
RIADENIE KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV ZÁKLADY

ING. LUKÁŠ ŠURAB



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



KOMPETENČNÉ
CENTRUM
KYBERNETICKEJ
BEZPEČNOSTI

STU

SLOVENSKÁ TECHNICKÁ
UNIVERZITA V BRATISLAVE

OBSAH

1. **Úvod a definície:** Prečo je riadenie incidentov kritické? Čo je to incident?
2. **Životný cyklus riadenia incidentov:** Porovnanie rámcov (NIST, SANS, ISO 27035).
3. **Základné hrozby a ich identifikácia:** Malvér, phishing a slabé heslá.
4. **Prvá pomoc a prevencia pre používateľov:** Kroky pri útoku a bezpečnostné návyky.
5. **Príprava na incidenty v organizácii:** Plánovanie, školenia a zálohovanie.
6. **Dokumentácia a komunikácia:** Kľúč k úspešnej reakcii.
7. **Fáza po incidente:** Analýza príčin (RCA) a poučenie sa.
8. **Právne a regulačné požiadavky:** GDPR a NIS2.
9. **Záver a kľúčové poznatky.**

ÚVOD – PREČO JE TO DÔLEŽITÉ?

Všadeprítomné riziko v digitálnom svete

- Organizácie aj jednotlivci čelia neustále rastúcemu počtu kybernetických hrozieb.
- Hrozby siahajú od bežných phishingových kampaní až po sofistikované útoky sponzorované štátmi.
- Efektívne riadenie incidentov nie je len technickou požiadavkou, ale **kritickým obchodným imperatívom**.
- Cieľom je minimalizovať škody, urýchliť obnovu a ochrániť reputáciu organizácie.

INFORMAČNÉ AKTÍVA

Aktívum – niečo, čo má hodnotu, je pre spoločnosť užitočné pre kontinuitu alebo operatívu

- **Informačné aktíva:** DB, dokumentácie, manuály, materiály, havarijné plány, prevádzkové procedúry...
- **Papierová dokumentácia**
- **SW aktíva:** systémový/aplikačný softvér, vývojové nástroje, utility...
- **Fyzické aktíva:** počítače, pásky, disky, klimatizácia, nábytok, komunikačné zariadenia...
- **Ľudia:** zamestnanci, zákazníci, partneri, predplatitelia
- **Reputácia**
- **Služby:** kúrenie, osvetlenie, energie, výpočtové a komunikačné služby...

DEFINÍCIA KYBERNETICKÉHO BEZPEČNOSTNÉHO INCIDENTU

Čo je incident?

- Udalosť, ktorá **ohrozí** alebo **poškodí** aktívum.

Čo presne je IT incident?

- Podľa definície ITIL 4 je to „**neplánované prerušenie IT služby alebo zníženie kvality IT služby**“.
- Táto definícia zahŕňa nielen zjavné útoky, ale aj latentné riziká.
 - **Príklad:** Zlyhanie jedného disku v zrkadlovej sade. Hoci služba beží ďalej, jej kvalita a odolnosť sú znížené.
- Riadenie incidentov je systematický proces zameraný na rýchlu obnovu služieb na dohodnuté úrovne (SLA).

ZÁKLADNÉ TYPY INCIDENTOV

- Prevádzkový incident
- IT incident (ITIL)
- Incident informaçnej bezpečnosti (ISO 27K)
- Kybernetický bezpečnostný incident (NIS2/ZKB)
- Incident GDPR
- Fyzický bezpečnostný incident
- OT/ICS incident
- Insider incident (CISA - USA)
- Incident dodávateľského reťazca

INCIDENT VS PROBLÉM

Incident:

- Neplánované prerušenie alebo zníženie kvality služby (jedno).
- Rieši sa okamžite.
- Viditeľné symptómy.
- Niečo, čo sa pokazilo teraz.

Problém:

- Príčina jedného alebo viacerých incidentov.
- Rieši sa systematicky.
- Skryté, nie vždy jasné symptómy
- Skrytá príčina, ktorá spôsobuje incidenty opakovane.

