Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Bezpečnostné riešenia na ochranu koncových zariadení

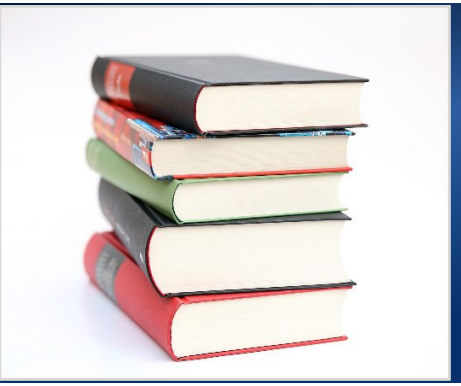
Ochrana koncových zariadení (Blok IV)

Kurz: Špecialista kybernetickej bezpečnosti vo verejnej správe

Martin Kontšek

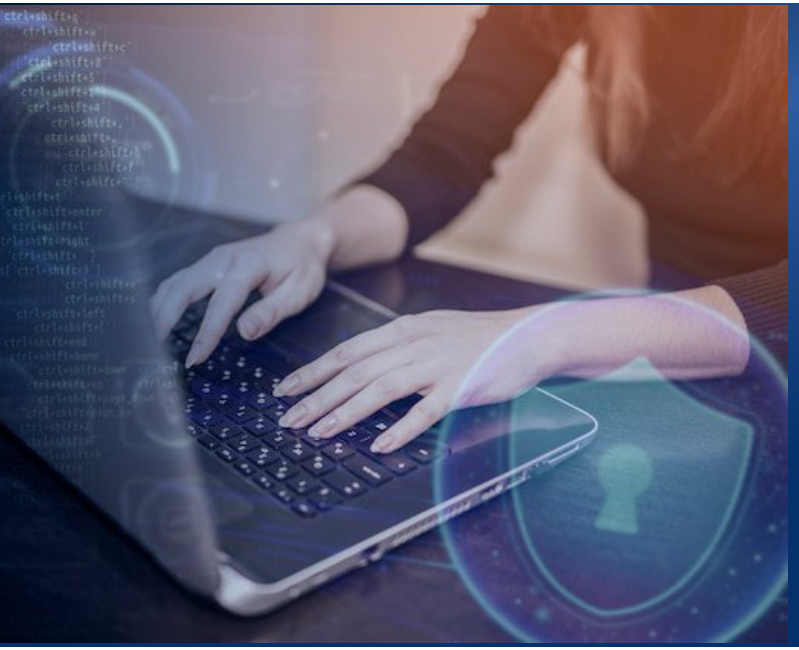
KC KYB UNIZA, https://kc.uniza.sk/

martin.kontsek@uniza.sk



Obsah

- Antimalvérová ochrana
- Host-based Intrusion Prevention Systems (HIPS)
- Endpoint Detection and Response (EDR)
- Extended Detection and Response (XDR)
- Hardening systémov a aplikácií



Antimalvérová ochrana

Antimalvérová ochrana

- Malvér
  - škodlivý softvér, ktorý ohrozuje bezpečnosť systému
- Antimalvér
  - softvér na detekciu, blokovanie a odstránenie malvéru
  - Detekcia zvyčajne pomocou signatúr
- Windows má vstavanú ochranu
  - Microsoft Defender Antivirus

Typ	Popis	Príklad
Ransomvér	Šifruje súbory, žiada výkupné	WannaCry
Trójsky kôň	Vydáva sa za legitímny softvér	Emotet
Spyware	Sleduje aktivitu používateľa	Agent Tesla
Rootkit	Skrýva prítomnosť malvéru	ZeroAccess
Adware	Zobrazovanie reklám	Fireball

