľností, komplexné hodnotenie rizík a podrobné podávanie správ.

7. Príprava na penetračné testovanie

Prečo testovať? CRA vyžaduje, aby PDE „vykonávalo účinné a pravidelné testy a kontroly kybernetickej bezpečnosti produktu s digitálnymi prvkami“ (príloha I, časť II, bod 3). Plánovanie a realizácia pravidelných hodnotení kybernetickej bezpečnosti zabezpečuje nepretržité monitorovanie a proaktívnu identifikáciu zraniteľných miest, čím sa zachová odolnosť voči novým hrozbám.

Kto bude testovať? V kontexte hodnotení v súlade s CRA má výber penetračného testera (alebo poskytovateľa) priamy vplyv na spoľahlivosť, reprodukovateľnosť a regulačnú relevantnosť výsledkov. MSP by mali vybrať pentesterov, ktorí preukážu nasledujúce:

- *Technická spôsobilosť*: Preukázané odborné znalosti v oblasti kybernetickej bezpečnosti produktov, vstavaných systémov, testovania firmvéru a analýzy zraniteľnosti softvéru. Poskytovatelia musia rozumieť rozdielom medzi testovaním produktov a tradičnými hodnoteniami podnikového prostredia.
- *Oboznámenosť s CRA*: Preukázateľná znalosť nariadenia o kybernetickej odolnosti, vrátane požiadaviek prílohy I časti I a II, a schopnosť vypracovať výstupy, ktoré podporujú vyhlásenia o zhode v kontexte požiadaviek CRA.
- *Odborná skúsenosť v danom sektore*: Ak je to relevantné, vyberte poskytovateľov s skúsenosťami v danej oblasti produktu.
- *Právne a etické záruky*: Overte, či testeri dodržiavajú jasné etické zásady, poskytujú poistné krytie a uzatvárajú dobre vymedzené právne zmluvy, vrátane ustanovení o zodpovednosti a spracovaní osobných údajov.
- *Certifikácie a akreditácie*: Užitočné sú certifikácie ako OSCP, OSCE, CREST alebo rovnocenné národné osvedčenia na európskej úrovni. V prípade vysoko rizikových alebo kritických produktov zvážte certifikáciu TIBER-EU alebo Red Team.

Ako dlho to potrvá? Časový harmonogram sa môže líšiť v závislosti od zložitosti produktu, úrovne znalostí (black/grey/white box) a klasifikácie CRA (štandardná, dôležitá alebo kritická), ale všeobecný odhad času potrebného na každú fázu možno zhrnúť takto:

1. Príprava (5–10 pracovných dní, *spolupráca testera a výrobcu*), vrátane:

- Definovanie rozsahu, cieľov a hraníc testovania
- Mapovanie požiadaviek CRA prílohy I
- Právne dohody a zosúladenie zainteresovaných strán
- Klient poskytuje technickú dokumentáciu

2. Vykonanie testovania a podávanie správ (3–10 pracovných dní, *vedené testerom*), vrátane:

- Získavanie informácií, ich využitie a analýza vplyvu
- Testovanie firmvéru produktu, rozhraní, API a bezpečnostných kontrol
- Príprava správy a komunikácia

3. Náprava (1–4 týždne, *vedená výrobcom*)

- Vývoj opravných záplat, opravy konfigurácie, interná kontrola kvality
- Voliteľné prijatie rizika a aktualizácia dokumentácie

4. Opätovné testovanie (1–2 pracovné dni, *spolupráca testera a výrobcu*)

- Opätovné overenie vyriešených problémov
- Konečné technické potvrdenia a zhromažďovanie dôkazov

8. Metodika penetračného testovania

8.1 Predbežné zapojenie a plánovanie

Prvým krokom je definovanie typu testu, ktorý je najvhodnejší, s ohľadom na fázu vývoja produktu, identifikované bezpečnostné riziká produktu (interné/externé), dostupnú dokumentáciu a možné vektory útoku (ako môže byť produkt zneužitý). Testovanie môže byť:

- **Black-box**: Testeri nemajú žiadne interné znalosti; simulujú externého útočníka.
- **Grey-box**: Testeri majú čiastočné znalosti. Často vedú čiastočný prístup.
- **White-box**: Úplné interné znalosti (zdrojový kód, architektúra); umožňuje hlboké testovanie.

Upozorňujeme, že laboratórne testovanie predpokladá čiastočné alebo úplné znalosti (white-box).

Vstupy:

- *Identifikácia produktu*. Pre testovanie white-box a grey-box: bude potrebná technická dokumentácia, vrátane: prípadov použitia v prevádzke, diagramov architektúry, verzie firmvéru/softvéru, zoznamu rozhraní – interných a externých (napr. USB, BLE, API, webové rozhranie, porty, protokoly) alebo akýchkoľvek známych aktív/komponentov relevantných pre testovanie, modelu hrozieb (ak je k dispozícii). Ďalej môžu byť užitočné podrobnosti o predchádzajúcich hodnoteniach alebo auditoch (ak sú k dispozícii), vrátane otvorených hlásení chýb alebo nevyriešených zistení z testovania.
- Odvetvové rámce (napr. OSSTMM3, PTES, NIST SP 800-115, OWASP)
- Regulačné požiadavky a dokumentácia o súlade, vrátane požiadaviek CRA prílohy I, časti I a II (pozri prílohu B: Požiadavky CRA)
- Kontaktné miesta a núdzové protokoly, vrátane postupu pre nepredvídané situácie (čo robiť v prípade neočakávaných udalostí, ako napr. prerušenie služby) počas testovania.
- Zmluvná dokumentácia (ak sa používajú externí testeri): Zmluvy o poskytovaní služieb, dohody o mlčanlivosti, povolenia na testovanie a vyhlásenia o zrieknutí sa zodpovednosti.

