UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH
Kompetenčné centrum kybernetickej bezpečnosti na UPJŠ

2026

Manažment zraniteľností

(technické stanovisko)

Projekt Kompetenčné centrum kybernetickej bezpečnosti na UPJŠ (KCKB UPJŠ) financovaný Európskou úniou z prostriedkov Plánu obnovy a odolnosti Slovenskej republiky, kód projektu: 17R05-04-V01-00007.

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

OBSAH

ÚVOD

Univerzita Pavla Jozefa Šafárika v Košiciach (ďalej len „UPJŠ“) prostredníctvom Kompetenčného centra kybernetickej bezpečnosti na UPJŠ (ďalej len „KC KB UPJŠ“) si dovoľuje reagovať na požiadavku Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (ďalej len „MIRRI“) zo dňa 2. júla 2025 na vypracovanie technických stanovísk v časti manažmentu zraniteľností, konkrétne na opis procesu a metodiku k zavedeniu pravidelného procesu opravy a odstraňovania zraniteľností na úrovni služieb poskytovaných vládnou jednotkou CSIRT – CSIRT.SK (ďalej len „VJ CSIRT“) podľa príslušnej legislatívy. Predkladaný text predstavuje odborný metodický podklad, ktorého cieľom je systematicky spracovať základné princípy, pojmy, procesné kroky a odporúčané postupy v oblasti identifikácie, hodnotenia, prioritizácie a odstraňovania bezpečnostných zraniteľností v prostredí organizácií verejnej správy.

Manažment zraniteľností patrí medzi základné predpoklady efektívneho riadenia informačnej a kybernetickej bezpečnosti. V podmienkach súčasného digitálneho prostredia, ktoré je charakteristické rastúcou komplexnosťou informačných systémov (vrátane informačných systémov verejnej správy), vysokou mierou prepojenosti služieb a dynamickým vývojom kybernetických hrozieb, je nevyhnutné zaviesť systematický, opakovateľný a auditovateľný proces práce s bezpečnostnými zraniteľnosťami. Každá neodhalená alebo včas neriešená zraniteľnosť môže predstavovať významné bezpečnostné riziko, ktoré môže viesť k narušeniu najmä dostupnosti, integrity alebo dôvernosti spracúvaných údajov a poskytovaných služieb.

Predložený materiál z tohto dôvodu vychádza z potreby vytvoriť prakticky využiteľný rámec pre pravidelné vykonávanie identifikácie bezpečnostných zraniteľností, ich vyhodnocovanie na základe technických aj organizačných kritérií, plánovanie a implementáciu nápravných opatrení, overovanie ich účinnosti, ako aj zabezpečenie primeranej evidencie, reportingu a komunikácie. Súčasťou textu je aj vymedzenie základných pojmov, opis životného cyklu manažmentu zraniteľností, prehľad metód a typov skenovania, ako aj stručné porovnanie vybraných nástrojov využiteľných pri automatizácii identifikácie zraniteľností a správy bezpečnostných záplat.

Dokument zároveň reflektuje širšie poslanie KC KB UPJŠ v oblasti podpory vzdelávania, výskumu a expertnej činnosti v informačnej a kybernetickej bezpečnosti. Jeho ambíciou nie je len teoretické vymedzenie problematiky, ale najmä poskytnutie odborne podloženej metodiky, ktorá môže slúžiť ako praktická pomôcka pri zavádzaní a zlepšovaní procesov manažmentu zraniteľností v súlade s požiadavkami relevantnej legislatívy a s potrebami služieb poskytovaných VJ CSIRT.

1 PREDSTAVENIE KC KB UPJŠ

Kompetenčné centrum kybernetickej bezpečnosti na Univerzite Pavla Jozefa Šafárika v Košiciach (KC KB UPJŠ) predstavuje kompetenčné centrum, v rámci ktorého sú realizované aktivity zamerané na vzdelávanie, výskum a expertnú činnosť v oblasti informačnej a kybernetickej bezpečnosti, ochrany dát, kyberkriminality a ochrany pred dezinformáciami. Súčasne KC KB UPJŠ realizuje medzinárodnú spoluprácu s akademickými partnermi zo zahraničia a poskytuje konzultácie pre možnosť prípravy a podania projektov v oblasti kybernetickej bezpečnosti.

Vytvorenie KC KB UPJŠ reflektuje viacero problémov, ktoré možno v súčasnosti identifikovať v oblasti informačnej a kybernetickej bezpečnosti (ďalej aj „KIB“):

- zvýšenie bezpečnostného povedomia relevantných subjektov zahŕňajúcich predovšetkým zamestnancov verejnej správy a študentov vysokoškolského a stredoškolského štúdia,
- vzdelávanie a výchova nových odborníkov pôsobiacich v tejto oblasti,
- výskum kybernetických hrozieb a identifikácia adekvátnych reakcií na tieto hrozby,
- zvýšenie operatívnej bezpečnosti v rámci verejnej správy poskytovaním expertných činností zo strany CSIRT tímu.

V rámci KC KB UPJŠ sa pripravoval študijný plán magisterského stupňa študijného programu aplikovaná informatika, ktorého jedna vetva sa zameriava na kybernetickú bezpečnosť. K tomuto študijnému plánu budú vytvorené, resp. modifikované viaceré predmety. Súčasne sa ako výstup kompetenčného centrá vytvára ponuka **vzdelávania** pre rôzne cieľové skupiny zamestnancov verejnej správy.

V kontexte projektu sa súčasne posilňuje **spolupráca so strednými školami**, najmä vo forme činnosti **KyberTímov**, ich vzdelávania a následného zapojenia do šírenia bezpečnostného povedomia medzi širokou verejnosťou.

V rámci vzdelávacích aktivít sa sumarizujú nové poznatky a skúsenosti z oblasti KIB, ale aj príbuzných oblastí. Tie sú aktuálne doplnené o rôzne formy zážitkového vzdelávania.

V rámci **výskumnej** činnosti dochádza v už existujúcich výskumných oblastiach k publikovaniu viacerých vedeckých výstupov a k vytvoreniu nových možných výskumných spoluprác na posilnenie výskumného a vývojového potenciálu KC KB UPJŠ.

2 ZÁKLADNÉ POJMY

Zraniteľnosť (Vulnerability) [1]

Slabina v systéme, aplikácii, procese alebo konfigurácii, ktorú môže útočník zneužiť na získanie neoprávneného prístupu, narušenie služby alebo úniku údajov. Zraniteľnosti môžu vzniknúť chybami v programovom kóde, nesprávnym nastavením alebo zastaranými verziami softvéru.

Exploit [2]

Konkrétny spôsob alebo nástroj, ktorým útočník zneužije zraniteľnosť. Exploity môžu mať podobu skriptov, programov alebo manuálnych postupov.

Proof of Concept (PoC) [3]

Demonštračný exploit, ktorý potvrdzuje existenciu a zneužiteľnosť zraniteľnosti, spravidla bez automatizovaného alebo deštruktívneho dopadu.

Patch (Záplata) [1]

Softvérová alebo konfiguračná aktualizácia, ktorou sa opravuje zistená zraniteľnosť alebo chyba. Môže byť vydaná výrobcom softvéru, open-source komunitou alebo interným vývojovým tímom.