Najčastejšie typy malvéru

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

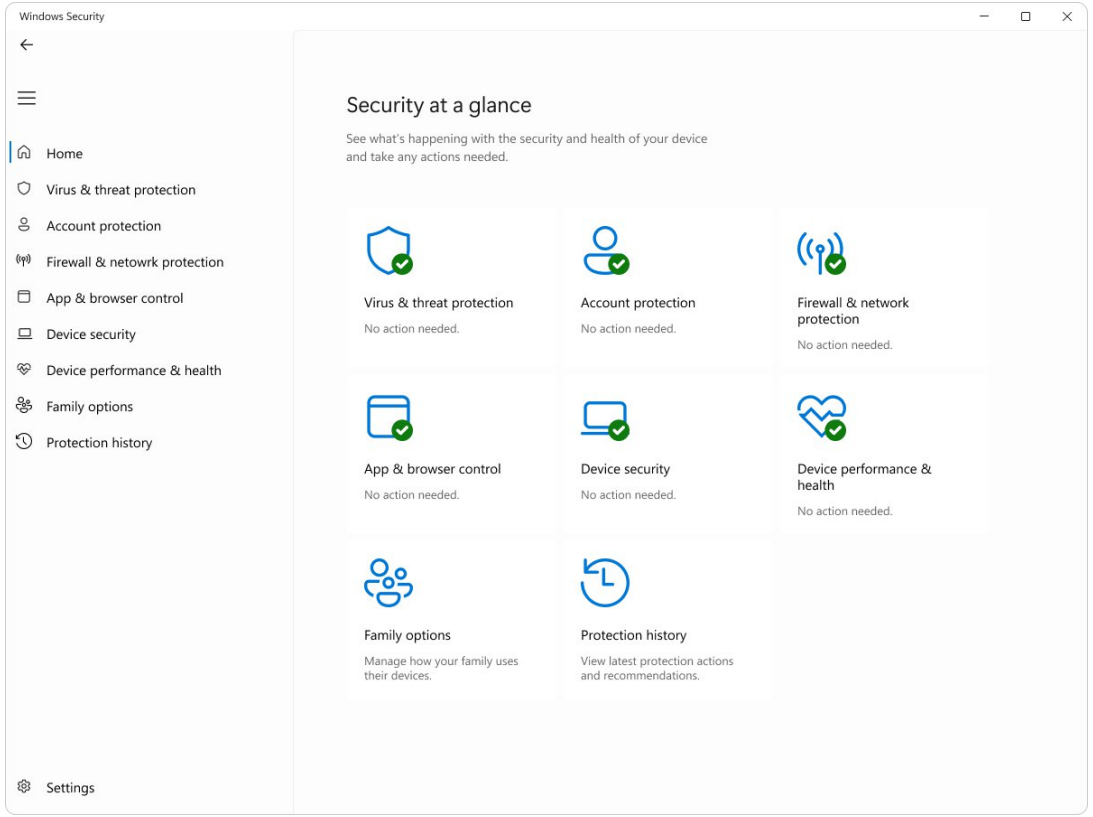
Ďalšie antimalvér nástroje pre Windows

- ESET NOD32 Antivirus
  - Ochrana v reálnom čase, detekcia malvéru a ransomware
- Norton AntiVirus
  - Ochrana v reálnom čase, detekcia malvéru a ransomware
- Kaspersky Standard Antivirus
- Bitdefender Antivirus Free
  - Ochrana v reálnom čase, detekcia malvéru, nízka záťaž systému.
- Avira Free Security
  - Antivírus, VPN (obmedzená), správca hesiel, ochrana webu.
- Malwarebytes Free
  - Manuálne skenovanie malvéru, adware, spyware.
- AVG AntiVirus Free
  - Ochrana pred vírusmi, škodlivými webmi, e-mailovými hrozbami.
- ClamWin
  - Open-source, manuálny vírus skener

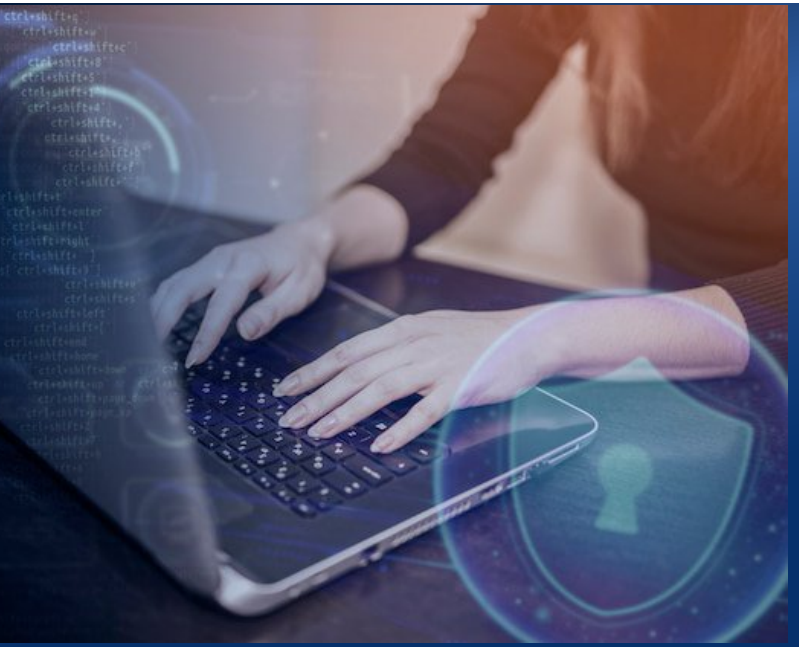
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Odporúčania pre antimalvér

- Aktivovať real-time ochranu v Defenderi
- Pravidelne aktualizovať Windows a Defender
- Nepoužívať viacero antimalvér programov naraz
- Vykonávať pravidelné skeny



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE



Host-based Intrusion Prevention Systems (HIPS)

Hostiteľský systém na prevenciu narušenia (HIPS)

- Host-based Intrusion Prevention System
- Monitoruje správanie aplikácií a systémových procesov (behaviorálna analýza)
- Detekuje pokusy o narušenie systému
- Vo Windows je HIPS súčasťou niektorých bezpečnostných balíkov

Funkcia	Antimalvér	HIPS
Detekcia známych hrozieb	áno	nie
Detekcia neznámych hrozieb	čiastočne	áno
Reakcia na správanie	nie	áno
Ochrana pred zero-day útokmi	čiastočne	áno

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ako HIPS funguje

- Sleduje
  - Zmeny v registroch (Windows)
  - Monitorovanie systémových volaní a procesov
  - Pokusy o modifikáciu systémových súborov
  - Neštandardné sieťové spojenia
  - Spúšťanie neautorizovaných procesov
  - Behaviorálna analýza aplikácií

- Reaguje
  - Blokovaním
  - Upozornením
  - Logovaním

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

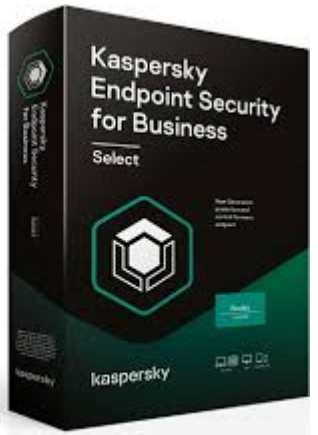
Kľúčové funkcie HIPS

- Detekcia exploitov na úrovni hosta
- Ochrana pred buffer overflow útokmi
- Kontrola prístupu k systémovým zdrojom
- Prevencia neautorizovaných zmien v registri alebo konfigurácii