Činnosti:

- *Definícia cieľov a stanovenie rozsahu*: Táto fáza začína jasne definovanými cieľmi a rozsahom. Zameriava sa na zabezpečenie toho, aby každý systém bol testovaný na svoje jedinečné funkcie. Vymedzenie rozsahu je kľúčové pre zosúladenie penetračného testovania s cieľmi CRA a jedinečnými vlastnosťami testovaného produktu. Vymedzenie rozsahu zahŕňa:
    - *Definícia hraníc produktu*: Definujte technický rozsah (softvér, hardvér, API, rozhrania) produktu s digitálnymi prvkami (PDE).
    - *Mapovanie CRA*: Na základe rizikovej triedy produktu identifikujte, ktoré požiadavky prílohy I CRA sa uplatňujú.
    - *Vstupné údaje pre modelovanie hrozieb*: Zahrnutie známych aktérov hrozieb, útočných plôch a kontextu produktu.
- *Hĺbka testovania: Hĺbka penetračného testovania by mala zodpovedať klasifikácii kritickosti produktu podľa zákona o kybernetickej odolnosti (CRA).*
    - *Testovanie produktov triedy I Dôležité*
    - *Dôležité produkty triedy II* vyžadujú dôkladnejšiu kontrolu firmvéru, mechanizmov aktualizácie, komunikácie medzi zariadením a cloudom, autentifikačných tokov a scenárov zneužitia protokolu.
    - *Kritické testovanie produktov* by malo zahŕňať overenie bezpečnosti na úrovni hardvéru, ako je detekcia manipulácie, odolnosť proti vstrekovaniu chýb a overenie bezpečného spustenia.
- *Právne, regulačné a etické hľadiská*: Testovanie sa vykonáva v súlade s právnymi a regulačnými požiadavkami (napr. ochrana súkromia, ochrana údajov, zákony o duševnom vlastníctve) a internými politikami. Všetky požadované povolenia sú zabezpečené a obmedzenia sú zdokumentované tak, aby testovacie prostredie nemalo vplyv na prevádzku výroby. (pozri prílohu B: Požiadavky CRA, príloha CRA I, časť I, body 1, 2 b), 2 g), 2 j) a príloha I, časť II, bod 1.)
- *Zriadenie testovacej laboratórie*, ktorá napodobňuje prevádzkové prostredie PDE.

Výstupy poskytované v rámci nasledujúcich fáz:

- Dokument o metodike na vysokej úrovni
- Formuláre právnych povolení
- Vymedzenie rozsahu
- Usmernenia pre zapojenie
- Správa o posúdení rizík produktu
- Informovanie zainteresovaných strán

Konečné výstupy:

- Dokument o plánovaní a požiadavkách (D1): Podrobný plán projektu penetračného testovania, v ktorom sa uvádza rozsah, úlohy, ciele, povolenia, harmonogram a nastavenie laboratória.
- Predbežné posúdenie rizík a zosúladenie zainteresovaných strán (D2): Pred začatím testovania je potrebné vykonať posúdenie rizík špecifických pre daný produkt s cieľom identifikovať akékoľvek potenciálne riziká, ktoré by penetračné testovanie mohlo predstavovať pre funkčnosť, integritu údajov alebo dostupnosť produktu. To zahŕňa posúdenie toho, ako by testovanie mohlo ovplyvniť kritické rozhrania, služby a údaje spracúvané produktom. Zainteresované strany sú informované a plán penetračného testovania musí byť zosúladený s ich kybernetico bezpečnostnými požiadavkami (vrátane prílohy B: Požiadavky CRA, príloha I časti I CRA) a toleranciou rizika.

8.2 Získavanie spravodajských informácií a prieskum

Vstupy:

- Definícia rozsahu
- Správa o posúdení rizík produktu

Činnosti:

- Otvorené zdroje informácií a zistenie aktív: V tejto fáze sa používajú otvorené zdroje informácií na zhromaždenie čo najrozsiahlejších informácií. Zahŕňa mapovanie digitálnej stopy každého produktu a prvku.
- Profilovanie cieľov a analýza hrozbového prostredia: Na určenie potenciálnych zraniteľností je potrebná analýza každého aktíva. Preskúma sa aj hrozbové prostredie, aby sa zabezpečilo, že pri penetračnom testovaní sa použijú realistické scenáre a taktiky protivníka sa odzrkadlia v simulovaných útokoch počas testovania.
- Vypracovanie scenárov na základe správania protivníka: Na základe zhromaždených informácií a údajov sa formulujú konkrétne scenáre útokov.

Výstupy do nasledujúcich fáz:

- Scenáre správania protivníka a profily cieľov
- Prvá verzia správy o zraniteľnosti (D3): Podrobné zistenia z externých aj interných hodnotení produktu, vrátane hodnotenia rizík, možnosti zneužitia a

návrhov nápravných opatrení, ktoré poskytujú komplexný prehľad o zraniteľnosti samotného produktu.

Konečné výstupy:

- V tejto fáze nie sú finalizované žiadne výstupy.

8.3 Testovanie vykonávania a zneužitia

Vstupy:

- Prvá verzia správy o zraniteľnosti (D3): Podrobné zistenia z externých aj interných hodnotení produktu, vrátane hodnotenia rizík, možnosti zneužitia a návrhov na nápravu, ktoré poskytujú komplexný prehľad o zraniteľnosti samotného produktu.
- Scenáre správania protivníka a profily cieľov
- Testovacie nástroje (napr. Nessus, Metasploit, Wireshark). Príklady testovacích nástrojov a rámcov sú uvedené v prílohe E.
- (ak je k dispozícii) zdrojový kód softvéru.