Patch Management [4]

Proces riadenia, testovania, nasadzovania a overovania záplat s cieľom odstrániť známe zraniteľnosti v systémoch. Zahŕňa aj správu výnimiek a dokumentáciu prípadov, kedy patch nie je možné nasadiť.

CVSS (Common Vulnerability Scoring System) [5]

Štandardizovaný systém hodnotenia závažnosti zraniteľností na stupnici od 0 do 10, pričom vyššie číslo znamená vyššiu závažnosť. CVSS berie do úvahy faktory ako zložitosť útoku, požiadavky na autentifikáciu, dopad na dôvernosť, integritu a dostupnosť. CVSS existuje vo viacerých verziách (napr. v2, v3.0, v3.1, v4.0) pričom aktuálne najpoužívanejšia verzia je CVSS v3.1.

CVE (Common Vulnerabilities and Exposures) [6]

Databáza identifikátorov zraniteľností, kde každá zraniteľnosť má jedinečné ID vo formáte CVE-YYYY-NNNNN. CVE poskytuje jednotný referenčný bod na zdieľanie informácií o zraniteľnostiach.

CWE (Common Weakness Enumeration) [7]

Klasifikácia typov slabín v softvéri a systémoch. CWE popisuje príčiny zraniteľností (napr. SQL Injection, Cross-Site Scripting, nesprávna validácia vstupov) a slúži najmä na analýzu koreňových príčin a zlepšovanie bezpečnosti vývoja softvéru.

CVD (Coordinated Vulnerability Disclosure) [8]

Proces koordinovaného nahlasovania a zverejňovania zraniteľností medzi výskumníkmi, výrobcami a dotknutými organizáciami. Cieľom CVD je zabezpečiť, aby mali zodpovedné strany dostatok času na prípravu opravy alebo mitigácie pred verejným zverejnením informácií o zraniteľnosti.

Mitigácia [1]
Opatrenie, ktorým sa znižuje riziko vyplývajúce zo zraniteľnosti, ak nie je možné ju úplne odstrániť. Môže ísť o dočasný workaround, zmenu konfigurácie, obmedzenie prístupu alebo segmentáciu siete.

Remediácia [1]
Kompletné odstránenie zraniteľnosti, najčastejšie aplikovaním patchu alebo inej trvalej opravy.

Vulnerability Assessment [1]

Formálne popísanie a vyhodnotenie zraniteľností v informačnom systéme a systematické preskúmanie systému za účelom zistenia bezpečnostných slabín a hodnotenia účinnosti bezpečnostných opatrení.

Vulnerability Management [9]

Cyklická a kontinuálna disciplína identifikácie, klasifikácie, hodnotenia, priorizácie, riadenia a riešenia zraniteľností v prostredí organizácie s cieľom znížiť riziko narušenia bezpečnosti.

3 MANAŽMENT ZRANITEĽNOSTÍ A JEHO ŽIVOTNÝ CYKLUS

Manažment zraniteľností je systematický proces identifikácie, hodnotenia, priorizácie, nápravy a monitorovania zraniteľností v informačných systémoch a službách [9]. Jeho cieľom je minimalizovať riziko vyplývajúce z potenciálne zneužiteľných zraniteľností, a tým chrániť dostupnosť, integritu a dôvernosť dát a služieb. Manažment zraniteľností musí reagovať na dynamicky sa meniace bezpečnostné hrozby, nové zraniteľnosti a zmeny v IT prostredí organizácie.

Životný cyklus manažmentu zraniteľností predstavuje kontinuálny a opakujúci sa proces, ktorého cieľom je systematicky identifikovať, vyhodnocovať a odstraňovať bezpečnostné slabiny v informačných systémoch organizácie. Tento proces je tvorený niekoľkými na seba nadväzujúcimi fázami, ktoré pokrývajú celý priebeh práce so zraniteľnosťami – od ich objavenia, cez analýzu a riešenie, až po overenie účinnosti prijatých opatrení a následné zlepšovanie procesov. Jednotlivé fázy spolu vytvárajú uzavretý cyklus, ktorý umožňuje priebežne znižovať bezpečnostné riziká a zvyšovať celkovú úroveň ochrany organizácie.

1. **Identifikácia**

V tejto fáze sa hľadajú zraniteľnosti v infraštruktúre a službách prostredníctvom automatizovaných skenerov, penetračných testov, monitorovania zdrojov spravodajstva o bezpečnostných hrozbách (threat intelligence) a prijímania externých hlásení. Kľúčové je pravidelné vykonávanie týchto činností podľa vopred stanoveného harmonogramu.

2. **Hodnotenie a priorizácia**

Každá nájdená zraniteľnosť sa vyhodnotí podľa závažnosti (napr. pomocou CVSS skóre) a možného dopadu na organizáciu. Na základe tohto hodnotenia sa stanoví priorita riešenia a termín na odstránenie alebo mitigáciu.

3. **Plánovanie a implementácia nápravných opatrení**

Po stanovení priority sa vypracuje plán opravy alebo mitigácie. Môže ísť o aplikovanie záplaty (patchu), úpravu konfigurácie, zavedenie workaroundu, segmentáciu siete alebo iné bezpečnostné opatrenia. V tejto fáze je dôležité testovanie v kontrolovanom prostredí, aby sa minimalizovalo riziko negatívneho dopadu na produkčné systémy.

4. **Overenie účinnosti**

Po implementácii nápravného opatrenia sa vykoná overenie (napr. opätovné skenovanie alebo cielený test), aby sa potvrdilo, že zraniteľnosť bola úspešne odstránená alebo jej riziko bolo znížené na akceptovateľnú hodnotu.

5. **Dokumentácia a reporting**

Všetky zistenia a vykonané kroky sa zaznamenávajú v centrálnom systéme evidencie zraniteľností. Dokumentácia slúži na internú kontrolu, audit a reportovanie vedeniu a regulačným orgánom.

6. **Revízia postupov**

Na základe skúseností z predchádzajúcich cyklov, výsledkov auditov a incidentov sa proces priebežne upravuje a optimalizuje. Môže ísť o zavedenie nových nástrojov, úpravu termínov zmluvy o úrovni poskytovania služby (ďalej len „Service level agreement“ alebo „SLA“) alebo zmeny v postupoch komunikácie.

4 IDENTIFIKÁCIA ZRANITEĽNOSTÍ

Identifikácia zraniteľností je základným krokom v procese riadenia informačnej a kybernetickej bezpečnosti. Cieľom je včasné odhalenie slabých miest v infraštruktúre, systémoch a aplikáciách, ktoré by mohli byť zneužité útočníkmi. Včasná detekcia umožňuje organizácii prijať nápravné opatrenia skôr, ako dôjde k incidentu, čím sa minimalizuje riziko finančných strát, poškodenia reputácie alebo prerušenia služieb.

Identifikácia zraniteľností sa realizuje kombináciou automatizovaných a manuálnych metód, ako sú pravidelné skenovanie zraniteľností, monitorovanie bezpečnostných upozornení výrobcov, analýza bezpečnostných hlásení a sledovanie relevantných databáz zraniteľností. Medzi kľúčové zdroje informácií patria najmä databázy CVE a národné alebo medzinárodné bezpečnostné autority.

