Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Monitorovanie a riešenie incidentov

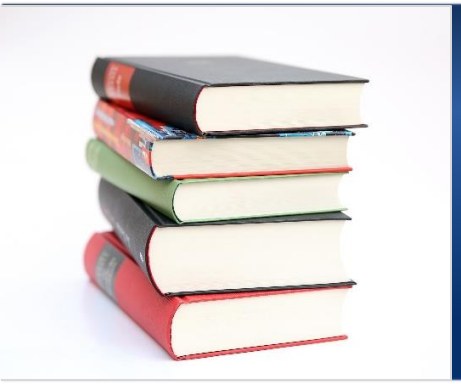
Autorizácia, monitorovanie a riešenie incidentov (Blok IV)

Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti

Ing. Martin Kontšek, PhD.

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

martin.kontsek@uniza.sk



Obsah

- Prečo je dôležité chrániť svoju digitálnu identitu
- Dôsledky odcudzenia identity
- Ako zabrániť neoprávnenému prístupu
- Metódy monitorovania prístupu
- Postupy pri riešení bezpečnostných incidentov
- Integrácia AAA mechanizmov do systémov a aplikácií vo verejnej správe

Prečo je dôležité chrániť svoju digitálnu identitu, dôsledky odcudzenia identity, ako zabrániť neoprávnenému prístupu

Prečo je dôležité chrániť digitálnu identitu

- Digitálna identita predstavuje všetky informácie, ktoré o sebe zdieľame online – od e-mailových adries, prihlasovacích údajov, cez fotografie až po citlivé údaje ako čísla účtov či rodné číslo.
- Ak sa tieto údaje dostanú do nesprávnych rúk, môžu byť zneužité na podvodné účely, čo môže mať vážne finančné aj osobné následky.
- Ochrana digitálnej identity je preto základom bezpečného pohybu v online prostredí. Pomáha predchádzať krádežiam, podvodom, strate dôveryhodnosti a chráni naše súkromie.

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

Dôsledky odcudzenia identity

Odcudzenie identity môže mať rôzne formy a následky:

- **Finančné straty:** Útočníci môžu vykonávať neoprávnené transakcie, vyberať peniaze z účtov alebo žiadať pôžičky na vaše meno.
- **Krádež účtov:** Strata prístupu k e-mailu, sociálnym sieťam alebo pracovným účtom môže viesť k zneužitiu vašich kontaktov a dát.
- **Poškodenie reputácie:** Útočníci môžu predstierať, že ste vy, a šíriť škodlivý obsah alebo podvody.
- **Právne problémy:** Ak je vaša identita použitá na nelegálne aktivity, môžete čeliť vyšetrovaniu alebo právnym komplikáciám.

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

Ako zabrániť neoprávnenému prístupu

- **Silné heslá:** Používajte dlhé, jedinečné heslá pre každú službu a pravidelne ich meňte.
- **Dvojfaktorová autentifikácia (2FA):** Aktivujte ju všade, kde je to možné – pridáva ďalšiu vrstvu ochrany.
- **Aktualizácie a antivírus:** Pravidelne aktualizujte operačný systém, aplikácie a používajte spoľahlivý antivírusový program.
- **Opatrnosť pri zdieľaní údajov:** Nikdy nezdieľajte citlivé informácie cez nezabezpečené kanály a overujte si zdroje.
- **Pozor na phishing:** Neotvárajte podozrivé e-maily, odkazy alebo prílohy. Overujte si adresy webových stránok.