Činnosti:

- Identifikácia zraniteľností a simulácia útoku: Zraniteľnosti sa identifikujú pomocou techník, ako je statická (SAST) a dynamická analýza bezpečnosti aplikácií (DAST) alebo manuálna kontrola kódu, ak je to vhodné. Na zvýšenie efektívnosti detekcie zraniteľností sa môže použiť umelá inteligencia založená na analýze hrozieb. Každý produkt sa testuje v súlade s ustanovenými normami. Činnosti posudzovania zraniteľnosti sa vykonávajú opakovane počas celého testovania a priamo sa zapracúvajú do správy o zraniteľnosti D4 a slúžia ako primárny základ pre neskoršie hodnotenie rizík. Vybrané testovacie scenáre, ktoré pochádzajú z ETSI TS 103701, sú uvedené v prílohe C, pretože by sa mohli spustiť ako súčasť penetračného testovania, ktoré by okrem bezpečnosti testovalo aj súlad s CRA. Činnosti počas tejto fázy tiež overujú požiadavky na bezpečný dizajn a ochranu v súlade s CRA. Pozri prílohu B: CRA príloha I, časť I, body 2(a), 2(b), 2(d), 2(e), 2(j), 2(k) a príloha I, časť II, bod 3.
- Techniky zneužitia a emulácia protivníka: Overovanie chýb pokusom o ich zneužitie v kontrolovanom prostredí. Ak sú k dispozícii nástroje, možno použiť skenovanie s podporou umelej inteligencie. Malé a stredné podniky, ktoré nemajú k dispozícii takéto nástroje, sa môžu spoľahnúť na ručnú kontrolu alebo

jednoduchšiu automatizáciu. Príkladmi sú detekcia anomálií v protokoloch alebo fuzzing založený na strojovom učení. Okrem toho sa posudzujú situácie, v ktorých by protivníci mohli obísť bezpečnostné opatrenia a získať neoprávnený prístup.

- Analýza po zneužití: Posúdenie vplyvu úspešného útoku, vrátane eskalácie privilégií v systéme a potenciálneho laterálneho pohybu k iným používateľom, komponentom alebo pripojeným systémom. To zahŕňa určenie, či útočník môže získať prístup k citlivým údajom, pohybovať sa medzi aplikačnými modulmi alebo segmentmi infraštruktúry alebo ohroziť kritické služby. Podrobnosti o funkčnom vplyve sa zhromažďujú analýzou potenciálnych dôsledkov každej zneužitých zraniteľnosti.
- Výsledky testovacích prípadov sú zahrnuté v konečných výstupoch tejto fázy, aby bolo možné sledovať testovacie aktivity v porovnaní s očakávaným správaním.

Výstupy do nasledujúcich fáz:

- Zoznam zraniteľností
- Dôkazy o zneužití (proof-of-concept)
- Predbežné hodnotenie rizík
- Správa o realizovateľnosti zneužitia
- Správa o simulácii taktík protivníka

Konečné výstupy:

- Správa o zraniteľnostiach (D3): Podrobné zistenia z externých aj interných hodnotení produktu, vrátane hodnotenia rizík, realizovateľnosti zneužitia a návrhov na nápravu, ktoré poskytujú komplexný prehľad o zraniteľnostiach ovplyvňujúcich samotný produkt.

8.4 Analýza vplyvu a podávanie správ

Vstupy:

- Zoznam zraniteľností
- Dôkazy o zneužití (dôkaz koncepcie)
- Predbežné hodnotenie rizík
- Štandardy hodnotenia rizík špecifické pre dané odvetvie
- Politiky klasifikácie údajov.

Činnosti:

- Hodnotenie rizík a posudzovanie funkčného vplyvu: Analýza závažnosti identifikovaných zraniteľností, meranie ich vplyvu na CIA (dôvernosť, integrita alebo dostupnosť). Priradenie rizikového ratingu na stanovenie priorít nápravných opatrení. Na zlepšenie celkovej fázy hodnotenia možno použiť aj modely hodnotenia rizík založené na umelej inteligencii, ktoré priraďujú úrovne rizík na základe informácií o hrozbách v reálnom čase a údajov o zneužívaní. Zahŕňa to hodnotenie integrity údajov, odolnosti a reakcie na zraniteľnosti v súlade s CRA. Pozri prílohu B: CRA príloha I, časť I, body 2 písm. e), 2 písm. f), 2 písm. i); príloha I, časť II, body 1, 2.
- Dokumentácia zistení a zhromažďovanie dôkazov: Zostavenie podrobných správ obsahujúcich popisy zraniteľnosti, technické dôkazy a dôkazy o zneužití. Zabezpečenie, aby zainteresované strany mali jasnú predstavu o kybernetícko bezpečnostných medzerách.
- Označenie súladu s regulačnými požiadavkami: Preložte výsledky testovania do pojmov súladu s regulačnými požiadavkami označením zistení, ktoré súvisia s požiadavkami CRA prílohy I a II uvedenými v prílohe B. Týmto spôsobom prispievate k správe o súlade s regulačnými požiadavkami, ktorú možno použiť na odôvodnenie vyhlásenia výrobcu o zhode.
- Odporúčania a realizovateľné stratégie nápravy: Poskytovanie podrobných usmernení na zmiernenie zistených rizík. Navrhovanie kybernetícko bezpečnostných kontrol, zmien konfigurácie a stratégií opravných záplat na zvýšenie odolnosti systému. Pozri prílohu B: Požiadavky CRA

Výstupy do nasledujúcich fáz:

- Správa o hodnotení rizík
- Komplexný dokument s nálezmi
- Podrobnosti o funkčnom vplyve
- Odporúčania na nápravu
- Plán nápravných opatrení podľa priority
- Správa o zosúladení s regulačnými požiadavkami

Konečné výstupy:

- Odporúčania a plán nápravných opatrení (D5): Odporúčania podľa priority s jasným plánom nápravných opatrení, vrátane krátkodobých, strednodobých a dlhodobých opatrení.

8.5 Post-angažovanosť Follow-Up

Vstupy:

- Správy o nápravných opatreniach
- Aktualizované konfigurácie systému a výsledky opätovného testovania.

Činnosti:

Overenie nápravných opatrení a opätovné testovanie: Opätovné testovanie s cieľom overiť, či boli kyberneticko bezpečnostné chyby odstránené. Zabezpečenie, aby nápravné opatrenia účinne odstránili zraniteľnosti. Činnosti po testovaní potvrdzujú súlad s očakávaniami CRA v oblasti bezpečnostných aktualizácií a zverejňovania.