KATEGORIZÁCIA INCIDENTOV

- **3-5** bodová škála **podľa závažnosti** – od tej sa odvádzajú **prostriedky** aj **doba reakcie**.
 - **Informačný** – pravidelné testovanie, bez eskalácie, očakávané, False positive
 - **Nízka závažnosť:**
 - Malý dopad, neohrozuje prevádzku ani údaje.
 - Riešiť v štandardnom čase, sledovať, či sa neopakuje.
 - **Stredná závažnosť:**
 - Ovplyvňuje viac používateľov alebo systémov, môže mať dopad na dáta.
 - Rýchle riešenie adminom alebo IR tímom, izolácia zariadenia, pri nutnosti eskalácia, hlbšia analýza.
 - **Vysoká závažnosť:**
 - Môže spôsobiť veľký dopad, únik údajov, výpadok biznisu alebo porušenie zákona.
 - Okamžitá eskalácia, zastavenie šírenia, informovanie vedenia, príslušných orgánov.
-

ŽIVOTNÝ CYKLUS RIADENIA INCIDENTOV – PREHĽAD RÁMCOV

Štruktúrovaný prístup k reakcii

Existuje niekoľko medzinárodne uznávaných rámcov, ktoré definujú fázy riadenia incidentov. Hoci sa líšia v počte krokov, ich základné princípy sú konzistentné.

- **NIST SP 800-61 Rev. 2:** Rámec od amerického Národného inštitútu pre štandardy a technológie.
- **SANS Incident Response Framework:** Rámec od SANS Institute, zameraný na technické aspekty.
- **ISO/IEC 27035:** Medzinárodný štandard pre riadenie incidentov informačnej bezpečnosti.

VÝZNAM PROCESU RIADENIA INCIDENTOV

Strategická investícia, nie len náklad

- **Minimalizácia strát:** Rýchla reakcia obmedzuje finančné straty, poškodenie dát a prestoje.
- **Rýchla obnova operácií:** Zabezpečuje kontinuitu podnikania.
- **Zníženie budúcich rizík:** Analýza incidentov pomáha predchádzať opakovaniu.
- **Ochrana reputácie:** Transparentná a efektívna komunikácia posilňuje dôveru.
- **Súlad s predpismi:** Vyhnutie sa pokutám a právnym následkom (GDPR, NIS2).

Fáza/Krok	NIST SP 800-61 Rev. 2	SANS Framework	ISO/IEC 27035
1. Príprava	Príprava	Príprava	Plánovanie a príprava
2. Detekcia a Analýza	Detekcia a analýza	Identifikácia	Detekcia, hlásenie, posúdenie
3. Reakcia (Zadržanie)	Zadržanie, odstránenie, obnova	Zadržanie	Reakcia
4. Reakcia (Odstránenie)	(súčasť kroku 3)	Odstránenie	Reakcia
5. Reakcia (Obnova)	(súčasť kroku 3)	Obnova	Reakcia
6. Poučenie	Aktivity po incidente	Poučenie	Poučenie a zlepšenie

POROVNANIE FÁZ ŽIVOTNÉHO CYKLU

FÁZA 1: PRÍPRAVA

Základ úspešnej reakcie

- **Aktivity:**

- Definovanie politík, procedúr, rolí a zodpovedností tímu.
- Výber a implementácia bezpečnostných nástrojov (napr. SIEM, EDR).
- Školenie personálu a vykonávanie cvičení (tabletop, simulácie).
- Stanovenie bezpečnostných baseline na detekciu anomálií.

FÁZA 2: DETEKCIA A ANALÝZA

Odhalenie a pochopenie incidentu

- **Aktivity:**
 - Monitorovanie systémov a sietí na anomálie a podozrivú aktivitu.
 - Zber a analýza logov, dát z EDR a iných bezpečnostných upozornení.
 - Klasifikácia a prioritizácia incidentov podľa ich závažnosti a dopadu.
 - Rozlíšenie skutočných incidentov od falošných poplachov (false positives).

FÁZA 3: REAKCIA (ZADRŽANIE)

Aktívny boj s hrozbou

Zadržanie (Containment):

- Izolácia postihnutých systémov s cieľom obmedziť šírenie hrozby.
- Zastavenie ďalších škôd a zachovanie forenzných dôkazov.
- Zablokovanie kompromitovaných účtov, resetovanie hesiel, blokovanie pripojenia na FW.
- Informovanie zodpovedného tímu, komunikácia s manažmentom a používateľmi.
- Všetko čo sa deje dokumentovať.
- Udržať systém zapnutý.