- Výhody:
  - Ochrana pred útokmi, ktoré obchádzajú sieťové IPS
  - Zníženie rizika zero-day exploitov
  - Granulárna kontrola nad aplikáciami
- Nevýhody:
  - Vyššia záťaž na systémové zdroje
  - Potreba detailnej konfigurácie
  - Možné falošné pozitívne detekcie

Príklady HIPS riešení pre Windows

- ESET Internet Security
  - Antimalvér, HIPS, firewall
- Comodo Internet Security
  - Antimalvér, HIPS, firewall, sandbox
- Kaspersky Endpoint Security
  - Antimalvér, HIPS, firewall
- Microsoft Defender Exploit Guard
  - HIPS
- Symantec Endpoint Protection



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

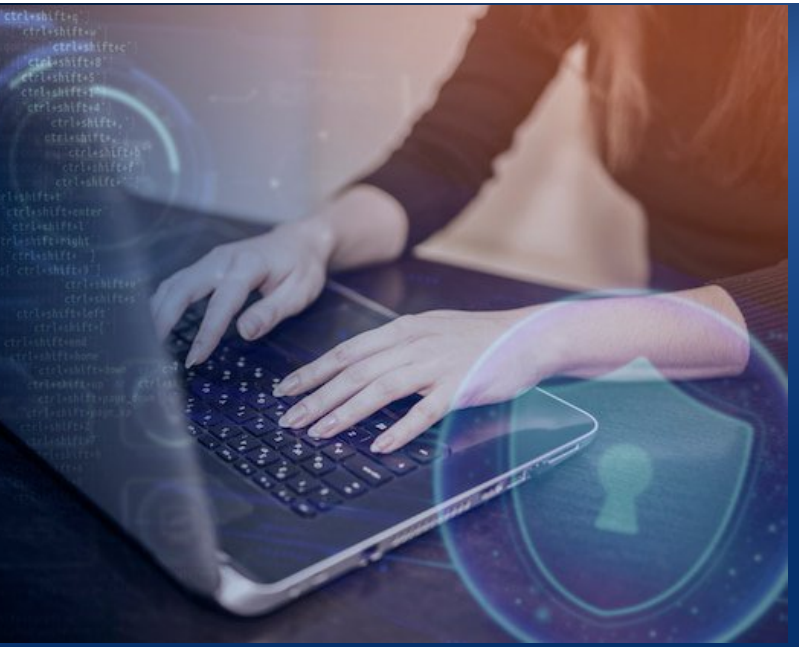
Príklady HIPS riešení pre Linux

- SELinux (Security-Enhanced Linux)
  - Mandatory Access Control (MAC) na úrovni jadra.
- AppArmor
  - Profilová ochrana aplikácií.
- OSSEC
  - Host-based IDS/IPS s kontrolou integrity súborov.

Odporúčania pre HIPS

- Používať HIPS v kombinácii s Defenderom alebo iným antimalvérom
- Prispôsobiť pravidlá podľa typu používateľa (domáci vs. firemný)
- Monitorovať logy a incidenty
- Testovať kompatibilitu s aplikáciami
- Vzdelávať používateľov o reakciách systému
- Integrácia s SIEM systémami
- Monitorovanie falošných pozitívnych detekcií

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE



Endpoint Detection and Response (EDR)

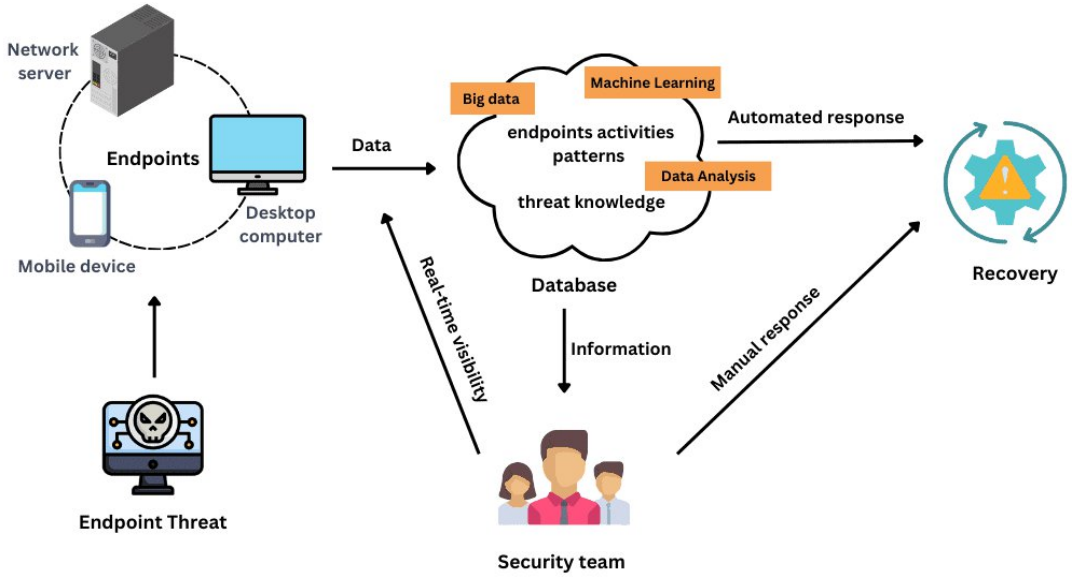
Čo je EDR

- Endpoint Detection and Response (EDR) je bezpečnostná technológia zameraná na monitorovanie, detekciu a reakciu na hrozby na koncových zariadeniach (endpointoch)
- Hlavné ciele EDR
  - Detekcia: Identifikácia podozrivých aktivít na zariadeniach
  - Analýza: Zhromažďovanie dát pre pochopenie útoku
  - Reakcia: Automatizované alebo manuálne kroky na zastavenie hrozby
  - Prevencia: Zníženie rizika budúcich útokov
- Rozdiel oproti HIPS
  - Vylepšenie HIPS o centrálne vyhodnocovanie hrozieb