- Pozri prílohu B: CRA príloha I, časť I, body 2(h), 2(m) a príloha I, časť II, body 2, 4, 7, 8.
- Neustále zlepšovanie a integrácia získaných skúseností: Aktualizácia testovacích metodík a bezpečnostných politík na základe zistení. Analytika založená na umelej inteligencii pomáha zlepšovať budúce hodnotenia kybernetickej bezpečnosti využívaním skúseností získaných z predchádzajúcich testov. (pozri: príloha: Požiadavky CRA, príloha CRA I, časť I)
- Zverejňovanie a oznamovanie zraniteľností: Po sprístupnení kyberneticko bezpečnostných aktualizácií musia výrobcovia pripraviť a zverejniť podrobnosti o odstránených zraniteľnostiach. V prípadoch, keď by zverejnenie predstavovalo neprimerané riziko, môže byť zverejnenie odôvodnene odložené, kým nebudú široko nasadené opravy (príloha CRA I, časť II, bod 4).

Konečné výstupy:

- Správa o penetračnom testovaní (D5): Typická správa o penetračnom testovaní obsahuje súhrn (všeobecný prehľad, celkové hodnotenie rizika, výsledky testov a odporúčania podľa priority), rozsah a metódu testovania (D1), činnosti, zistenia (s ďalšími podrobnosťami, vrátane zraniteľností (D2) a dôkazov o zneužití) a odporúčania (D4). Tento dokument možno považovať za „preskúmanie bezpečnosti produktu s digitálnymi prvkami“ na účely požiadavky CRA uvedenej v prílohe I časti II bode 3 (Uplatňovať účinné a pravidelné testy a preskúmania kybernetickej bezpečnosti produktu s digitálnymi prvkami).

8.6 Výstupy

Každá úloha bude mať za výsledok komplexný súbor výstupov určených na riešenie technických aj strategických potrieb. Pre každú fázu metodiky budú výstupy jedného z dvoch typov: (a) výstupy, ktoré sa použijú ako vstupy do nasledujúcej fázy, a (b) výstupy celého cvičenia. Výstupy celého cvičenia sú uvedené nižšie.

- Dokument plánovania a požiadaviek (D1): Podrobný plán projektu penetračného testovania, v ktorom sú uvedené ciele, rozsah, úlohy, postupy v prípade nepredvídaných okolností, autorizácia, harmonogram a nastavenie laboratória.
- Predbežné posúdenie rizík a zosúladenie zainteresovaných strán (D2): Dôkladná analýza potenciálnych rizík pred začatím testovania, ktorá zabezpečí zosúladenie s zainteresovanými stranami, pokiaľ ide o rozsah, priority a ciele.
- Správa o zraniteľnosti (D3): Podrobné zistenia z externých aj interných hodnotení produktu, vrátane hodnotenia rizík, možnosti zneužitia a návrhov nápravných opatrení, ktoré poskytujú komplexný prehľad zraniteľnosti ovplyvňujúcej samotný produkt.
- Odporúčania a plán nápravných opatrení (D4): Prioritizované odporúčania s jasným plánom nápravných opatrení, vrátane krátkodobých, strednodobých a dlhodobých opatrení.
- Správa o penetračných testoch (D5): Všeobecný prehľad pre technicky neznalé zainteresované strany, ktorý sumarizuje kľúčové zistenia a strategické odporúčania.

8.7 Príkladové scenáre

Účelom tejto časti je poskytnúť ilustratívne príklady scenárov penetračných testov, vrátane približných požiadaviek na zdroje a pravdepodobného časového harmonogramu. Tieto scenáre majú iba informatívny charakter a môžu sa výrazne líšiť v závislosti od konkrétneho cvičenia.

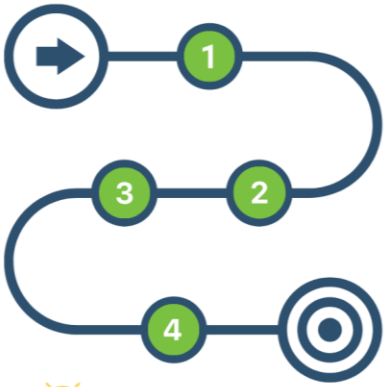
Scenár 1: Správa identít a prístupu (dôležitý produkt CRA: trieda I)

Testovací prístup

- **Typ testovania:** Sivý rámček (Boli poskytnuté základné prihlasovacie údaje. Pentester musí vymenovať interné funkcie a privilégiá IAM).
- **Zložitosť:** Stredná (5–15 funkcií/modulov IAM).
- **Odhadovaná náročnosť:** 8 – 12 dní práce (uplynulo ~15 – 20 dní).

Zistenia a dopad

- Nesprávna manipulácia s reláciou odhalila tokeny relácie neoprávneným používateľom.
- Logika záložnej MFA umožňovala obísť proces pomocou metód sociálnej obnovy.
- Záznamy IAM neoznačili eskaláciu privilégií prostredníctvom manipulácie s rolami.



Odporúčania

- Implementujte tokeny zabezpečenej relácie s atribútmi HttpOnly, Secure a SameSite.
- Vynucujte prísne viacfaktorové overovacie postupy bez neoverenej záložnej metódy.
- Povoliť protokolovanie a upozornenia na pokusy o zvýšenie privilégií a zmeny rolí.

Cesta útoku

1. **Prieskum:** Vymenovať koncové body prihlásenia do IAM, mechanizmy MFA a logiku správy relácií.
2. **Zneužitie zraniteľnosti:** Obídenie záložnej MFA prostredníctvom sociálnej obnovy. Únos administrátorskej relácie prostredníctvom zberu tokenov.
3. **Analýza dopadu a reportovanie:** Identifikujte riziko neoprávneného prístupu k administračnému portálu a interným konfiguráciám.
4. **Následná činnosť:** Oprava logiky záložného MFA a prekonfigurovanie správy relácií.

Vplyv dodržiavania predpisov ratingových agentúr

Nezabezpečená záložná viacfaktorová autentifikácia porušuje prílohu I, časť I, bod 2(d) zákona CRA: "Zabezpečiť ochranu pred neoprávneným prístupom pomocou vhodných kontrolných mechanizmov."
Absencia protokolovania o zvýšení privilégií porušuje prílohu I, časť I, bod 2(l) zákona CRA: "Poskytovať informácie súvisiace s bezpečnosťou zaznamenávaním a monitorovaním relevantnej internej aktivity."