FÁZA 4: REAKCIA (ODSTRÁNENIE)

Aktívny boj s hrozbou

Odstránenie (Eradication):

- Úplné odstránenie hrozby z prostredia – malvér, zraniteľnosti, perzistencie, backdoors, neautorizované účty, škodlivé skripty...
- Validácia, že neexistujú ďalšie kompromitované systémy.
- Porovnanie systémov s baseline.
- Preskenovanie siete, aktualizácie, zmena konfigurácií.

FÁZA 5: REAKCIA (OBNOVA)

Aktívny boj s hrozbou

Obnova (Recovery):

- Obnovenie systémov a dát do normálnej prevádzky z čistých záloh.
- Opätovné nasadenie konfigurácií zo schválených šablón.
- Dôkladné testovanie a monitorovanie obnovených systémov.
- Doladenie záverečného technického reportu.

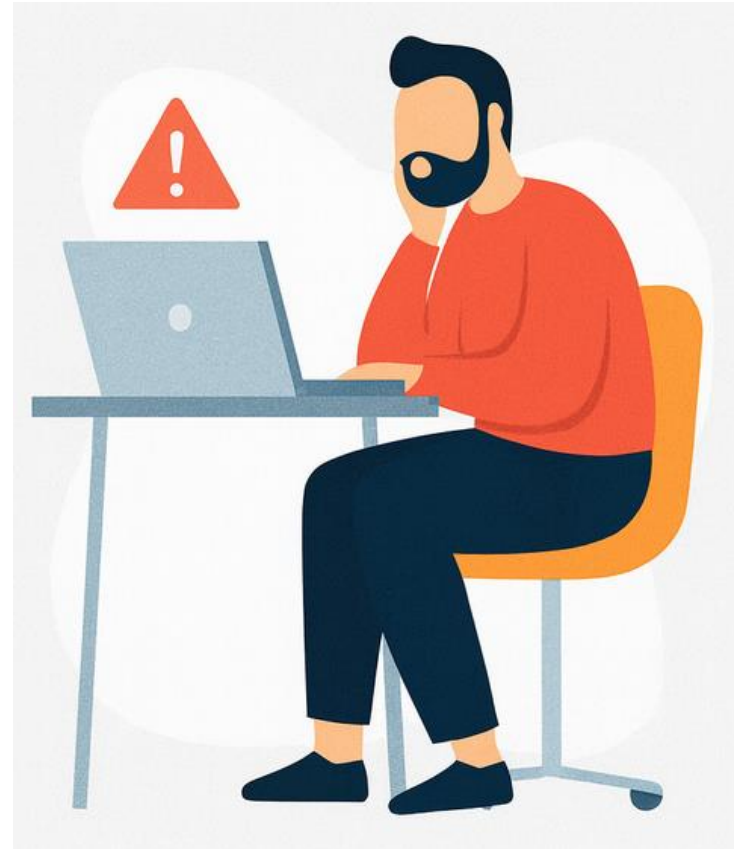
FÁZA 6: AKTIVITY PO INCIDENTE (POUČENIE)

Učenie sa z chýb pre budúcu odolnosť

- **Aktivity:**
 - Vykonanie podrobného preskúmania incidentu.
 - Analýza hlavnej príčiny (RCA) na identifikáciu slabých miest.
 - Implementácia zlepšení do plánov, politík a technických opatrení.
 - Dokumentácia a zdieľanie poznatkov v rámci organizácie.

NAJČASTEJŠIE CHYBY PRI INCIDENTOCH

- Reštart PC pred analýzou
- Mazanie logov
- Nenahlásenie incidentu
- Nikto nevie, komu volať
- Chýba dokumentácia krokov
- Podcenenie incidentu
- Komunikácia mimo organizácie



ZÁKLADNÉ HROZBY: MALVÉR

Škodlivý softvér v rôznych podobách

- **Ransomware:** Šifruje dáta a požaduje výkupné za ich obnovenie.
- **Spyware:** Tajne sleduje aktivitu používateľa a kradne informácie.
- **Vírusy a trójske kone:** Šíria sa a poškodzujú súbory alebo preberajú kontrolu nad systémom.

PRÍZNAKY MALVÉROVEJ INFEKCIE

Ako spoznať, že niečo nie je v poriadku?

- Dramatické spomalenie počítača alebo prehliadača.
- Časté mrznutie, pády systému alebo "modrá obrazovka smrti" (BSOD).
- Zmenené, vymazané alebo zašifrované súbory.
- Nové, neznáme programy alebo ikony na ploche.
- Programy sa spúšťajú alebo zatvárajú samé od seba.
- Vyskakovacie reklamy alebo falošné systémové upozornenia.
- Vysoká a neočakávaná sieťová aktivita.