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Kľúčové funkcie EDR a architektúra

- Kontinuálne monitorovanie endpointov
- Zber a korelácia dát (procesy, sieťová aktivita, súbory)
- Behaviorálna analýza
- Incident Response (izolácia zariadenia, odstránenie malvéru)
- Integrácia so SIEM



- Architektúra
  - Agent na endpointe: Zbiera dáta o aktivitách.
  - Cloudová alebo lokálna platforma: Analyzuje dáta, aplikuje pravidlá.
  - Dashboard: Prehľad incidentov, reporty, reakcie.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Výhody a nevýhody EDR

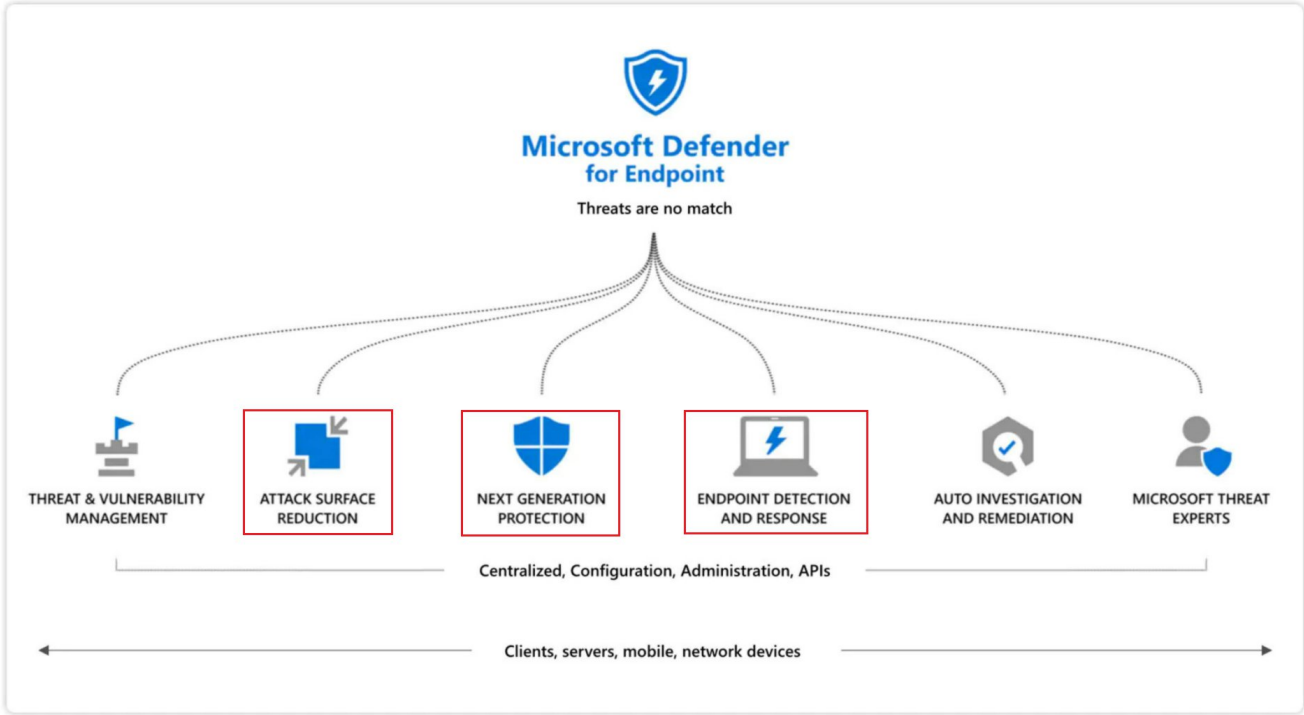
- Výhody:
  - Rýchla detekcia pokročilých hrozieb.
  - Zníženie času na reakciu (MTTR).
  - Lepšia viditeľnosť nad koncovými zariadeniami.
  - Podpora forenznej analýzy.

- Nevýhody:
  - Vyššie náklady na implementáciu.
  - Potreba odborného personálu.
  - Možné falošné pozitívne detekcie.
  - Závislosť na správnej konfigurácii.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