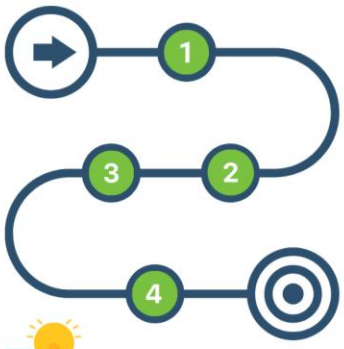
Scenár 2: Správa bezpečnostných informácií a udalostí (SIEM) (dôležitý produkt CRA: trieda II)

Testovací prístup

- **Typ testovania:** Sivý rámček (poskytnuté prihlasovacie údaje SIEM; pentester simuluje adverzárne vstupy a manipuláciu s protokolmi).
- **Zložitosť:** Vysoká (15 – 30 zdrojov protokolov, súborov pravidiel a integrácií).
- **Odhadovaná dĺžka práce:** 12 – 15 dní (uplynulo ~20 – 25 dní).

Zistenia a dopad

- *Systém SIEM nedokázal spustiť upozornenia pri opakovaných neúspešných pokusoch o prihlásenie.*
- *Vkladanie do syslogu umožňovalo skrytie záznamov o narušení.*
- *Kontroly integrity protokolov sa dali obísť vyhýbaním sa užitočnému zaťaženiu.*



Odporúčania

- *Nakonfigurujte pravidlá detekcie anomálií pre prahové hodnoty založené na autentifikácii.*
- *Vyčistite vstupy protokolov, aby ste zabránili ich vkladaniu do protokolov.*
- *Na zabezpečenie integrity použite kryptografické podpisovanie a overovanie protokolov.*

Cesta útoku

1. **Prieskum:** Skontrolujte body príjmu SIEM, pravidlá korelácie a prahové hodnoty upozornení.
2. **Zneužívanie zraniteľnosti:** Vkladanie upravených protokolov na skrytie skutočných útokov. Zneužívanie chýbajúcej korelácie udalostí pri neúspešných prihláseniach.
3. **Analýza vplyvu a reportovanie:** Vyhodnoťte, ako potlačenie upozornení umožňuje trvalý prístup.
4. **Následná činnosť:** Zlepšenie logiky parsovania a súborov pravidiel auditu.

Vplyv dodržiavania predpisov ratingových agentúr

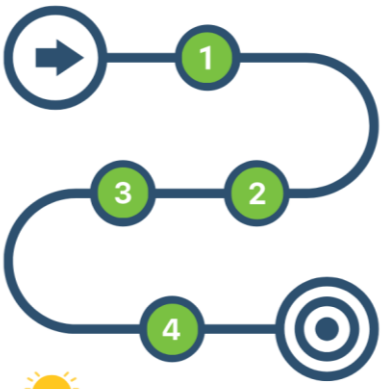
Manipulácia s protokolmi bez detekcie porušuje prílohu I, časť I, bod 2(l) zákona CRA: "Zaznamenávanie a monitorovanie relevantnej internej činnosti."

Obídenie upozornení pri opakovaných zlyhaniach prihlásenia. Porušenia CRA. Príloha I, časť I, bod 2(h): "Chrániť dostupnosť základných a základných funkcií… vrátane zmiernenia rizík proti útokom typu „donial-of-service"."

Scenár 3: Brána inteligentného meradla (kritický produkt CRA)

Testovací prístup

- **Typ testovania:** Sivá krabica (poskytnuté špecifikácie firmvéru a rozhrania; Pentester vykonáva testovanie protokolov a vstavaných modulov).
- **Zložitosť:** Vysoká (zložité vstavané systémy a proprietárne protokoly).
- **Odhadovaná náročnosť:** 15 – 20 dní práce (uplynulo ~25 – 30 dní).



Cesta útoku

1. **Prieskum:** Identifikácia koncových bodov aktualizácie firmvéru a komunikačných vzorcov.
2. **Zneužitie zraniteľnosti:** Opätovné použitie zachytenej prevádzky aktualizácií firmvéru. Nasadenie falošného firmvéru.
3. **Analýza vplyvu a podávanie správ:** Preukázanie úplného prevzatia logiky brány inteligentných meračov.
4. **Následné kroky:** Prepracovanie zabezpečeného bootovania s kryptografickým refazcom a možnosťou opakovaného prehrávania záplat.

Zistenia a dopad

- *Proces aktualizácie firmvéru akceptoval nepodpísané obrázky.*
- *Bezpečné overenie bootovania bolo obídené chybami bootloaderu.*
- *Útoky opakovaného prehrávania zachytené a odoslané späť platné šifrované komunikácie.*

Odporúčania

- *Vynútiť kontrolu digitálneho podpisu počas inštalácie firmvéru.*
- *Zvyšovať odolnosť bootloaderu na overenie kryptografických refazcov dôvery.*
- *Zahrňte jednorazové hodnoty a kontroly aktuálnosti na zmiernenie útokov opakovaného prehrávania.*

Vplyv dodržiavania predpisov ratingových agentúr

Chýbajúce overenie firmvéru porušuje prílohu I, časť I, bod 2(k) zákona CRA: "Znížte dopad incidentu pomocou vhodných techník zmierňovania zneužitia."

Útoky opakovaného prehrávania využívajúce komunikáciu firmvéru porušujú prílohu I, časť I, bod 2(e) zákona CRA: "Chráňte dôvernosť uložených alebo prenášaných údajov pomocou najmodernejších mechanizmov."