Významným zdrojom informácií o zraniteľnostiach je aj **EUVD (European Vulnerability Database)** prevádzkovaná agentúrou ENISA. EUVD poskytuje overené a štruktúrované informácie o zraniteľnostiach relevantných pre európsky kontext, vrátane prepojenia na CVE identifikátory, hodnotenia závažnosti a dopadov.

Súčasťou manažmentu zraniteľností je pravidelné vykonávanie skenovania zraniteľností, ktorého frekvencia a rozsah by mali vychádzať z klasifikácie aktív, ich kritickosti a miery vystavenia hrozbám. V praxi sa uplatňujú najmä tieto odporúčania [23, 24, 25]:

- **Externé (internet-facing) skenovania** systémov a služieb dostupných z verejnej siete by mali byť vykonávané pravidelne, spravidla aspoň raz mesačne, prípadne častejšie pri systémoch s vysokou kritickosťou alebo po významných zmenách konfigurácie.
- **Interné sieťové skenovania** zamerané na identifikáciu zraniteľností v internej infraštruktúre sa typicky vykonávajú štvrťročne alebo mesačne, v závislosti od veľkosti prostredia a úrovne rizika.
- **„Authenticated“ skenovania** (so systémovými alebo aplikačnými účtami) sú považované za efektívnejšie a mali by byť realizované pravidelne, ideálne v rovnakých intervaloch ako interné skeny, keďže poskytujú presnejší obraz o stave systémov.
- **Kompletné (full) skenovania** infraštruktúry majú zmysel najmä periodicky alebo pri významných zmenách prostredia, ako je nasadenie nových systémov, migrácie alebo rozsiahle aktualizácie.
- **Ad-hoc skenovania** by mali byť vykonané po identifikácii kritických zraniteľností, bezpečnostných incidentoch alebo po aplikovaní nápravných opatrení za účelom overenia ich účinnosti.

4.1 METÓDY IDENTIFIKÁCIE ZRANITEĽNOSTÍ

Identifikácia zraniteľností sa realizuje kombináciou viacerých prístupov. Môže ísť o nahlásenie zraniteľností externou entitou, interné penetračné testy alebo použitie automatizovaných nástrojov.

Automatizované skenovanie zraniteľností – využitie špecializovaných nástrojov ako Nessus, OpenVAS, Achilles alebo podobných riešení, ktoré dokážu detegovať známe zraniteľnosti, nesprávne konfigurácie a chýbajúce aktualizácie. Tieto skenery čerpajú údaje z databáz zraniteľností, ktoré sú špecifikované vo forme pluginov, NVT zdrojov (feedov) alebo iných pravidiel detekcie. Pri detekcii zraniteľností zo siete (bez autentifikácie) skener porovnáva služby a odpovede zariadení so známymi signatúrami zraniteľností v týchto pluginoch/feedoch. **Nessus pluginy** obsahujú pravidlá na identifikáciu konkrétnych CVE alebo kontrol konfigurácií. Ich pravidelné aktualizovanie (vo väčšine prípadov na dennej báze) sú kľúčové pre to, aby skener vedel detegovať novozverejnené zraniteľnosti. Ak neexistuje plugin pre konkrétnu chybu, Nessus ju nemusí automaticky nájsť pri externom skenovaní. Ak neexistuje plugin alebo pravidlo, organizácia by mala uvažovať o alternatívnych mechanizmoch overenia ako napríklad autentifikovaný skenovanie (credentialed scanning) alebo penetračný test.

Skenovanie zraniteľností pomocou automatizovaných nástrojov môže byť vykonávané po súhlase správcu služby, resp. časti siete. Odporúčané je skenovať počas pracovnej doby, kedy sa otestujú systémy počas bežnej prevádzky. V špecifických prípadoch je lepšie vykonávať skenovanie mimo pracovnej doby, nakoľko to môže obmedziť priebeh prevádzky. Nevýhodou tohto prístupu môže byť nedostupnosť všetkých zariadení v čase testovania.

Penetračné testy a red-team cvičenia – manuálne alebo poloautomatizované testovanie reálnych scenárov útokov s cieľom odhaliť zraniteľnosti, ktoré nemusia byť zachytené automatizovanými skenermi. Vykonávajú sa na systémoch, resp. častiach infraštruktúry dohodnutej vopred. Rovnako ako rozsahu testu sa špecifickú aj ďalšie pravidlá, podľa ktorých sa penetračný test môže vykonávať. Penetračné testy poskytujú hlbší pohľad na reálnu mieru rizika a potenciálny dopad. Tento kontext poskytujú najmä z dôvodu, že penetračný tester ma k dispozícii kontext, v ktorom sa zraniteľnosť vyskytuje. **Penetračné testovanie** je zamerané na identifikáciu konkrétnych technických zraniteľností v vopred definovanom rozsahu a odporúča sa vykonávať raz ročne alebo po významných zmenách informačného systému. **Red-team cvičenia** simulujú pokročilého útočníka a overujú schopnosť organizácie detegovať a reagovať na útok naprieč technickými aj procesnými kontrolami, pričom sa vykonávajú menej často, spravidla raz za 2–3 roky.

Threat Intelligence a externé hlásenia – Ide o systematické využívanie informácií z dôveryhodných interných a externých zdrojov, ktoré upozorňujú na nové, kritické alebo aktívne zneužívané zraniteľnosti a súvisiace hrozby (CERT/CSIRT odporúčania, databázy zraniteľností a exploitov, bug bounty programy, výrobcovia softvéru).

- **CERT/CSIRT odporúčania**: Národné a sektorové CERT/CSIRT tímy poskytujú kontextualizované informácie o aktuálnych hrozbách a zraniteľnostiach z daného regiónu, často doplnené o odporúčané mitigácie.

- **Databázy zraniteľností a exploitov (CVE, NVD, EUVD):** Poskytujú štruktúrované technické informácie o zraniteľnostiach vrátane identifikátorov, popisu, závažnosti (CVSS) a dostupnosti opráv.
- **Bug bounty programy:** Poskytujú včasné informácie o novoobjavených zraniteľnostiach, často ešte pred ich masovým zneužívaním. Ich prínosom je rýchlosť a technická hĺbka, avšak informácie je potrebné overovať z hľadiska dôveryhodnosti a dopadu na konkrétne prostredie organizácie.
- **Bezpečnostné oznámenia výrobcov softvéru a hardvéru:** Obsahujú oficiálne informácie o zraniteľnostiach, dostupných patchoch a odporúčaných krokoch na ich odstránenie.

Externé hlásenia zraniteľností by mali obsahovať identifikáciu produktu, resp. služby, popis zraniteľnosti, spôsob zistenia, PoC alebo exploit, dopad, dátum a čas objavenia, kontaktné informácie a ďalšie relevantné zistenia.

4.2 TYPY SKENOVANÍ

V rámci automatizovaného skenovania zraniteľností sa v praxi využívajú viaceré typy skenovaní, ktoré sa líšia mierou prístupu k cieľovým systémom, presnosťou výsledkov a prevádzkovým dopadom. Výber vhodného typu skenovania závisí od cieľa skenovania, typu aktív a organizačných obmedzení resp. štruktúry.