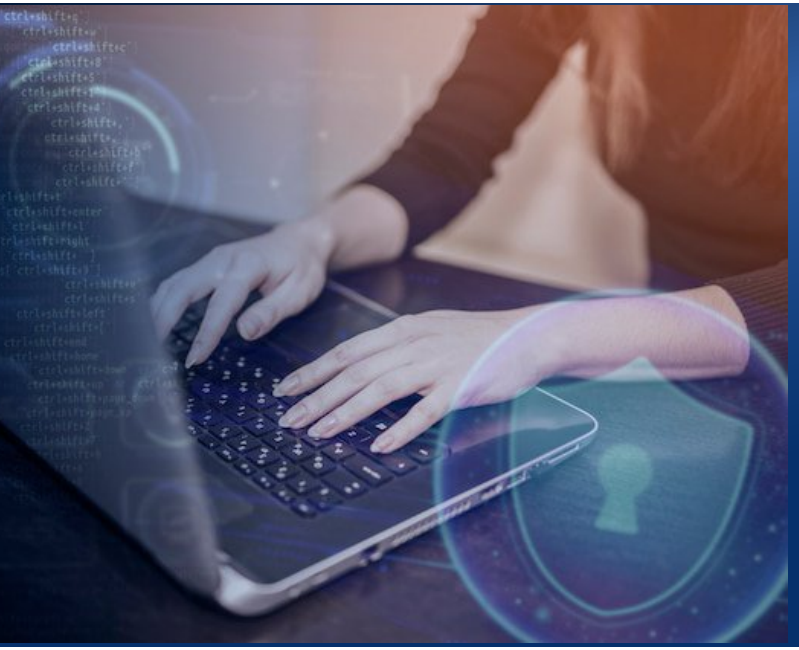
Príklady EDR riešení

- Microsoft Defender for Endpoint
- CrowdStrike Falcon
- SentinelOne
- Sophos Enpoint Intercept X



SentinelOne™

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE



Extended Detection and Response (XDR)

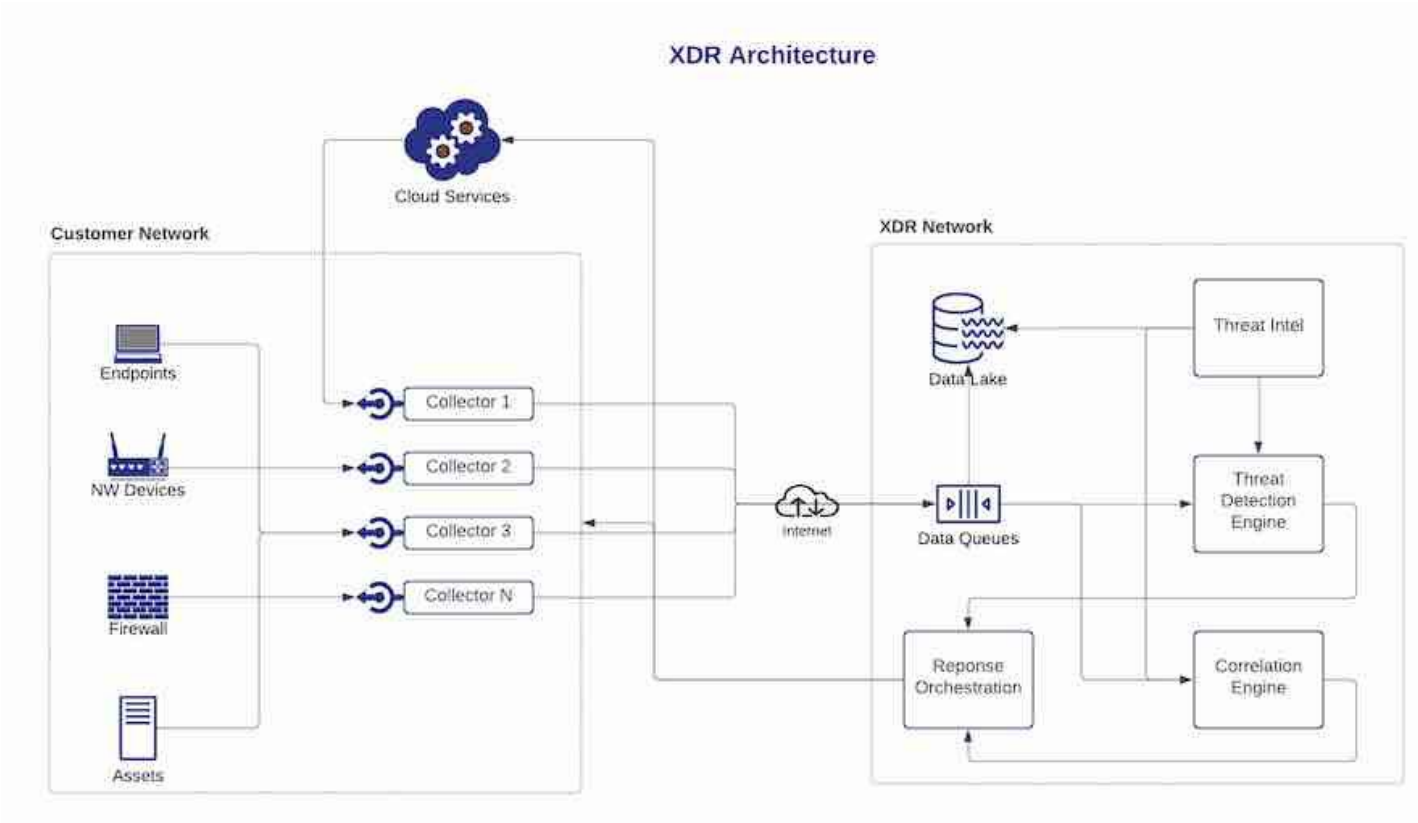
XDR

- Extended Detection and Response (XDR) je pokročilá bezpečnostná platforma, ktorá integruje detekciu a reakciu naprieč viacerými vrstvami – endpointy, sieť, e-mail, cloud
- Prečo vzniklo XDR:
  - EDR rieši iba endpointy
  - Potreba centralizovanej viditeľnosti a automatizácie
- Hlavné ciele XDR:
  - Konsolidácia dát z viacerých zdrojov
  - Pokročilá korelácia udalostí
  - Centralizovaná viditeľnosť naprieč infraštruktúrou
  - Automatizovaná reakcia na incidenty (izolácia, blokovanie, odstránenie)
  - Zníženie času na detekciu a reakciu (MTTD, MTTR)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Architektúra XDR

- Zdroje dát:
  - Endpointy (EDR)
  - Sieťové zariadenia (NDR)
  - Cloudové služby
  - E-mailové brány
- Analytická vrstva:
  - AI/ML na koreláciu a detekciu.
- Reakčná vrstva:
  - Automatizované playbooky.