ZÁKLADNÉ HROZBY: PHISHING

Psychologická manipulácia s cieľom získať údaje

- Útočník sa vydáva za legitímnu spoločnosť (banka, kuriér, sociálna sieť) prostredníctvom e-mailu, SMS alebo telefonátu.
- Cieľom je získať citlivé údaje: heslá, čísla kreditných kariet, osobné informácie.

AKO ROZPOZNAŤ PHISHINGOVÝ E-MAIL?

Varovné signály

- **Žiadosť o citlivé informácie:** Legitímne spoločnosti ich nikdy nežiadajú e-mailom.
- **Podozrivý odosielateľ:** Skontrolujte celú e-mailovú adresu, nielen meno. (@clients.amazon.org vs @amazon.com).
- **Nezhodné odkazy:** Prejdite kurzorom myši nad odkazom, aby sa zobrazila skutočná adresa.
- **Neočakávané prílohy:** Neotvárajte ich, ani keď vyzerajú legitímne.
- **Slabá gramatika a pravopis.**
- **Vytváranie nátlaku a naliehavosti:** Frázy ako "Váš účet bude zablokovaný", "Okamžite potvrdte platbu".

ZÁKLADNÉ HROZBY: SLABÉ HESLÁ A KRÁDEŽ ÚDAJOV

Najčastejší vstupný bod pre útočníkov

- **Riziká:**
 - Slabé a ľahko uhádnuteľné heslá.
 - Opakované používanie rovnakého hesla pre viacero služieb.
- **Metódy útočníkov:**
 - **Brute-force útoky:** Skúšanie všetkých možných kombinácií.
 - **Credential Stuffing:** Vkladanie uniknutých prihlasovacích údajov z iných služieb.

OCHRANA PRÍSTUPOVÝCH ÚDAJOV

Jednoduché kroky s obrovským dopadom

1. Používajte silné a jedinečné heslá:

- Dlhé (aspoň 12-15 znakov), komplexné (písmená, čísla, symboly).
- Pre každý účet použite iné heslo. Ideálne je použiť správcu hesiel.

2. Aktivujte viacfaktorovú autentifikáciu (MFA/2FA):

- Pridáva druhú vrstvu zabezpečenia (napr. kód z mobilnej aplikácie, SMS, hardvérový kľúč).
- **Výrazne chráni účet aj v prípade, že vaše heslo bolo ukradnuté.**

PRVÁ POMOC PRI KYBERNETICKOM ÚTOKU (PRE POUŽÍVATEĽA)

Čo robiť, ak máte podozrenie na útok?

1. **Odpojte sa od internetu:** Vypnite Wi-Fi, vytiahnite sieťový kábel. Tým zabránite ďalšej komunikácii malvéru.
2. **Zmeňte heslá:** Okamžite zmeňte heslá k dôležitým účtom (e-mail, banka) z iného, čistého zariadenia.
3. **Spustite antivírusovú kontrolu:** Prevedte hĺbkovú kontrolu systému.
4. **Identifikujte postihnuté údaje:** Zistite, aké informácie mohli byť kompromitované.
5. **Nahláste incident:** Informujte príslušné orgány (ak je to nutné).

NAHLASOVANIE INCIDENTU NA SLOVENSKU

Kam sa obrátiť?

- **Národný bezpečnostný úrad (NBÚ):**
 - Incident je možné nahlásiť prostredníctvom zabezpečenej webovej stránky NBÚ.
 - NBÚ spracováva aj dobrovoľné hlásenia incidentov.
 - Oficiálne stránky verejnej správy používajú doménu gov.sk a protokol https://.
- **Miestna polícia:**
 - V prípade trestného činu (podvod, krádež) je možné podať sťažnosť na najbližšej policajnej stanici.

PREVENCIA A ZÁKLADNÉ BEZPEČNOSTNÉ NÁVYKY

Najlepšou obranou je prevencia

- **Pravidelne aktualizujte softvér:** Operačný systém aj všetky aplikácie. Aktualizácie opravujú známe zraniteľnosti.
- **Používajte renomovaný antivírusový softvér:** A udržujte ho aktívny a aktualizovaný.
- **Pravidelne zálohujte dôležité dáta:** Na externé úložisko alebo do cloudu. Kľúčové pri ransomware.
- **Buďte opatrní:** Neotvárajte podozrivé odkazy a prílohy, nest'ahujte softvér z neznámych zdrojov.
- **Obmedzte administrátorské oprávnenia:** Pre každodennú prácu používajte štandardný účet.