Unauthenticated (neautentifikované) skenovanie prebieha bez prihlasovacích údajov a simuluje pohľad externého útočníka. Skenovanie sa vykonáva výhradne na základe sieťovej komunikácie, identifikácie otvorených portov, služieb a ich verzií. Tento typ skenovania sa využíva najmä na hodnotenie internet-facing systémov alebo identifikáciu exponovaných systémov. Nevýhodou je nižšia presnosť výsledkov a vyššia miera false positive (ďalej len „FP“) výsledkov.

Credentialed (authenticated) skenovanie využíva autentifikačné údaje (napr. lokálne alebo doménové účty) a umožňuje skeneru získať detailné informácie priamo zo systému. Tento prístup umožňuje presnejšiu identifikáciu chýbajúcich záplat a nesprávnych konfigurácií. Výhodou je nižšia FP, schopnosť detegovať zraniteľnosti, ktoré nie sú viditeľné zo siete. Zároveň ide o typ skenovania, ktorý môže mať vyšší dopad na prevádzku. Sú uprednostňované pre vybrané časti organizácie, resp. menšie časti infraštruktúry, nie však na plošné skenovanie.

Agent-based skenovanie využíva lokálne nainštalovaného agenta na cieľovom systéme, ktorý zhromažďuje informácie o stave systému a odosiela ich do centrálneho nástroja. Tento prístup je vhodný pre mobilné zariadenia, zariadenia, ktoré sú často offline (pravidelné skenovanie by ich nemuselo zachytiť), systémy, ktoré nie sú trvalo dostupné zo siete. Nevýhodou je vyšší nárok na správu agentov, obmedzená použiteľnosť pre uzavreté systémy a sieťové zariadenia a kompatibilita s rôznymi operačnými systémami.

V praxi sa najčastejšie používa **kombinovaný prístup**. Tento prístup využíva kombináciu predchádzajúcich prístupov, kde neautentifikované skenovanie poskytuje plošný prehľad,

autentifikované skenovanie zabezpečuje presnejšie výsledky na konkrétnych častiach infraštruktúry a agent-based skenovanie dopĺňa ďalšie špecifické prípady použitia.

4.3 NÁSTROJE NA AUTOMATIZOVANÚ IDENTIFIKÁCIU ZRANITEĽNOSTÍ

Tabuľka 1 ukazuje porovnanie dostupných nástrojov na automatizáciu skenovania zraniteľností. Porovnanie ukazuje, že výber nástroja na skenovanie zraniteľností závisí predovšetkým od rozpočtu, veľkosti organizácie a typu prostredia. Porovnávali sme nástroje Nessus, OpenVAS, Burp Suite a Rapid7 InsightVM.

- **Nessus [10]** je univerzálny a overený nástroj pre infraštruktúrne skenovanie s jednoduchým používaním a bohatou databázou zraniteľností, vhodný pre väčšinu organizácií. Jedná sa o komerčný, platený nástroj. Nessus je vhodný na sieťové a host-based skeny, ktoré umožňujú širokú škálu aktív od serverov, pracovných staníc a sieťových zariadení a služieb. Musí však byť k dispozícii signatúry zraniteľností pre tieto zariadenia v pluginoch.
- **OpenVAS [11]** predstavuje open-source alternatívu, ktorá je vhodná na základné pokrytie, ale vyžaduje viac manuálnej práce a know-how. OpenVAS taktiež poskytuje skenovanie IP adresovateľných zariadení. Rovnako však musí obsahovať pluginy pre dané služby a zraniteľnosti.
- **Burp Suite [12]** je špecializovaný na penetračné testovanie webových aplikácií a mal by dopĺňať infraštruktúrne skenery, najmä ak organizácia poskytuje webové služby. Burp Suite neposkytuje sieťové skenovanie zariadení a infraštruktúry ako Nessus. Primárne sa zameriava na webové aplikácie a služby.
- **Rapid7 InsightVM [13]** je komplexné enterprise riešenie, ktoré umožňuje pokročilé priorizovanie a integrácie, ale je vhodnejšie pre väčšie organizácie s dostatočným rozpočtom. Rapid7 podobne ako Nessus poskytuje aj sieťové a host-based skenovanie infraštruktúry a služieb, spolu s ďalšími funkcionalitami ako napríklad inventarizácia aktív atď.

Nástroj	Typ	Primárne použitie	Typy skenovania	Agent / Agentless	CS/CD / API	Integrácie	Reporting a licencovanie	Frekvencia aktualizácii zdrojov
Tenable Nessus	Komerčný	Network & host vulnerability scanning / assessment	Network/host scanning, konfiguračné kontroly	Primárne agentless	API, podpora automatizácie	SIEM, ITSM, Tenable One integrácie	Komerčné licencovanie, robustné reporty & dashboardy	Denne
OpenVAS / Greenbone	Open-source	Network vulnerability scanning	Network/host scanning, konfigurácie, NVT feedy	Agentless	API, skriptovateľné	Integrácia cez API/skripty, Greenbone komerčné edície	Open-source; enterprise support v platených verziách	Denne
Burp Suite	Komerčný (Community/ Pro/ Enterprise)	Web application security testing (proxy + scanner)	Web application scanning, manuálne testy, intruder/fuzzer	Agentless	REST API, CI/CD integrácie (Pro/Enterprise)	Integrácie s bugtrackermi, CI/CD	Community free, Pro/Enterprise platené; silné reporty pre web app	Denne/ pri vydaní novej verzie
Rapid7	Komerčný	Vulnerability management + priorizácia rizík	Agent-based aj agentless, on-prem + cloud + web	Aj agentless scan enginy	Plná API podpora, CI/CD, remediácia projekty	Integrácie so SIEM, ITSM, patch management	Komerčné licencovanie (per-asset), live dashboards	Denne

Tabuľka 1 Porovnanie automatizovaných nástrojov na skenovanie zraniteľností

5 HODNOTENIE (POSUDZOVANIE) A PRIORIZÁCIA

Cieľom **fázy hodnotenia** je spracovať zistenú zraniteľnosť tak, aby bola jednoznačne pochopená jej závažnosť a potenciálny dopad na organizáciu. Na základe hodnotenia sa určí priorita riešenia a termín, do ktorého musí byť vykonaná náprava alebo prijaté iné opatrenia.

V Slovenskej republike sú bezpečnostné opatrenia pre správu zraniteľností a kybernetických hrozieb upravené v ustanovení § 20 ods. 2 písm. b) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a následne rozpracované vo vyhláške NBÚ č. 227/2025 Z. z. o bezpečnostných opatreniach. Podľa prílohy č. 1 tejto vyhlášky sú prevádzkovatelia základných služieb povinní najmenej raz ročne vykonávané pravidelné posudzovanie zraniteľností (ak ide o prevádzkovateľov kritickej základnej službe, potom sa toto posudzovanie vykonáva raz za 6 mesiacov).