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

Metódy monitorovania prístupu

Význam logovania a analýzy logov

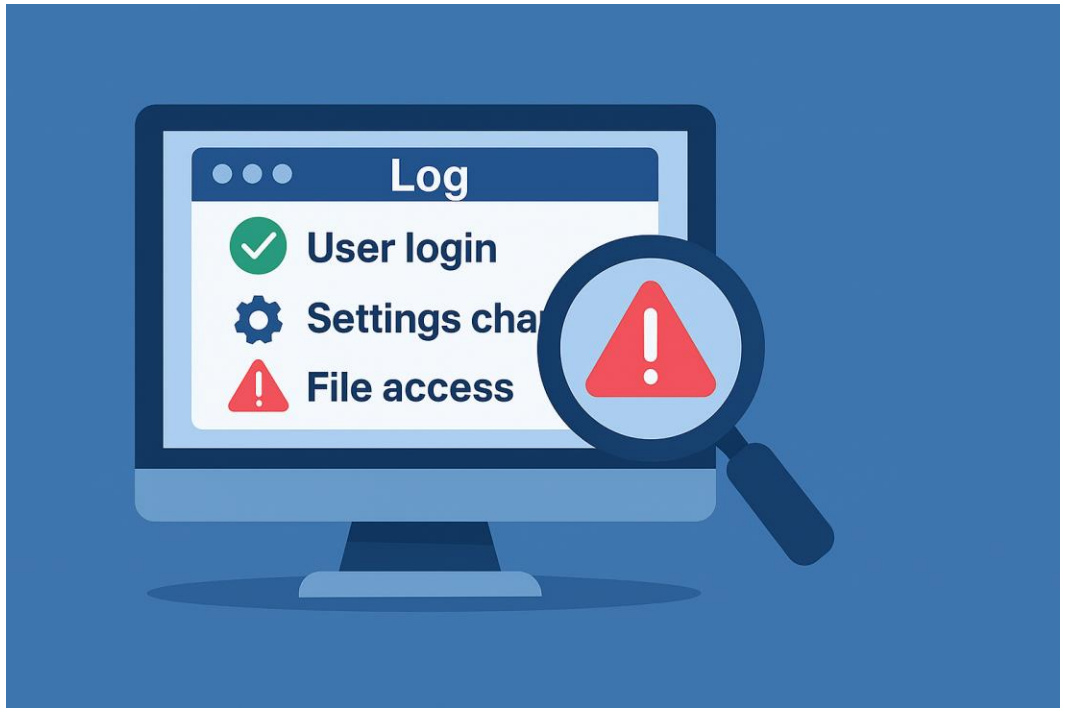
- Logovanie zaznamenáva všetky dôležité udalosti v systéme (prihlásenia, zmeny nastavení, prístup k súborom).
- Analýza logov pomáha odhaliť podozrivé aktivity a identifikovať neoprávnené prístupy.
- Bez logovania by bolo takmer nemožné spätne zistiť, čo sa stalo pri bezpečnostnom incidente.
- Logy sú kľúčové pre forenznú analýzu a dodržiavanie legislatívnych požiadaviek (napr. GDPR).

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

Bezpečnostné monitorovanie

Ako sa monitorujú systémy a prístupy:

- Prístupové záznamy a auditné logy sledujú, kto, kedy a odkiaľ pristupoval k systému.
- Monitorovanie zahŕňa aj sledovanie zmien konfigurácie a pokusov o prihlásenie.



Význam pravidelného logovania:

- Pomáha odhaliť potenciálne riziká (napr. opakované neúspešné prihlásenia).
- Umožňuje rýchlu reakciu na incidenty a minimalizáciu škôd.
- Slúži ako dôkazový materiál pri vyšetrovaní.

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

Úloha bezpečnostného špecialistu

- Sleduje prístupové záznamy a auditné logy v reálnom čase alebo prostredníctvom SIEM nástrojov (napr. Splunk, ELK).
- Hľadá anomálie, ako sú:
  - Neoprávnené prístupy
  - Prístupy z neznámych IP adries
  - Neobvyklé časy prihlásenia
- Vyhodnocuje riziká a prijíma opatrenia na ich elimináciu.