Výhody a nevýhody XDR

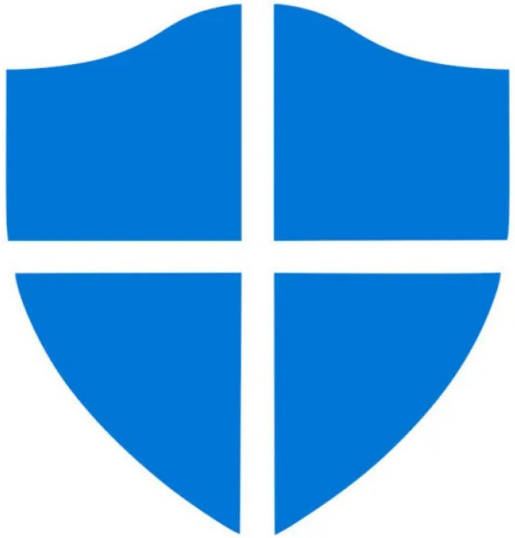
- Výhody:
  - Zníženie komplexity bezpečnostných riešení
  - Lepšia detekcia pokročilých hrozieb
  - Rýchlejšia reakcia na incidenty
  - Nižšie náklady oproti viacerým samostatným riešeniam

- Nevýhody:
  - Vyššie náklady na implementáciu
  - Potreba integrácie s existujúcimi systémami
  - Závislosť na jednom dodávateľovi (vendor lock-in)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Príklady XDR riešení

- Microsoft Defender XDR
- Palo Alto Cortex XDR
- Trend Micro Vision One
- SentinelOne Singularity XDR



paloalto NETWORKS

CORTEX XDR

TREND MICRO
Vision One

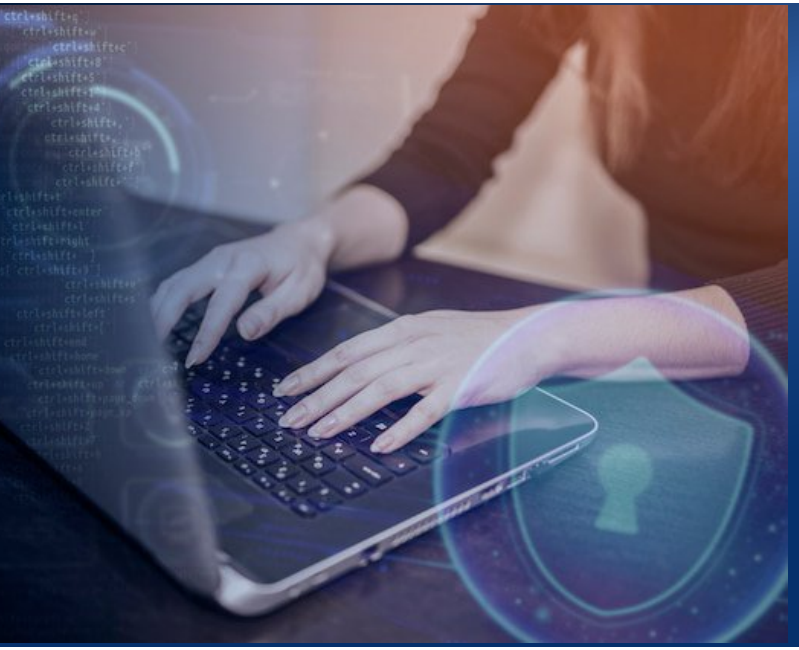
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Odporúčania a budúci vývoj

- Začať s integráciou existujúcich EDR/NDR riešení
- Využiť automatizované playbooky
- Monitorovať efektivitu korelácie a reakcií
- Školenie tímu na incident response

- Využitie generatívnej AI na prediktívnu analýzu
- Lepšia integrácia s Zero Trust architektúrou
- Rozšírenie na IoT a výrobné prostredia

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE



Hardening systémov a aplikácií

Čo je hardening

- súbor techník, osvedčených postupov a nástrojov za účelom **zníženia zraniteľnosti** v aplikáciách, infraštruktúre, firmvéri a iných oblastiach
- Podľa NIST:
  - „Hardening je proces **eliminácie prostriedkov útoku** opravením zraniteľností a vypnutím nepodstatných služieb.“
- Súčasťou je
  - zakázanie oprávnení, portov, vymazanie nepotrebných aplikácií, používateľských účtov a ďalších funkcií,
  - čo má za dôsledok **zosilnenie systému**, takže útočníci majú menšiu šancu získať prístup k citlivým informáciám počítačového systému.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Všeobecné princípy hardeningu

- Šifrovanie všetkej citlivej komunikácie.
- Spúšťanie iba nevyhnutných aplikácií.
- Rozloženie služieb na odlišné servery.
- Prideľovanie minimálnych prístupových práv.
- Časté aktualizácie systému.
- Používanie whitelistu namiesto blacklistu.
- Implementácia IDS/IPS a antivírusov.
- Auditné záznamy – ukladanie a analýza.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Výhody hardeningu