5.1 METODIKA HODNOTENIA

Hodnotenie by malo byť kombináciou štandardizovaného skórovania (napr. CVSS) a interných kritérií, ktoré reflektujú špecifiká organizácie. CVSS poskytuje technické skóre (0 – 10) vyjadrujúce závažnosť zraniteľnosti, pričom existuje vo viacerých verziách (v2, v3.0, v3.1 a najnovšie v4.0). Jednotlivé verzie sa líšia v spôsobe výpočtu aj v zohľadňovaných metrikách – napríklad verzia 3.x zaviedla detailnejšie hodnotenie dopadu na dôvernosť, integritu a dostupnosť, zatiaľ čo verzia 4.0 ďalej rozširuje kontext hodnotenia o faktory ako exploitabilita v čase či prostredie organizácie. V praxi je v súčasnosti najrozšírenejšie používaná verzia 3.1, pričom prechod na verziu 4.0 postupne prebieha [5]. Do konečného hodnotenia sa premietne aj dôležitosť aktíva pre organizáciu, expozičný faktor (či je služba dostupná z internetu), dostupnosť exploitov (databáza známych exploitov).

Prístup k hodnoteniu rizika, ktoré je kombináciou pravdepodobnosti zneužitia danej zraniteľnosti a dopadu na organizáciu je v súlade s odporúčaniami NIST a ISO/IEC. Na základe týchto odporúčaní je dôležite sa zamerať primárne na túto kombináciu, teda pravdepodobnosť zneužitia zraniteľnosti, ktorá sa skladá z technickej závažnosti, dostupnosti exploitov a expozície systému a dopadu na organizáciu, kde je potrebné sa pozerať na kritickosť aktíva a typ údajov, ktoré sa v systéme nachádzajú.

Pre praktické rozhodovanie je odporúčané použiť maticu, ktorá kombinuje technické skóre (CVSS), kritickosť aktíva a stav, či je služba dostupná z internetu. Následne výsledkom priradiť priority Critical / High / Medium / Low.

5.2 SLA A CIEĽOVÉ TERMÍNY

Metodika by mala mať definované viazané termíny remediácie resp. mitigácie podľa kategórie (napr. závažnosti). Termíny možno upraviť podľa lokálnych požiadaviek, dostupnosti zdrojov a právnych požiadaviek. V prípade, že termín nie je reálne dosiahnuteľný, takáto výnimka musí byť

zdokumentovaná. V súčasnej dobe slovenská právna úprava neobsahuje právne záväzne lehoty na mitigáciu zraniteľností.

Príklad možných termínov pre mitigáciu zraniteľností:

- Critical: 14 dní
- High: 30 dní
- Medium: 90 dní
- Low: 120 dní

Pre zvýšenie presnosti hodnotenia je vhodné základné skóre obohacovať o externé kontextové informácie z dôveryhodných zdrojov. V praxi ide najmä o overenie, či sa daná zraniteľnosť nachádza v katalógu CISA Known Exploited Vulnerabilities (KEV) [14], či je k dispozícii verejne dostupný exploit (napr. ExploitDB) alebo či existujú doplňujúce technické informácie v nástrojoch typu CIRCL Vulnerability Lookup [15]. Prítomnosť zraniteľnosti v KEV katalógu alebo existencia funkčného exploitu významne zvyšuje pravdepodobnosť zneužitia a mala by sa premietnuť do vyššej priority riešenia, aj v prípadoch, keď samotné CVSS skóre nie je extrémne vysoké.

6 IMPLEMENTÁCIA NÁPRAVNÝCH OPATRENÍ

Táto kapitola stanovuje rámec a postupy pre efektívne riešenie zraniteľností - od rozhodovania o vhodnom opatrení až po jeho bezpečné nasadenie a overenie. Popisuje, kto za jednotlivé kroky zodpovedá, aké sú požiadavky na plánovanie a testovanie zmien, aké mechanizmy musia byť použité pri nasadzovaní opráv a ako sa vykonáva overenie úspešnosti. Cieľom je zabezpečiť, aby nápravné opatrenia minimalizovali prevádzkové riziká, boli v súlade s internými politikami a regulačnými požiadavkami a zostali auditovateľné pre následné vyhodnotenie a zlepšovanie procesu.

Súčasťou implementácie nápravných opatrení je aj **systematický patch management**, ktorý musí byť úzko prepojený s procesmi riadenia zmien, riadenia zraniteľností a riadenia rizík. Organizácia zabezpečuje, aby bezpečnostné záplaty pochádzali z dôveryhodných zdrojov, boli overené z hľadiska integrity, otestované v kontrolovanom prostredí a nasadené do produkcie v primeranom čase na základe rizika. Patchovanie je plánovanou súčasťou bežnej údržby systémov, pričom v prípade kritických zraniteľností musí byť umožnené aj urýchlené (hotfix) nasadenie. Ak nie je možné patch aplikovať, rozhodnutie musí byť zdôvodnené, zdokumentované a kompenzované primeranými mitigujúcimi opatreniami spolu s akceptáciou reziduálneho rizika. Celý proces musí byť auditovateľný a podporený evidenciou testovania, schvaľovania, nasadenia a prípadného rollbacku.

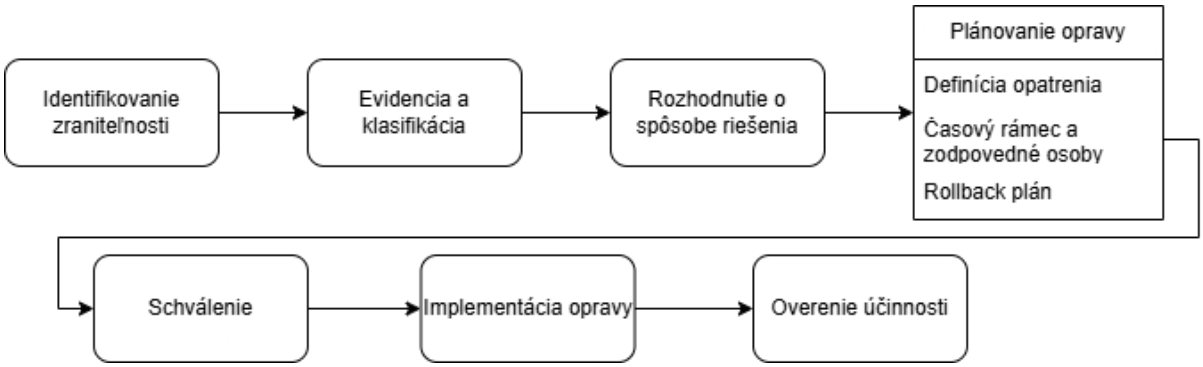
6.1 ROZHODOVACÍ PROCES

Pri každom náleze je dôležité rozhodnutie, akým spôsobom bude daná zraniteľnosť riešená. Ak je k dispozícii trvalá oprava (patch), preferovanou cestou je riadené nasadenie patchu. Ak patch nie je k

dispozícii, nie je bezpečné ho okamžite aplikovať, alebo by spôsobil neprijateľný dopad na prevádzku, sú akceptovateľné dočasné mitigácie (workaroundy) — napr. obmedzenie prístupu, firewall pravidlá, segmentácia siete, dočasné zníženie práv procesov. Deaktivácia služby alebo izolácia systému je poslednou možnosťou používanou pri vysokom riziku zneužitia a nemožnosti iných riešení. Každé rozhodnutie musí byť zdôvodnené a zaznamenané.