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

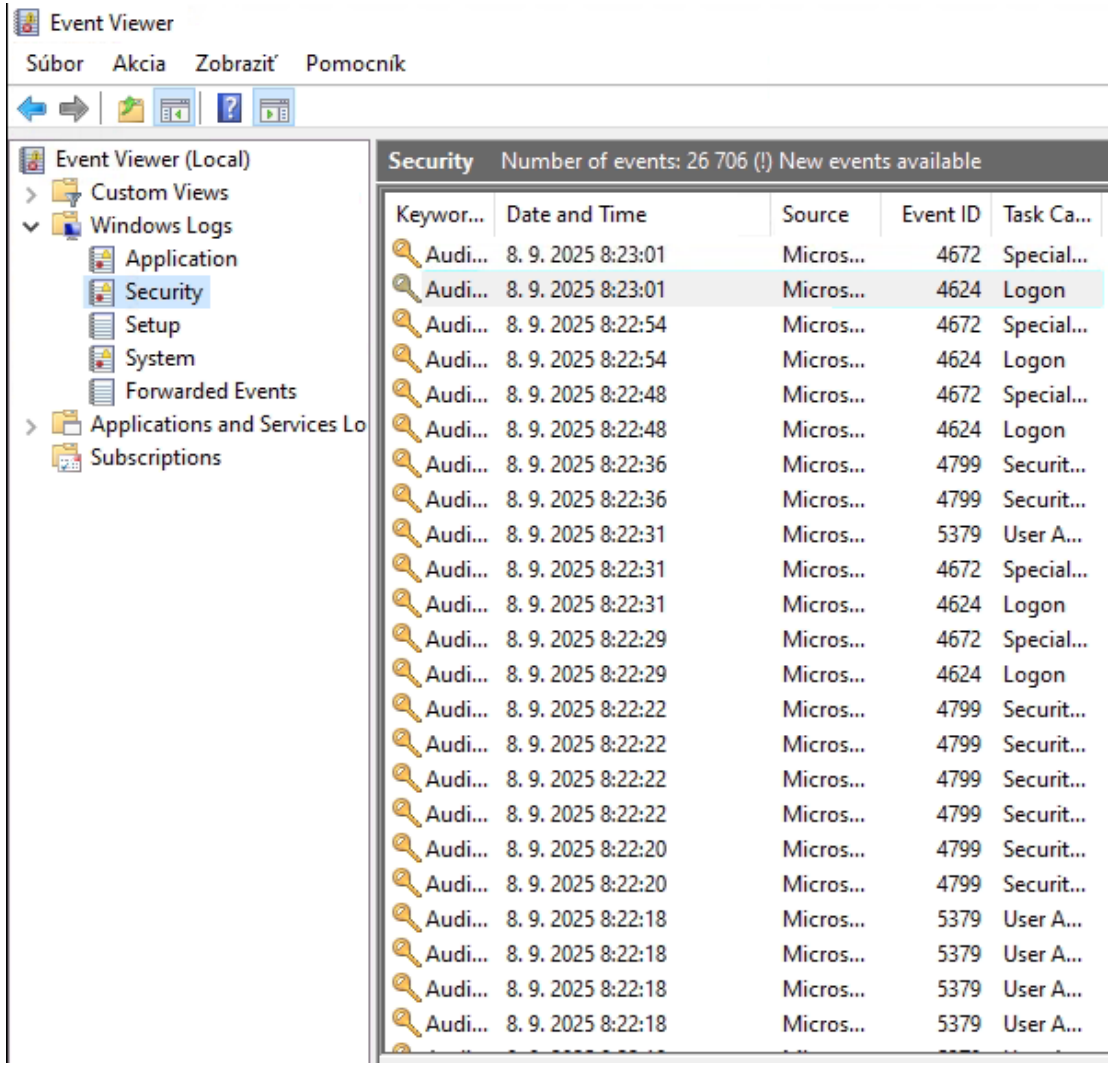
Čo sa stane, ak sa prístup nemonitoruje

- **Útočníci môžu zostať neodhalení celé mesiace**
  - Bez monitorovania si nevšimnete, že niekto používa váš účet alebo zariadenie.
  - Priemerný čas odhalenia útoku bez monitoringu môže byť viac ako 200 dní.
- **Riziko úniku dát a finančných strát**
  - Citlivé dokumenty, osobné údaje alebo firemné dáta môžu byť odcudzené.
  - Firmy môžu čeliť vysokým pokutám (napr. GDPR až do 20 miliónov €).
- **Poškodenie reputácie firmy alebo jednotlivca**
  - Únik dát môže spôsobiť stratu dôvery zákazníkov a partnerov.
  - Negatívne mediálne pokrytie môže mať dlhodobý dopad.
- **Ťažšie vyšetrovanie incidentov bez logov**
  - Ak sa niečo stane, bez záznamov nie je možné zistiť, čo sa presne udialo.
  - IT tím nemá dôkazy, kto, kedy a ako získal prístup.
- **Možnosť právnych problémov**
  - Nedodržanie legislatívnych požiadaviek (napr. GDPR, ISO 27001).
  - Riziko súdnych sporov zo strany klientov alebo partnerov.