PRÍPRAVA NA INCIDENTY V ORGANIZÁCI – PLÁN REAKCIE (IRP)

Plánovanie pre prípad krízy

- **Incident Response Plan (IRP):** Kľúčový dokument, ktorý definuje postupy, roly, zodpovednosti a eskaláciu.
- **Kľúčové aspekty IRP:**
 - **Definovanie rolí:** Jasne určený tím pre reakciu (Incident Coordinator, Technical Analyst, Communication Lead atď.) a jeho zástupcovia.
 - **Pravidelná aktualizácia:** Plán musí odrážať nové hrozby a zmeny v infraštruktúre.
 - **Školenia a cvičenia:** Tím musí byť trénovaný a plán pravidelne testovaný prostredníctvom simulácií.

PRÍPRAVA NA INCIDENTY V ORGANIZÁCIÍ – ZÁLOHOVANIE A DRP

Záchranná sieť vašej organizácie

- **Zálohovanie:**
 - Kritické systémy a dáta musia byť pravidelne zálohované.
 - **Kľúčové je zabezpečiť, aby zálohy boli čisté (neinfikované) a uložené oddelene od primárnych systémov (offline, off-site).**
- **Plán obnovy po havárii (Disaster Recovery Plan - DRP):**
 - Detailný plán, ako obnoviť prevádzku po závažnom incidente.
 - Musí byť pravidelne testovaný.

DOKUMENTÁCIA POČAS INCIDENTU

Ak to nie je zapísané, nestalo sa to

Každý incident musí byť zaznamenaný a sledovaný.

- **Čo zaznamenávať:**

- Jedinečný identifikátor, dátum a čas detekcie.
- Chronologický popis udalostí.
- Dotknuté systémy a aplikácie.
- Závažnosť a kategória incidentu.
- Zoznam všetkých vykonaných krokov (zadržanie, odstránenie, obnova).
- Informácie o spracovaní forenzných dôkazov.

DOKUMENTÁCIA POČAS INCIDENTU

- **Čo zaznamenávať:**
 - Identifikácia a kontext (komu nahlásené, detekcia, forma nahlásenia).
 - Ľudské kroky (Kto zasahoval a kedy, kontakty, eskalácie).
 - Technické detaily (IoC, logy, dotknuté časti topológie).
 - Dopad (rozsah, CIA, biznis, dotknuté aktíva).
 - Komunikácia (interna, externa (legal)).
 - Uchovanie dôkazov (spôsob odobratia, hashe, kde a ako, kto).
 - Čas a zdroje.
 - Návrhy na zlepšenie.

KOMUNIKÁCIA POČAS INCIDENTU

Transparentnosť a koordinácia

Efektívna komunikácia je rovnako dôležitá ako technická reakcia.

- **Komunikačný plán by mal definovať:**
 - **Kto potrebuje byť informovaný:** Interní manažéri, zamestnanci, právnici, PR tím, externí partneri, zákazníci.
 - **Aké kanály sa použijú:** Interné (napr. Slack, e-mail) a externé (napr. statusová stránka, sociálne médiá).
 - **Kto má oprávnenie komunikovať:** Jasne definované roly, aby sa predišlo chaosu.
 - **Jasné eskalácie:** Protokoly pre eskaláciu problému na vyšší manažment.

FÁZA PO INCIDENTE: ANALÝZA HLAVNEJ PRÍČINY (RCA)

Prečo sa to stalo a ako tomu predísť?

- **Root Cause Analysis (RCA):** Štruktúrovaný proces, ktorý hľadá základné príčiny problému, nielen jeho symptómy.
- **Metódy:**
 - **Metóda "5 Prečo":** Opakované pýtanie sa "prečo", kým sa neodhalí koreňová príčina.
 - **Fishbone (Ishikawa) diagramy.**
- **Cieľ:** Učenie a zlepšovanie, **nie hľadanie vinníka.**
 - Prostredie psychologickkej bezpečnosti je kľúčové pre úspešnú RCA.