6.2 Plánovanie opravy

Po rozhodnutí o spôsobe nápravy sa vypracuje plán, ktorý obsahuje: popis opatrenia, časový rámec, požadované okno na nasadenie, kontaktné osoby a rollback plán. Nasadenie záplaty alebo opravy musí prejsť cez schválenie zodpovednej osoby. Obrázok č. 1. znázorňuje diagram plánovania opravy spolu s ďalšími krokmi.



Obrázok č. 1 Diagram plánovania opravy

6.3 Nasadenie opravy

Následne je potrebné vykonať nasadenie záplaty resp. opatrenia v testovacom prostredí. Ak sú k dispozícii automatizované testy, je potrebné ich spustiť, zaznamenať a následne vyhodnotiť výsledky.

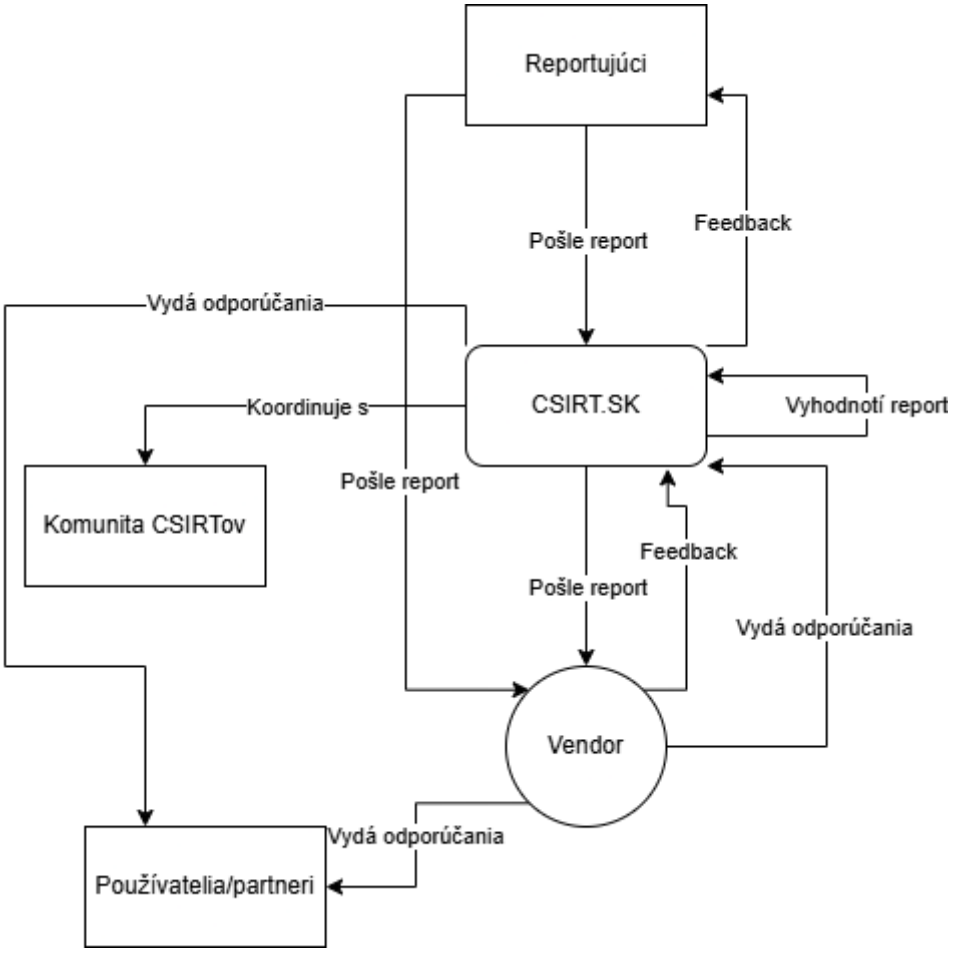
Nasadenie na produkčné systémy sa vykonáva v schválenom časovom okne. Všetky kroky nasadenia musia byť zdokumentované a mali by byť dostupné postupy, ktoré umožnia rýchly návrat do predchádzajúceho stavu pri neočakávaných problémoch. Počas a po nasadení je potrebné monitorovať systémové metriky a aplikačné logy, aby sa rýchlo odhalili vedľajšie efekty.

6.4 Overenie účinnosti

Po nasadení sa vykoná overenie účinnosti nasadeného patchu. Overenie sa môže vykonať opätovným skenovaním zraniteľností, cieleným pentestom alebo špecifický test, ktorý preukáže, že identifikovaný problém bol odstránený alebo mitigovaný v súlade s cieľmi. Len po úspešnom overení sa ticket uzavrie ako „vyriešený“.

7 ZVEREJNENIE ZRANITEĽNOSTI A KOMUNIKÁCIA

Táto kapitola popisuje, ako VJ CSIRT prijíma, spracúva a komunikuje informácie o zraniteľnostiach či už sú hlásené internými tímami, externými výskumníkmi alebo tretími stranami (odporúčania vendorov, iné CSIRT / CERT tímy, bug bounty programy). Definuje zodpovednosti, komunikačné kanály, termíny reakcií a princípy koordinovaného zverejňovania tak, aby boli zabezpečené rýchle a bezpečné kroky pri riešení nálezov a minimalizované riziká pre dotknuté systémy a používateľov. Obrázok 2. znázorňuje formou diagramu postup zverejňovania zraniteľnosti.



Obrázok 2 Diagram zverejnenia zraniteľností

7.1 POLITIKA ZVEREJŇOVANIA ZRANITEĽNOSTÍ

Politika zverejňovanie zraniteľností zabezpečuje postup podľa zásad zodpovedného oznamovania: prijatie hlásenia, potvrdenie hlásenia a následná spolupráca s oznamovateľom, resp. dodávateľom na overení a náprave pred zverejnením detailov. CSIRT zabezpečuje ochranu dôverných informácií a nešíri

PoC kódy alebo iné citlivé detaily, ktoré by uľahčili zneužitie, pokiaľ to nie je nevyhnutné pre technickú koordináciu opravy.

Koordinované zverejnenie sa riadi dohodnutým časovým plánom s dodávateľom alebo majiteľom systému. Verejné oznámenie sa uskutoční až po dostupnosti adekvátneho riešenia, respektíve skôr len v odôvodnených prípadoch (napr. pri neprimeranej nečinnosti dodávateľa) po zhodnotení rizika. Všetky kroky komunikácie sú auditovateľné — CSIRT dokumentuje prijatie hlásenia, priebeh triáže, komunikáciu s tretími stranami a rozhodnutie o zverejnení. Táto politika zároveň stanovuje očakávané reakčné časy a základné požiadavky na obsah hlásenia, aby bolo umožnené efektívne a bezpečné riešenie nahlásenej zraniteľnosti.

7.2 Prijatie a potvrdenie prijatia hlásenia

Primárny kanál pre prijímanie hlásení je oficiálny e-mail / portál CSIRT. Hlásenia prijaté cez iné kanály (telefón, sociálne siete) sú akceptované, avšak presmerované do oficiálneho ticketu. V žiadosti o nahlásenie by mal oznamovateľ poskytnúť aspoň: popis zraniteľnosti, kroky na reprodukciu, dôkazy (logy/screenshots), dotknuté systémy a kontaktné údaje oznamovateľa.