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

Aktivita: Kontrola logov vo Windows

- Otvorte Event Viewer (Prehliadač udalostí):
  - Stlačte Win + R, napíšte eventvwr.msc a potvrďte.
- Skontrolujte kategórie vo Windows Logs:
  - Security – prihlásenia, odhlásenia, zmeny oprávnení
  - System – systémové udalosti
- Vyhľadávajte udalosti s ID:
  - 4624 – úspešné prihlásenie
  - 4625 – neúspešné prihlásenie
- Pravidelná kontrola pomáha odhaliť podozrivé aktivity.



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

Typy logov a ich význam

Systémové logy:

- Obsahujú informácie o chode operačného systému, chybách, aktualizáciách a reštartoch.
- Pomáhajú identifikovať problémy so stabilitou systému.

Aplikačné logy:

- Zaznamenávajú činnosť aplikácií, napr. chyby pri spustení alebo komunikácii so serverom.
- Umožňujú vývojárom a administrátorom riešiť problémy.

Bezpečnostné logy:

- Obsahujú údaje o prihláseniach, odhláseniach, zmenách oprávnení a pokusoch o prístup.
- Kľúčové pre detekciu neoprávnených aktivít.

Auditné logy:

- Detailné záznamy o činnostiach používateľov a administrátorov.
- Slúžia na forenznú analýzu a dodržiavanie noriem a nariadení (napr. GDPR, ISO 27001).

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

Najčastejšie indikátory podozrivých aktivít

- Opakované neúspešné prihlásenia: Môže ísť o brute force útok.
- Prihlásenia z neobvyklých lokalít: Napr. prístup z iného kontinentu.
- Zmeny oprávnení bez schválenia: Indikátor kompromitovaného účtu.
- Aktivita mimo pracovného času: Neobvyklé prihlásenia v noci alebo cez víkend.
- Neobvyklý objem prenesených dát: Možný únik dát (data exfiltration).

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

Príklady udalostí spúšťajúcich upozornenia podozrivej aktivity

- 5 neúspešných prihlásení z jedného účtu/IP v priebehu 10 min.
- Prihlásenie mimo bežných hodín pre bežného používateľa.
- Prístup správcu na koncové zariadenie mimo času údržby.
- Vymazanie Security logu na zariadení.
- Nové členstvo v privilegovanej skupine (napr. Administrators, Domain Admins).
- Neobvyklý objem prenesených dát z pracovnej stanice (možný únik dát).

Odporúčania pre logovanie z pohľadu GDPR

- Minimalizácia dát: logujte len nevyhnutné údaje (nie obsah dokumentov).
- Prístup len pre oprávnených: role-based access, audit prístupu k logom.
- Retenčná lehota: vopred definujte (napr. 90 dní operatívne, 1 rok archív).
- Pseudonymizácia/Hashing tam, kde to dáva zmysel.
- Transparentnosť: informujte používateľov, že sa udalosti logujú.

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

Odporúčané postupy pre zamestnancov

- Hlásenie podozrivých udalostí: Každý incident okamžite oznámte IT oddeleniu.
- Nepoužívajte administrátorské účty na bežnú prácu: Minimalizujte riziko zneužitia.
- Dodržiavajte politiku silných hesiel a 2FA: Znížite riziko neoprávneného prístupu.
- Nepoužívajte rovnaké heslo na viacerých stránkach.
- Buďte opatrní pri otváraní e-mailov a odkazov: Phishing je častý spôsob získania prístupu.
- Zamykajte počítač, keď odchádzate: Stlačte Win + L vždy, keď opustíte pracovisko.

Postupy pri riešení bezpečnostných incidentov

Prečo je dôležité mať definované postupy

- Minimalizácia škôd: Rýchla reakcia znižuje finančné a reputačné straty.
- Predchádzanie chaosu: Jasné úlohy a zodpovednosti pre všetkých.
- Legislatívne požiadavky: GDPR, ISO 27001, NIS2 vyžadujú Incident Response plán (plán krokov pri incidente).
- Zvýšenie dôvery: Partneri a zákazníci očakávajú pripravenosť.
- Zníženie stresu: Zamestnanci vedia, čo robiť, aj pod tlakom.

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

Čo obsahuje plán reakcie na incidenty

- Definícia incidentu: Čo sa považuje za incident (napr. únik dát, malware, phishing).
- Kontaktné osoby: Incident Response tím (IT, právne, PR).
- Postup krok za krokom: Detekcia → Izolácia → Analýza → Obnova → Poučenie.
- Komunikačný plán: Interná komunikácia + externá (zákazníci, médiá).
- Dokumentácia: Incident report, časová os, prijaté opatrenia.
- Pravidelné testovanie: Simulácie (table-top exercises).