- Vyššia miera bezpečnosti
  - zníženie rizika, že systém sa stane obeťou kybernetických útokov
- Väčšia efektivita systému
  - zvýšenie výkonu zariadenia alebo infraštruktúry a menšie riziko prevádzkových problémov
- Dlhodobé úspory
  - ušetríme financie, ktoré by boli nevyhnuté na
    - obnovu po havárií
    - strata reputácie
    - pokuty... GDPR, a iné

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Typy hardeningu

Týka sa všetkého, čo útočník môže využiť na preniknutie do systému

1. Hardening harvéru
2. Hardening operačného systému
3. Hardening aplikácií
4. Hardening siete

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Hardening hardvéru (server, PC)

- Fyzické zabezpečenie systému
- Vypnutie nepotrebných HW zariadení (USB porty, Wi-Fi)
- Vypnutie USB portov počas zavádzania systému
- Zapnutie UEFI Secure Boot
- Heslo správcu do UEFI/BIOS
- Heslo pre bootloader
- Zašifrovanie pevného disku s operačným systémom
- Pravidelná aktualizácia UEFI/BIOS a mikrokódu procesora a OOB manažmentu
- Pravidelná obmena nepodporovaného hardvéru
- Nákup hardvéru z overených zdrojov (Trusted Supply Chain)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Hardening operačného systému

- Pravidelná aktualizácia
- Používanie len podporovaného OS
- Offline inštalácia: Nepripájať systém na internet pred nastavením firewallu
- Rozdelenie partícií: systém a dáta zvlášť
- Základná sieťová konfigurácia: Vypnúť DHCP a IPv6, ak nie sú potrebné.
- Odinštalovanie nepotrebných aplikácií prípadne ovládačov (zakázanie/vypnutie)
- Riadenie prístupu
  - Nastavenie vlastných rolí pre používateľov a použite silných hesiel
  - Nastavenie oprávnení podľa potreby
  - Vymazanie neaktívnych používateľov
  - Nepoužívať účet root, ktorý má silné oprávnenia na bežnú prácu
  - Obmedzenie počtu členov v skupinách správcov

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Hardening operačného systému (2)

- Firewall aj v OS
  - Povoliť iba potrebné porty (SSH, HTTP/HTTPS, DNS, NTP).
  - Blokovať všetky ostatné spojenia.
  - IDS/IPS
  - Limitovať pokusy na vzdialené pripojenie
  - Adaptívny firewall - Automaticky blokuje podozrivé IP adresy na základe logov
- Pravidelná údržba a audit
  - Auditné záznamy: /var/log/syslog, /var/log/auth.log – nastaviť len na pridanie, nie vymazanie
  - Automatizované spracovanie logov: Logwatch, Splunk.
  - Centralizácia logov
  - Synchronizácia času: NTP daemon – kritické pre korektné logy.
- Blokovanie zmien DNS konfigurácie v OS
- Overený zdroj aktualizácii OS
- Hardening vzdialeného prístupu SSH
  - Zakázať root login, zmeniť port, povoliť len kľúče nie heslá, obmedziť prístup na konkrétnych používateľov

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Hardening OS - ochrana jadra Linuxu

- Kernel lockdown
  - Mechanizmus, ktorý obmedzuje prístup používateľského priestoru k funkciám jadra, ktoré by mohli ohroziť integritu systému.
  - Zavedený v Linuxe od verzie 5.4 ako súčasť bezpečnostných opatrení.
  - Zabraňuje eskalácii privilégií cez zneužitie rozhraní jadra.
  - Chráni pred útokmi, ktoré obchádzajú bezpečnostné mechanizmy (napr. Secure Boot).
    - Integrity mode: Blokuje akcie, ktoré by mohli meniť jadro (napr. zápis do /dev/mem).
    - Confidentiality mode: Navyše blokuje čítanie citlivých údajov z jadra (napr. kryptografické kľúče).
  - Súvisiace opatrenia:
    - Aktivovať NX/XD bit v BIOS/UEFI (blokovanie spustenia kódu v dátových oblastiach).
    - Zakázať nepotrebné moduly jadra (blacklist v /etc/modprobe.d/).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Hardening OS - ochrana jadra Linuxu (2)

- SELinux (Security-Enhanced Linux)
  - Implementuje Mandatory Access Control (MAC).
  - Politiky definujú, čo procesy môžu robiť.
  - Režimy: Enforcing, Permissive, Disabled.
  - Odporúčanie: Používať Enforcing mode na produkcii.

- AppArmor
  - Alternatíva k SELinuxu, jednoduchšia konfigurácia.
  - Funguje na princípe profilov aplikácií.
  - Režimy: Enforce (vynucuje), Complain (len loguje).

- ASLR (Address Space Layout Randomization)
  - Náhodné rozmiestnenie pamäťových oblastí (stack, heap, knižnice).
  - Znižuje úspešnosť exploitov typu buffer overflow.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Hardening OS – Windows 11

- Zapnúť automatické aktualizácie OS, ovládačov a aplikácií, kontrola histórie aktualizácií
- Antivírusová ochrana (Full scan, Offline scan, Periodické skeny), Ransomware Protection
- Zapnúť Microsoft Defender Firewall pre všetky siete. Možnosť doplniť o FW tretích strán
- Silné autentifikačné metódy - Windows Hello (biometria, PIN), Microsoft účet
- Šifrovanie dát - BitLocker, dešifrovací kľúč na bezpečné miesto
- Ochrana pred škodlivým SW - Reputation-based protection, aplikácie len z dôveryhodných zdrojov
- Vypnúť File & Printer Sharing, zakázať AutoPlay pre USB zariadenia
- Nastaviť Privacy & Security (kamera, mikrofón, poloha) v prehliadači
- Aktualizovať prehliadač, používať rozšírenia len z dôveryhodných zdrojov
- Nastaviť User Account Control na vysokú úroveň, kontrolovať aplikácie po štarte
- Zálohovanie dát - Vytvárať system image backup a inkrementálne zálohy na offline úložisko