Po prijatí hlásenia CSIRT odošle potvrdenie prijatia do 72 hodín (3 pracovné dni) s unikátnym ID. Počiatočná triáž (overenie, priradenie priority podľa matice) prebehne v rozmedzí 5 pracovných dní od prijatia. Ak ide o zraniteľnosť s dôkazmi aktívneho zneužívania, triáž prebehne okamžite a spustia sa zrýchlené postupy na mitigáciu. Tieto časové rámce sú odporúčané a mali by byť upravené podľa dostupných kapacít a regulačných požiadaviek.

7.3 Koordinácia s tretími stranami

Ak je zraniteľnosť v produktoch tretích strán, CSIRT iniciuje koordináciu s vendorom, žiada o status opravného balíka a o odhad termínu nápravy. Pri vhodných prípadoch CSIRT asistuje s žiadosťou o pridelenie CVE identifikátora a sleduje status opráv. Koordinované zverejnenie obsahuje časový plán, po dohode s vendorom.

8 Patch management

Cieľom tejto časti metodiky je stanoviť jednotný proces správy a nasadzovania bezpečnostných záplat vo všetkých systémoch a službách, ktoré sú predmetom činnosti VJ CSIRT. Patch management je kľúčovým nástrojom prevencie zneužitia známych zraniteľností a jeho správne nastavenie má zásadný vplyv na úroveň kybernetickej bezpečnosti.

8.1 Riadenie zodpovednosti

Za patch management zodpovedá kombinácia viacerých rolí. Vlastník systému zabezpečuje plánovanie, testovanie a realizáciu nasadenia záplat. Pri fyzickom nasadení patchov spolupracuje s prevádzkovým tímom. Bezpečnostný tím sleduje publikované zraniteľnosti, vyhodnocuje ich závažnosť a prioritu a overuje, či bolo nápravné opatrenie úspešne aplikované. Riadiaci pracovníci schvaľujú výnimky a akceptáciu rizika v prípade, že záplatu nie je možné nasadiť.

8.2 IDENTIFIKÁCIA A PRIORIZÁCIA

Proces začína identifikáciou zraniteľnosti. Vstupom pre identifikáciu môžu byť výstupy zo skenovacích nástrojov, odporúčania výrobcov, databázy zraniteľností, informácie z threat intelligence, alebo externé hlásenia (napr. od CERT). Každá zraniteľnosť sa vyhodnotí pomocou CVSS skóre a interného posúdenia dopadu na organizáciu. Na základe toho sa stanoví priorita a termín nápravy. Pre kritické a vysoko závažné zraniteľnosti, sa uplatňujú kratšie doby pre nasadenie nápravy – napríklad do 14 dní. Zraniteľnosti so strednou alebo nízkou závažnosťou sa riešia do 90 dní resp. 120 dní, ak interné posúdenie neurčí inak.

8.3 NASADENIE PATCHU

Pred samotným nasadením sa vykoná testovanie, aby sa minimalizovalo riziko negatívneho dopadu na produkčné služby. Ak je to možné, využívajú sa automatizované testy na overenie funkčnosti a kompatibility. Následne po schválení prebieha nasadenie do produkčného prostredia. Po aplikovaní záplaty sa vykoná overenie prostredníctvom opätovného skenu, aby sa potvrdilo, že zraniteľnosť bola úspešne odstránená. Po úspešnom odstránení sa záznam uzatvára ako vyriešený.

V prípade, že záplatu nie je možné nasadiť, zodpovedná osoba navrhne kompenzačné opatrenia. Môže ísť o situácie absencie záplaty od vendora, následnej nekompatibility bežiacej služby alebo nekompatibility hardvéru. V takýchto prípadoch navrhne zodpovedná osoba iný spôsob mitigácie ako je workaround, sieťová segmentácia alebo obmedzenie prístupu. Tieto prípady sa zaznamenávajú do dokumentu. Dlhodobá výnimka sa môže riešiť formálnou akceptáciou rizika.

8.4 NÁSTROJE A AUTOMATIZÁCIA

Pre efektívnu správu patchov sa odporúča využívať centralizované nástroje, ktoré umožňujú plánovanie, distribúciu, reporting a evidenciu nasadených záplat. Takéto nástroje by mali poskytovať auditovateľné logy o vykonaných zmenách a podporovať integráciu s ticketovacím systémom, čím sa zabezpečí sledovateľnosť a kontrola celého procesu.

Automatizácia patch managementu, najmä v oblasti distribúcie aktualizácií a sledovania ich stavu, výrazne znižuje riziko ľudskej chyby, skracuje čas potrebný na nasadenie záplat a umožňuje rýchlejšiu reakciu na kritické zraniteľnosti.

Prehľad vybraných nástrojov na správu záplat, ich licenčných modelov, podporovaných platforiem a vybraných funkcionalít je uvedený v Tabuľke 2. Uvedené nástroje slúžia ako príklady riešení, ktoré je možné využiť v rámci procesu patch managementu, pričom ich konkrétne nasadenie by malo vychádzať z potrieb a štruktúry organizácie.

Nástroj	Typ licencie	Platformy	Offline patching	Integrácia s WSUS/SCCM	Ďalšie funkcionality
Chocolatey [16]	Open source / Platený	Windows	Áno	Áno	Automatizovaná správa softvéru cez PowerShell, podpora pre viac ako 7 500 balíčkov, možnosť interného hostovania balíčkov.
WinGet [17]	Open source	Windows 10/11/Server 2025	Nie	Nie	Nástroj pre inštaláciu, aktualizáciu a konfiguráciu aplikácií, integrácia s Microsoft Store a ďalšími zdrojmi.
APT (Advanced Packaging Tool) [18]	Open source	Linux (Debian, Ubuntu)	Áno	Nie	Štandardný balíčkový manažér pre Debian a Ubuntu, podpora pre automatické aktualizácie a správu záplat.
Microsoft SCCM (System Center Configuration Manager) [19]	Platený	Windows Server	Áno	Áno	Komplexný enterprise nástroj na správu zariadení, vrátane distribúcie záplat a aplikácií, podpora pre reporting a compliance.
WSUS (Windows Server Update Services) [20]	Bezplatný	Windows Server	Áno	Áno	Nástroj od Microsoftu na správu distribúcie aktualizácií pre Windows zariadenia, podpora pre reporting a schvaľovanie záplat.
SolarWinds Patch Manager [21]	Platený	Windows Server	Áno	Áno	Automatizovaná správa záplat pre Windows servery a pracovné stanice, integrácia s WSUS a SCCM, podpora pre offline patching a reporting.

Invanti Patch for Endpoints Manager [22]	Platený	Windows, macOS, Linux	Áno	Áno	Komplexné riešenie pre správu záplat naprieč rôznymi platformami a aplikáciami, podpora pre vzdialené patchovanie, reporting a compliance.