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

Príklady incidentov na ktorých si ukážeme riešenie

- Phishing:
  - Zamestnanec klikne na škodlivý odkaz.
- Malware:
  - Infekcia po otvorení prílohy.
- Únik dát:
  - Nesprávne odoslaný e-mail s citlivými údajmi.
- Brute force útok:
  - Opakované pokusy o prihlásenie.
- Interné zneužitie:
  - Zamestnanec kopíruje dáta na USB.

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

Všeobecný postup riešenia incidentu

- Identifikácia: Zistiť, čo sa stalo (logy, alerty, hlásenia).
- Izolácia: Odpojiť zariadenie, zablokovať účet.
- Analýza: Určiť rozsah a príčinu.
- Eradikácia: Odstrániť hrozbu (malware, zraniteľnosť).
- Obnova: Obnoviť systémy do bezpečného stavu.
- Poučenie: Dokumentovať a aktualizovať politiky.

Najčastejšie chyby pri riešení incidentov

- Oneskorená reakcia: Čakanie na potvrdenie problému.
- Nedostatočná komunikácia: IT vie, ale manažment nie.
- Chýbajúca dokumentácia: Ťažké poučenie z incidentu.
- Mazanie dôkazov: Predčasné čistenie logov alebo zariadení.
- Žiadne školenia: Zamestnanci nevedia, čo hlásiť.

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

Príklad riešenia phishingového útoku

- Krok 1: Zamestnanec nahlási podozrivý e-mail.
- Krok 2: IT izoluje zariadenie a zablokuje účet.
- Krok 3: Skontroluje logy a SIEM alerty.
- Krok 4: Reset hesiel, zapnutie 2FA.
- Krok 5: Používateľ absolvuje školenie.

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

Príklad riešenia malware útoku

- Krok 1: Odpojiť zariadenie od siete.
- Krok 2: Spustiť antivírus a forenznú analýzu.
- Krok 3: Identifikovať zdroj infekcie.
- Krok 4: Vyčistiť alebo preinštalovať systém.
- Krok 5: Aktualizovať politiky a školenia.

Príklad riešenia úniku dát

Krok 1: Identifikácia

- Zistiť, aké dáta unikli (osobné údaje, finančné informácie, interné dokumenty).
- Overiť zdroj úniku (e-mail, cloud, USB, nesprávne nastavené oprávnenia).

Krok 2: Izolácia

- Zablokovať prístup k postihnutým účtom alebo systémom.
- Odpojiť zariadenia, ak je únik stále aktívny.

Krok 3: Analýza

- Určiť rozsah úniku (koľko záznamov, aké typy dát).
- Skontrolovať logy a SIEM alerty na zistenie príčiny.

Krok 4: Oznámenie

- Informovať interný Incident Response tím a manažment.
- Ak ide o osobné údaje, nahlásiť únik úradu (napr. GDPR do 72 hodín).
- Informovať dotknuté osoby, ak je to povinné.

Krok 5: Eradikácia a obnova

- Odstrániť príčinu (opraviť nastavenia, zaviesť šifrovanie, zmeniť heslá).
- Obnoviť systémy a zabezpečiť dáta.

Krok 6: Poučenie

- Dokumentovať incident (časová os, prijaté opatrenia).
- Aktualizovať politiky a školenia zamestnancov.

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

Príklad riešenia Brute Force útoku

Krok 1: Identifikácia

- Sledovať SIEM alebo logy.
- Indikátor: Veľké množstvo neúspešných pokusov z jednej IP alebo účtu.

Krok 2: Izolácia

- Dočasne zablokovať účet, ktorý je cieľom útoku.
- Zablokovať IP adresu útočníka na firewalle alebo IDS/IPS.

Krok 3: Analýza

- Overiť, či došlo k úspešnému prihláseniu po sérii pokusov.
- Skontrolovať, či útočník nezískal prístup k iným účtom.

Krok 4: Eradikácia

- Resetovať heslá postihnutých účtov.
- Zapnúť alebo resetovať dvojfaktorovú autentifikáciu (2FA).
- Skontrolovať politiky hesiel (minimálna dĺžka, komplexnosť).

Krok 5: Obnova

- Obnoviť normálnu prevádzku po potvrdení, že útok je zastavený.
- Monitorovanie systém pre opakované pokusy.