Príloha A: Výber zvažovaných PDE

Dôležité: Trieda I

- *Systémy správy identít*
- *Prehliadače*
- *Správcovia hesiel*
- *Softvér na vydávanie digitálnych certifikátov*
- *Routre*
- *Produkty pre inteligentné domácnosti*
- *Nosiče na monitorovanie zdravia*
- *Systémy SIEM*

Dôležité: Trieda II

- *Firewally*

Kritické produkty

- *Brána pre inteligentné meracie zariadenia*

Príloha B: Požiadavky CRA

1. Príloha I časť I – Základné požiadavky na kybernetickú bezpečnosť

Požiadavka CRA	Odkaz na požiadavku CRA
Produkty s digitálnymi prvkami sa navrhujú, vyvíjajú a vyrábajú tak, aby sa zaistila primeraná úroveň ich kybernetickej bezpečnosti voči rizikám	Prílohy I Časť I Bod 1
Produkty s digitálnymi prvkami sa na základe posúdenia kybernetickobezoečnostných rizík uvedeného v článku 13 ods. 2 a podľa potreby: a) sprístupňujú na trh bez známych zneužiteľných zraniteľností	Prílohy I Časť I Bod 2(a)
b) sprístupňujú na trhu v konfigurácii zabezpečenej na úrovni štandardného nastavenia, pokiaľ sa výrobca a komerčný používateľ v súvislosti s individualizovaným produktom s digitálnymi prvkami nedohodnú inak, vrátane možnosti vrátiť nastavenie produktu na pôvodné	Prílohy I Časť I Bod 2(b)
c) zaisťujú, aby zraniteľnosti bolo možné riešiť bezpečnostnými aktualizáciami, prípadne aj automatickými bezpečnostnými aktualizáciami, ktoré sa inštalujú v primeranom čase aktiváciou podľa predvoleného nastavenia, s jasnou a ľahko použiteľnou možnosťou pre používateľa odmietnuť ich po oznámení o dostupných aktualizáciách a možnosti ich dočasného odkladu	Prílohy I Časť I Bod 2(c)

(d) zabezpečujú ochranu pred neoprávneným prístupom vhodnými mechanizmami kontroly, a to okrem iného aj systémami na správu overovania, identity alebo prístupu, a oznamujú, že došlo k možnému neoprávnenému prístupu	Prílohy I Časť I Bod 2(d)
(e) chránia dôvernosť uložených, vysielaných alebo inak spracúvaných osobných alebo iných údajov, napríklad šifrovaním príslušných neaktívnych alebo prenášaných údajov najmodernejšími mechanizmami, a použitím iných technických prostriedkov	Prílohy I Časť I Bod 2(e)
(f) chránia integritu uložených, vysielaných alebo inak spracúvaných osobných alebo iných údajov, príkazov, programov a konfigurácie proti akejkoľvek manipulácii alebo úprave, ktorú neschválil používateľ, a oznamujú prípady poškodenia	Prílohy I Časť I Bod 2(f)
(g) spracúvajú iba osobné alebo iné údaje, ktoré sú primerané, relevantné a obmedzené na to, čo je potrebné vo vzťahu k účelu produktu s digitálnymi prvkami (minimalizácia údajov), na ktorý bol určený	Prílohy I Časť I Bod 2(g)
(h) chránia dostupnosť hlavných a základných funkcií aj po incidente, a to aj prostredníctvom opatrení na zvýšenie odolnosti a zmiernenie útokov na vyradenie služby	Prílohy I Časť I Bod 2(h)
(i) minimalizujú nepriaznivý vplyv samotných produktov alebo pripojených zariadení na dostupnosť služieb iných zariadení alebo sietí	Prílohy I Časť I Bod 2(i)
(j) navrhujú, vyvíjajú a vyrábajú na obmedzenie plochy útoku vrátane externých rozhraní	Prílohy I Časť I Bod 2(j)
(k) navrhujú, vyvíjajú a vyrábajú na obmedzenie vplyvu incidentu s využitím vhodných mechanizmov a techník na zmiernenie zneužitia zraniteľností	Prílohy I Časť I Bod 2(k)

(l) poskytujú bezpečnostné informácie zaznamenávaním a monitorovaním príslušnej internej činnosti vrátane prístupu k údajom, službám alebo funkciám a ich zmene s mechanizmom odmietnutia (opt-out) pre používateľa	Prílohy I Časť I Bod 2(l)
(m) poskytujú používateľom možnosť bezpečne a jednoducho natrvalo odstrániť všetky údaje a nastavenia a ak takéto údaje možno preniesť do iných produktov alebo systémov, zabezpečiť, aby sa tak dialo bezpečne.	Prílohy I Časť I Bod 2

2. Príloha I časť II – Požiadavky na riešenie zraniteľností

Výrobcovia produktov s digitálnymi prvkami:

Požiadavka CRA	CRA Citation
identifikujú a dokumentujú zraniteľnosti a komponenty v produktoch s digitálnymi prvkami, a to aj zostavením zoznamu softvéru v obvykle používanom strojovo čitateľnom formáte, ktorý obsahuje závislosti produktu minimálne na najvyššej úrovni;	Prílohy I Časť II Bod 1
vo vzťahu k rizikám, ktorým sú vystavené produkty s digitálnymi prvkami, bezodkladne riešia a naprávajú zraniteľnosti, a to aj poskytovaním bezpečnostných aktualizácií; ak je to technicky možné, nové bezpečnostné aktualizácie sa poskytujú oddelene od aktualizácií funkcií;	Prílohy I Časť II Bod 2
vo vzťahu k rizikám, ktorým sú vystavené produkty s digitálnymi prvkami, bezodkladne riešia a naprávajú zraniteľnosti, a to aj poskytovaním bezpečnostných aktualizácií; ak je to technicky možné, nové bezpečnostné aktualizácie sa poskytujú oddelene od aktualizácií funkcií;	Prílohy I Časť II Bod 3
po sprístupnení bezpečnostnej aktualizácie poskytujú a zverejňujú informácie o opravených zraniteľnostiach vrátane opisu zraniteľností, informácie umožňujúce používateľom identifikovať postihnutý produkt s digitálnymi prvkami, vplyvy zraniteľností, ich závažnosť a jasné a prístupné informácie,	Prílohy I Časť II Bod 4