Tabuľka 2 Porovnanie nástrojov na automatizovanú správu záplat a aktualizácií

ZÁVER

Manažment zraniteľností je nevyhnutnou súčasťou moderného systému riadenia kybernetickej a informačnej bezpečnosti a predstavuje jeden z kľúčových nástrojov na znižovanie rizika úspešného kybernetického útoku. Jeho význam spočíva najmä v tom, že umožňuje organizácii prejsť od reaktívneho riešenia bezpečnostných incidentov k proaktívnemu prístupu, založenému na včasnej identifikácii slabých miest, ich dôslednom vyhodnotení a koordinovanej realizácii primeraných opatrení. Len organizácia, ktorá má zavedený systematický, opakovateľný a auditovateľný proces práce so zraniteľnosťami, dokáže dlhodobo udržiavať primeranú úroveň ochrany svojich informačných aktív a služieb.

Predložený text poukazuje na to, že efektívny manažment zraniteľností musí byť postavený na kombinácii viacerých vzájomne previazaných prvkov. Patrí medzi ne pravidelná identifikácia bezpečnostných zraniteľností prostredníctvom automatizovaných nástrojov aj manuálnych testovacích metód, kvalifikované hodnotenie ich závažnosti s prihliadnutím na technické aj organizačné faktory, dôsledná priorizácia podľa reálneho rizika, bezpečné a riadené nasadzovanie opráv, overovanie účinnosti prijatých opatrení a dôkladná dokumentácia všetkých vykonaných krokov. Dôležitou súčasťou procesu je aj koordinovaná komunikácia pri zverejňovaní zraniteľností a zodpovedne nastavený patch management, ktorý zabezpečuje, aby boli známe slabiny odstraňované v primeranom čase a kontrolovaným spôsobom.

Zároveň je potrebné zdôrazniť, že úspešnosť manažmentu zraniteľností nezávisí len od použitých technológií, ale aj od jasného rozdelenia rolí, dostupnosti odborných kapacít, nastavenia interných procesov a podpory zo strany vedenia organizácie. Automatizované nástroje, databázy zraniteľností a externé threat intelligence zdroje predstavujú významnú pomoc, samy osebe však nedokážu nahradiť kvalifikované rozhodovanie, správnu interpretáciu výsledkov ani efektívnu koordináciu medzi bezpečnostnými, prevádzkovými a riadiacimi tímami.

Z pohľadu dlhodobého budovania odolnosti organizácie je preto nevyhnutné vnímať manažment zraniteľností ako kontinuálny proces zlepšovania, ktorý sa musí pravidelne revidovať a prispôsobovať novým technológiám, zmenám v infraštruktúre a vývoju hrozieb.

POUŽITÉ ZDROJE

[1] NIST. (n.d.). Glossary. National Institute of Standards and Technology. Dostupné z https://csrc.nist.gov/glossary

[2] Cisco. (n.d.). What is an exploit? Cisco. Dostupné z https://www.cisco.com/site/us/en/learn/topics/security/what-is-an-exploit.html

[3] TechTarget. (n.d.). Proof of concept (PoC) exploit. TechTarget. Dostupné z https://www.techtarget.com/searchsecurity/definition/proof-of-concept-PoC-exploit

[4] IBM. (n.d.). Patch management. IBM. Dostupné z https://www.ibm.com/think/topics/patch-management

[5] FIRST. (n.d.). Common Vulnerability Scoring System (CVSS). Forum of Incident Response and Security Teams. Dostupné z https://www.first.org/cvss/

[6] MITRE. (n.d.). CVE. The MITRE Corporation. Dostupné z https://www.cve.org/

[7] MITRE. (n.d.). CWE. The MITRE Corporation. Dostupné z https://cwe.mitre.org/

[8] ENISA. (n.d.). Vulnerability disclosure. European Union Agency for Cybersecurity. Dostupné z https://www.enisa.europa.eu/topics/vulnerability-disclosure

[9] IBM. (n.d.). Vulnerability management. IBM. Dostupné z https://www.ibm.com/think/topics/vulnerability-management

[10] Tenable. (n.d.). *Nessus*. Tenable. Dostupné z https://www.tenable.com/products/nessus

[11] Greenbone / OpenVAS. (n.d.). *OpenVAS — Open Vulnerability Assessment Scanner*. Dostupné z https://www.openvas.org/

[12] PortSwigger. (n.d.). *Burp Suite — Web vulnerability scanner and testing platform*. PortSwigger. Dostupné z https://portswigger.net/burp

[13] Rapid7. (n.d.). *InsightVM — Vulnerability management*. Rapid7. Dostupné z https://www.rapid7.com/products/insightvm/

[14] CISA. (n.d.). Known Exploited Vulnerabilities Catalog. Cybersecurity and Infrastructure Security Agency. Dostupné z https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[15] CIRCL. (n.d.). Vulnerability-Lookup. Computer Incident Response Center Luxembourg. Dostupné z https://vulnerability.circl.lu/

[16] Chocolatey Software. (n.d.). Chocolatey. Dostupné z https://chocolatey.org/

[17] Microsoft. (n.d.). Windows Package Manager (winget). Microsoft Learn. Dostupné z https://learn.microsoft.com/en-us/windows/package-manager/winget/

[18] Debian. (n.d.). APT. Debian Wiki. Dostupné z https://wiki.debian.org/Apt

[19] Microsoft. (n.d.). System Center. Microsoft. Dostupné z https://www.microsoft.com/en-us/system-center

[20] Microsoft. (n.d.). Windows Server Update Services (WSUS). Microsoft Learn. Dostupné z https://learn.microsoft.com/en-us/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus

[21] SolarWinds. (n.d.). Patch Manager. SolarWinds. Dostupné z https://www.solarwinds.com/patch-manager

[22] Ivanti. (n.d.). *Patch for Endpoint Manager*. Dostupné z: https://www.ivanti.com/products/patch-for-endpoint-manager?utm_source=chatgpt.com

[23] Holm Security. (n.d.). What are internet-facing assets? Holm Security. Dostupné z https://support.holmsecurity.com/knowledge/what-are-internet-facing-assets

[24] Wiz. (n.d.). Internal vulnerability scanning. Wiz. Dostupné z https://www.wiz.io/academy/vulnerability-management/internal-vulnerability-scanning

[25] Intruder. (n.d.). Authenticated scanning. Intruder. Dostupné z https://www.intruder.io/glossary/authenticated-scanning

[26] U.S. General Services Administration. (2023, 13. marec). *Vulnerability management process (CIO-IT Security-17-80 Rev. 4)*. Dostupné z https://www.gsa.gov/system/files/Vulnerability-Management-Process-%5BCIO-IT-Security-17-80-Rev-4%5D-03-13-2023.pdf

[27] GÉANT. (n.d.). *Vulnerability training*. GÉANT Security. Dostupné z https://security.geant.org/vulnerability-training/

[28] European Union Agency for Cybersecurity. (2025, jún). *NIS2 technical implementation guidance: On Commission Implementing Regulation (EU) 2024/2690 — Technical and methodological requirements of cybersecurity risk-management measures* (Verzia 1.0). Publications Office of the European Union. Dostupné z: https://doi.org/10.2824/2702548

[29] EUVD (European Vulnerability Database). Dostupné z: https://euvd.enisa.europa.eu/