Krok 6: Poučenie

- Dokumentácia incident (čas, IP, účty, prijaté opatrenia).
- Aktualizácia pravidiel firewallu a SIEM alertov.
- Školenie zamestnancov o bezpečnosti hesiel.

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

Poučenie z útoku a ich prevencia

- Post-incident review: Čo fungovalo, čo zlyhalo.
- Aktualizácia postupov: Na základe skúseností.
- Školenia: Simulácie útokov (phishing testy).
- Technické opatrenia: Patch management, 2FA, zmena logického dizajnu siete (segmentácia).

Integrácia AAA mechanizmov do systémov a aplikácií vo verejnej správe

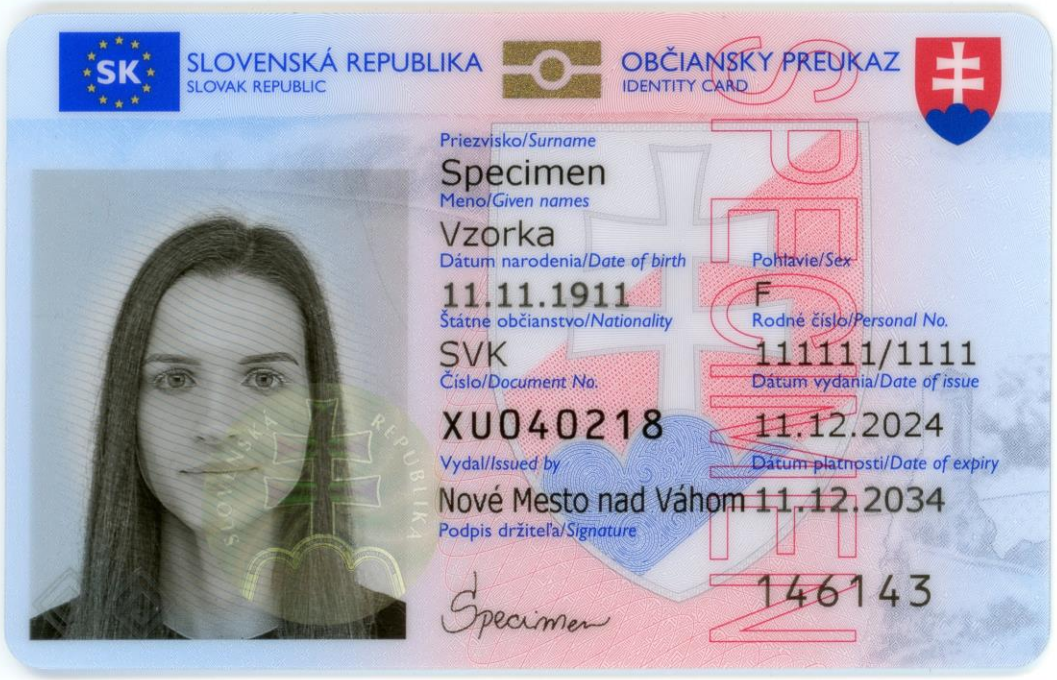
AAA mechanizmy

- Autentifikácia – overenie identity používateľa
- Autorizácia – určenie oprávnení používateľa
- Audit (accounting) – zaznamenávanie a kontrola aktivít, účtovanie

- Jednotné prihlásenie do viacerých systémov
- Rôzne metódy prihlásenia:
  - Heslá a PIN kódy
  - Biometria (odtlačky, rozpoznávanie tváre)
  - Elektronický občiansky preukaz (eID)
  - Dvojfaktorová autentifikácia (2FA)

Príklady použitia AAA vo verejnej správe

- Slovensko (Česko – NIA, Estónsko...): eID a autentifikácia do štátnych portálov



- Univerzita: jednotné prihlásenie do systémov
  - Osobné číslo/login + heslo (do niektorých systémov prihlásenie čipovou kartou)
  - Počítače, WiFi, email, Office, Teams, vzdelávanie, strava, rezervácia učební...
  - Len karta – vstup do budov a učební, vyberanie stravy, parkovanie
  - Podobne aj iné školy ako aj firmy

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

Monitorovanie a riešenie incidentov

Autorizácia, monitorovanie a riešenie incidentov (Blok IV)

Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti

Ing. Martin Kontšek, PhD.

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

martin.kontsek@uniza.sk