ktoré používateľom pomôžu zraniteľnosti napraviť; keď sa výrobcovia domnievajú, že bezpečnostné riziká zverejnenia prevažujú nad bezpečnostnými prínosmi, v riadne odôvodnených prípadoch môžu odložiť zverejnenie informácií o vyriešenej zraniteľnosti dovtedy, kým používateľom neposkytnú možnosť použiť príslušnú záplatu;	
zavádzajú a presadzujú politiku koordinovaného zverejňovania informácií o zraniteľnostiach;	Prílohy I Časť II Bod 5
prijímajú opatrenia na uľahčenie výmeny informácií o potenciálnych zraniteľnostiach svojho produktu s digitálnymi prvkami, ako aj komponentov tretích strán vo svojom produkte, a to aj poskytnutím kontaktnej adresy na oznamovanie zraniteľností zistených v produkte s digitálnymi prvkami;	Prílohy I Časť II Bod 6
zaistia mechanizmy bezpečnej distribúcie aktualizácií pre produkty s digitálnymi prvkami s cieľom zabezpečiť včasnú opravu zraniteľností alebo ich zmiernenie a aby sa v relevantnom prípade bezpečnostné aktualizácie uskutočňovali automaticky;	Prílohy I Časť II Bod 7
ak sú k dispozícii bezpečnostné aktualizácie na riešenie zistených bezpečnostných problémov, zabezpečujú ich bezodkladné šírenie a ak sa výrobca a komerčný používateľ nedohodli v súvislosti s individualizovaným produktom s digitálnymi prvkami inak, bezplatné šírenie sprievodných informačných správ s relevantnými informáciami pre používateľov, aj o možných potrebných krokoch.	Prílohy I Časť II Bod 8

Príloha C: Výber testovacích skupín a testovacích prípadov ETSI TS 103701 s priradením k požiadavkám CRA

ID testovacej skupiny	Testovací prípad (koncepčný)	Linked CRA requirement ref.
TSO 5.1: Žiadne univerzálne predvolené heslá	(5.1-1) Účelom tohto testovacieho prípadu je koncepčné posúdenie mechanizmov overovania na základe hesla.	Prílohy I Časť II Bod 2(d)
	(5.1-2) Účelom tohto testovacieho prípadu je koncepčné posúdenie mechanizmov generovania predinštalovaných hesiel.	Prílohy I Časť II Bod 2(d)
TSO 5.2: Implementácia prostriedkov na správu hlásení o zraniteľnostiach	(5.2-1) Účelom tohto testovacieho prípadu je koncepčné posúdenie zverejnenia politiky zverejňovania zraniteľností.	Prílohy I Časť II Bod 5
	(5.2-2) Účelom tohto testovacieho prípadu je koncepčné posúdenie spôsobu, akým sa reaguje na zraniteľnosti, a) a potvrdenie, že sú splnené predpoklady na implementáciu, b).	Prílohy I Časť II Bod 2
TSO 5.3: Aktualizácia softvéru	(5.3-1) Účelom tohto testovacieho prípadu je koncepčné posúdenie aktualizovateľnosti softvérových komponentov z hľadiska absencie aktualizácií softvéru, a) a mechanizmov aktualizácie, b).	Prílohy I Časť II Bod 7
	(5.3-2) Účelom tohto testovacieho prípadu je koncepčné posúdenie mechanizmu inštalácie aktualizácií z hľadiska primeraných opatrení na zabránenie zneužitiu inštalácie aktualizácií na zariadení užívateľa (DUT − Device Under Test) útočníkom útočníkom.	Prílohy I Časť II Bod 7
	(5.3-3) Účelom tohto testovacieho prípadu je koncepčné posúdenie mechanizmov aktualizácií z hľadiska jednoduchosti pre používateľa.	Prílohy I Časť I Bod 2(c)

		Prílohy I Časť II Bod 8
TSO 5.4: Bezpečné ukladanie citlivých bezpečnostných parametrov	(5.4-1) Účelom tohto testovacieho prípadu je koncepčné posúdenie bezpečného ukladania citlivých bezpečnostných parametrov s ohľadom na bezpečnostné požiadavky (a-c) a úplnosť dokumentácie (IXIT - Information eXchange and Interface Testing) d).	Prílohy I Časť I Bod 2(d)
	(5.4-2) Účelom tohto testovacieho prípadu je koncepčné posúdenie odolnosti proti neoprávnenému zásahu do pevne zakódovaných identít.	Prílohy I Časť I Bod 2(e)
TSO 5.5: Bezpečná komunikácia	(5.5-1) Účelom tohto testovacieho prípadu je koncepčné posúdenie kryptografie použitej pre komunikačné mechanizmy týkajúce sa používania osvedčených postupov v oblasti kryptografie (a-c) a zraniteľnosti voči uskutočniteľnému útoku d).	Prílohy I Časť I Bod 2(e)
	(5.5-4) Účelom tohto testovacieho prípadu je koncepčné posúdenie funkčnosti zariadenia prostredníctvom sieťového rozhrania v inicializovanom stave, pokiaľ ide o autentizáciu a autorizáciu.	Prílohy I Časť I Bod 2(d)
TSO 5.7: Zabezpečenie integrity softvéru	(5.7-1) Účelom tohto testovacieho prípadu je koncepčné posúdenie mechanizmov bezpečného spustenia DUT.	Prílohy I Časť I Bod 2(f)
	(5.7-2) Účelom tohto testovacieho prípadu je koncepčné posúdenie mechanizmov varovania a) a mechanizmov obmedzenia komunikácie b) v prípade zistenia neoprávnenej zmeny softvéru.	Prílohy I Časť I Bod 2 (f)
TSO 5.8: Zabezpečenie ochrany osobných údajov	(5.8-1) Účelom tohto testovacieho prípadu je koncepčné posúdenie kryptografie použitej na komunikáciu osobných údajov medzi zariadením a službou.	Prílohy I Časť I Bod 2(e)
TSO 5.9: Odolnosť systémov	(5.9-1) Účelom tohto testovacieho prípadu je koncepčné posúdenie mechanizmov odolnosti voči výpadkom siete a napájania.	Prílohy I Časť I Bod 2(h)

voči výpadkom	(5.9-3) Účelom tohto testovacieho prípadu je koncepčné posúdenie opatrení odolnosti komunikačných mechanizmov.	Prílohy I Časť I Bod 2(h)

Príloha D: Porovnanie metodík

Zoznam metodík penetračného testovania po odvetviach			
Rozsah	**Úloha v tejto príručke**		
	Hlavný	**Stredný**	**Žiadny**
Skupiny testov a postupy špecifické pre jednotlivé produkty v súlade s prílohou I CRA.	**ETSI TS 103 701**		