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Hardening softvérových aplikácií

- sústreďuje už na konkrétne aplikácie, bežiace v danom operačnom systéme

- Aktualizácia a automatická oprava aplikácií, vrátane aplikácií tretích strán
- Používanie firewall a ďalších programov zameraných na ochranu voči malwaru, spywaru, ...
- Zašifrovanie údajov
- Odstrániť alebo vypnúť nepotrebné moduly (napr. CGI v Apache)
- Každá služba musí bežať pod vlastným používateľom, nikdy ako root
- Zapnúť auditné záznamy, sledovať prístupové logy
- Testovať konfigurácie pred nasadením do produkcie
- Odizolovať aplikácie (napr. kontajnery)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Hardening databáz

- dôležité informácie organizácie
- na prístup k databáze – zväčša vzdialený prístup, DBMS
- zabezpečiť svoju databázu aj systém správy databáz (DBMS)
- ale aj vhodnou implementáciou bezpečnostných opatrení
  - … OS dáva povolenia iným aplikáciám na vykonanie určitých zmien v systéme

Hardening zahŕňa tieto procesy:

- Použitie komplexných hesiel na prístup
- Ak sa zistí podozrivá aktivita pri prihlasovaní, tak je potrebné uzamknúť účet
- Šifrovanie údajov
- Vypnutie nepotrebných funkcií a služieb
- Pravidelná aktualizácia DBMS

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

Hardening web servera

- nesprávna konfigurácia zvyšuje riziko útokov (XSS, MITM, Directory Traversal)
- Skrytie informácií o verzii
- Vypnutie Directory Listing
- Zapnúť SSL/TLS a HSTS
- Bezpečnostné hlavičky
  - HttpOnly a Secure, X-Frame-Options, X-XSS-Protection
- Obmedzenie metód - Povoliť iba GET a POST
- Vypnúť nepotrebné moduly
- Povoliť logovanie (ErrorLog, CustomLog)
- Spúšťať web server pod samostatným používateľom
- Nastaviť prísne oprávnenia (napr. chmod 750)
- Pravidelné aktualizácie a skeny zraniteľností

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Hardening siete

- monitorovať a hlásiť podozrivé aktivity v danej sieti
  - čo pomáha administrátorom zabrániť neoprávnenému prístupu do siete

Techniky zahŕňajú:

- Použitie VPN alebo reverzného proxy na pripojenie
- Správne nastavenie sieťových firewallov, IDS/IPS
- Kontrola privilégií prístupu k sieti a pravidiel v sieti
- Zakázanie nepotrebných alebo nepoužívaných sieťových portov
- Zašifrovanie sieťovej prevádzky
- Zakázanie sieťových služieb a zariadení, ktoré nie sú využívané v sieti
- Zakázať nezabezpečené protokoly, ako sú SMBv1, Telnet a http

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Benchmark pre hardening

- stanoviť si základnú líniu
  - zabezpečený stav systému, ktorý by sme sa mali snažiť dosiahnuť
  - Potom už len sledovať odchýlky
  - Zväčša pomocou benchmarku
    - súbor najlepších bezpečnostných postupov poskytovaných expertmi v oblasti KB
      - NIST (National Institute of Standards and Technology)
      - CIS (Center of Internet Security, https://learn.cisecurity.org/benchmarks)
      - Výrobcovia...
    - akceptované vládou, obchodom, priemyslom a akademickou obcou
    - konkrétne:
      - najskôr vykonať hodnotenie systému, pre ktorý chceme aplikovať systém hardening
        - ako sa súčasná konfigurácia zhoduje s relevantným CIS benchmarkom
        - často sú dostupné nástroje na automatické testovanie systému
      - potom nakonfigurovať systém, ktorý bude spĺňať bezpečnostné odporúčania

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Lynis

- Lynis
  - jeden z najdôveryhodnejších nástrojov automatického auditu na správu softvérových záplat, skenovanie škodlivého softvéru a detekciu zraniteľností
  - určený pre systémy Linux, macOS, BSD
  - na skenovanie systému, či neobsahuje
    - základné bezpečnostné zraniteľnosti
    - chyby v konfigurácii
    - používateľské účty bez hesla
    - neoprávnené povolenia k súborom
    - audit brány firewall atď.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ubuntu Security Guide

- Nástroj od Canonical na automatizovaný hardening a auditovanie Ubuntu systémov
- Zjednodušuje aplikáciu bezpečnostných štandardov ako:
  - CIS Benchmarks (Center for Internet Security)
  - DISA-STIG (Defense Information Systems Agency Security Technical Implementation Guide)
- Ručný hardening podľa stovky odporúčaní je časovo náročný
- USG poskytuje automatizované skripty na aplikáciu pravidiel a kontrolu compliance
- Možnosť výberu profilov podľa prostredia
  - CIS level1, 2, workstation, server
- Podľa výsledkov auditu umožňuje automatické nasadenie opráv

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

Bezpečnostné riešenia na ochranu koncových zariadení

Ochrana koncových zariadení (Blok IV)

Kurz: Špecialista kybernetickej bezpečnosti vo verejnej správe

Martin Kontšek

KC KYB UNIZA, https://kc.uniza.sk/

martin.kontsek@uniza.sk