Vymedzuje základné požiadavky na kybernetickú bezpečnosť spotrebiteľských zariadení IoT. V tejto metodike dopĺňa TS 103 701 definovaním očakávanej bezpečnosti už v návrhu, ktorá sa overuje testovaním.	**ETSI EN 303 645**		
Poskytuje štruktúrovaný spôsob merania bezpečnostnej úrovne pomocou definovaných metrík (napr. skóre RAV). Použitie metrík OSSTMM3 môže podporiť sledovanie vnútornej zrelosti a môže byť uvedené v dokumentácii CRA, ak je to odôvodnené.	**OSSTMM3**		
Široko použiteľný pre IT systémy, siete a aplikácie. Je tiež najpodrobnejší, s jasnými fázami pre analýzu následkov zneužitia a vplyvu na podnikanie.		**PTES**	
Menej presné pokyny týkajúce sa krokov pred a po zapojení, zameranie na technickú realizáciu.		**NIST SP 800-115**	
Zamerané na aplikácie, s obmedzenými pokynmi špecifickými pre IoT.		**Príručka testovania OWASP**	
Zameriava sa na mapovanie správania protivníkov a TTP. Neposkytuje štruktúrovanú metodiku testovania, ale vylepšuje simulácie útokov a bezpečnostné operácie.			**Rámec MITRE ATT&CK**
Zamerajte sa na technické, procedurálne a compliance aspekty bezpečnostných posúdení.			**ISSAF**
Inteligentný tím červených hráčov prispôsobený kritickým sektorom, s dôrazom na realistické simulácie útokov založené na nových hrozbách.			**TIBER-EU**

Príloha E: Testovacie nástroje a rámce

Kategória	**Nástroje**
Regulačné a compliance smernice	CRA (nariadenie o kybernetickej odolnosti), PSD2 (revidovaná smernica o platobných službách), SWIFT CSP (program bezpečnosti zákazníkov)

Získavanie informácií	recon-ng (rámec prieskumu), Maltego (ťažba dát a analýza prepojení), Shodan (skenovanie internetu v hľadaní pripojených zariadení), theHarvester (nástroj na zhromažďovanie informácií), SpiderFoot (automatizované zhromažďovanie OSINT)
Bezpečnosť siete	Nmap (skenovanie siete), Wireshark (analýza paketov), Nessus (skenovanie zraniteľnosti), OpenVAS (skenovanie zraniteľnosti s otvoreným zdrojovým kódom)
Bezpečnosť webu a API	Burp Suite (testovanie webovej bezpečnosti), Checkmarx ZAP (automatizované skenovanie zraniteľnosti webu), Bruno (testovanie bezpečnosti API), Caido
Využívanie a red teaming	Metasploit (rámec pre zneužitie), BloodHound (analýza útokov na Active Directory), Cobalt Strike (nástroj pre red teaming)
Bezpečnosť cloudu	ScoutSuite (audity bezpečnosti viacerých cloudov), Prowler (hodnotenie bezpečnosti AWS), CloudMapper (vizualizácia architektúry AWS a bezpečnostné kontroly)
Bezpečnosť výroby	FactorySecure (monitorovanie bezpečnosti výrobných systémov), OTORIO RAM2 (platforma pre bezpečnosť prevádzkových technológií), Claroty (testovanie priemyselnej kybernetickej bezpečnosti)
AI a automatizácia	Darktrace (detekcia anomálií pomocou strojového učenia), Vectra AI (detekcia hrozieb pomocou umelej inteligencie), MITRE CALDERA (automatizovaná emulácia protivníka), SnapAttack (automatizovaný nástroj pre red teaming)
Analýza firmvéru	binwalk (reverzné inžinierstvo firmvéru), Ghidra (súprava nástrojov pre reverzné inžinierstvo softvéru)
Skenovanie IoT	Shodan (vyhľadávanie zariadení a zraniteľností), Firmwalker (skener konfigurácie firmvéru), JTAGulator (identifikácia hardvérového rozhrania)

Hardvérové rozhrania	USBlyzer (analýza protokolu USB), Logic Analyzers (kontrola digitálnych signálov), UART/Serial tools (ladenie sériového rozhrania)
Testovanie protokolov	Scapy (nástroj na manipuláciu s paketmi), Wireshark (analýza protokolov), CAN-utils (testovanie protokolu Controller Area Network)

Príloha E: Bezpečnostné usmernenia a osvedčené postupy

Zatiaľ čo kapitola 5 opisuje testovacie normy a metodiky integrované do tejto metodiky penetračného testovania, táto príloha obsahuje osvedčené postupy v oblasti kybernetickej bezpečnosti a pokyny na implementáciu usporiadané podľa kategórií produktov.

Kategória produktu	**Príslušné normy a usmernenia**
Systémy správy identít, prehliadače, správcovia hesiel, softvér pre digitálne certifikáty, systémy SIEM	OWASP ASVS Norma pre overovanie bezpečnosti aplikácií ISO/IEC 27001 Riadenie bezpečnosti informácií CIS Benchmarks Usmernenia pre bezpečnú konfiguráciu ISVS Norma pre overovanie bezpečnosti internetu vecí
Spotrebiteľské zariadenia IoT: smerovače, zariadenia pre inteligentné domácnosti, nositeľné zariadenia na monitorovanie zdravia,	ETSI EN 303 701 Kybernetická bezpečnosť pre spotrebiteľský internet vecí: Posudzovanie zhody so základnými požiadavkami ISO/IEC 27400:2022, Kybernetická bezpečnosť. Bezpečnosť a súkromie internetu vecí. Usmernenia ENISA Príručka osvedčených postupov pre kybernetickú bezpečnosť IoT, Bezpečný životný cyklus vývoja softvéru GDPR (Všeobecné nariadenie o ochrane údajov), ISO/IEC 27701 (Správa informácií o súkromí), Usmernenia IoT Security Foundation
Brány pre inteligentné meracie zariadenia	NIST SP 800-82 Príručka pre bezpečnosť priemyselných riadiacich systémov, IEC 62443 Priemyselné komunikačné siete – Bezpečnosť sietí a systémov
Výrobný sektor	ISO 9001 Systémy manažérstva kvality CMMC Certifikácia modelu pripravenosti kybernetickej bezpečnosti