FÁZA PO INCIDENTE: PROCES "LESSONS LEARNED"

Premena incidentu na príležitosť

- Formálny proces na zhodnotenie reakcie na incident a identifikáciu oblastí na zlepšenie.
- **Kroky:**
 - **Zber dát:** Zhromaždenie všetkej dokumentácie (správy, logy, komunikácia).
 - **Identifikácia zúčastnených:** Rozhovory so všetkými, ktorí sa podieľali na reakcii.
 - **Analýza:** Čo fungovalo dobre? Čo sa dalo urobiť lepšie? Kde boli prekážky?
 - **Vytvorenie akčných plánov:** Konkrétne, merateľné kroky na zlepšenie s priradenými zodpovednosťami a termínmi.

PRÁVNE POŽIADAVKY: GDPR

Ochrana osobných údajov a ohlasovacie povinnosti

- **GDPR (General Data Protection Regulation):** Nariadenie EÚ o ochrane osobných údajov.
- **Povinnosť ohlásiť narušenie osobných údajov:**
 - **Komu:** Dozornému orgánu (na Slovensku **Úrad na ochranu osobných údajov SR - ÚOOÚ SR**).
 - **Kedy:** Bez zbytočného odkladu, najneskôr **do 72 hodín** od zistenia narušenia.
 - **Dotknutým osobám:** Bez zbytočného odkladu, ak narušenie predstavuje vysoké riziko pre ich práva a slobody.
- **Povinná dokumentácia:** Všetky narušenia musia byť interne zdokumentované.

PRÁVNE POŽIADAVKY: SMERNICA NIS2

Zvyšovanie kybernetickej odolnosti v EÚ

- **Smernica NIS2:** Rozširuje rozsah regulácie na ďalšie sektory a sprísňuje požiadavky.
- Na Slovensku transponovaná zákonom s účinnosťou od 1. januára 2025.
- **Povinnosť ohlásiť významný incident:**
 - **Komu:** Príslušnému CSIRT tímu alebo orgánu (na Slovensku **NBÚ**).
 - **Časové lehoty:**
 - **Do 24 hodín:** Včasné varovanie.
 - **Do 72 hodín:** Oznámenie incidentu s počiatočným posúdením.
 - **Do 1 mesiaca:** Záverečná správa.

KEDY SA INCIDENT NEHLÁSI

Incident sa NEHLÁSI, ak:

- Nemá dopad na regulovanú službu (NIS2).
- Nedošlo k porušeniu osobných údajov (GDPR).
- Je to interný prevádzkový alebo technický problém, bez bezpečnostného dopadu.
- Incident neohrozuje **dostupnosť, integritu ani dôvernosť**.
- Je to **neúspešný útok bez následkov** (zablokovaný AV/EDR, IDS alert bez dopadu).
- Udalosť nemá **žiadny alebo zanedbateľný dopad** na služby a infraštruktúru.
- Zasiahnuté bolo len **testovacie** prostredie **bez osobných údajov**.
- Existuje istota, že **nedošlo k úniku alebo kompromitácii dát**.
- **!!!Nahlasuje sa dopad, nie pokus!!!**

VÝZNAMNÝ INCIDENT PODĽA NIS2

Významný incident je taký incident, ktorý má **reálny dopad** na **službu, zákazníkov, dáta** alebo **spoločnosť**.

- **Závažný prevádzkový dopad**
- **Závažný bezpečnostný dopad**
- **Závažný spoločenský dopad**
- **Závažný ekonomický dopad**
- **Technické indikátory významného incidentu:**
 - ransomvér alebo šifrovanie systémov.
 - kompromitácia AD, root/admin účtov, cloudového účtu.
 - výpadok VPN, identity, centrálného SIEM/EDR
 - preukázané exfiltrovanie dát

PRÁVNE POŽIADAVKY: SMERNICA NIS2

Zvyšovanie kybernetickej odolnosti v EÚ

- **Smernica NIS2:** Rozširuje rozsah regulácie na ďalšie sektory a sprísňuje požiadavky.
- Na Slovensku transponovaná zákonom s účinnosťou od 1. januára 2025.
- **Povinnosť ohlásiť významný incident:**
 - **Komu:** Príslušnému CSIRT tímu alebo orgánu (na Slovensku **NBÚ**).
 - **Časové lehoty:**
 - **Do 24 hodín:** Včasné varovanie.
 - **Do 72 hodín:** Oznámenie incidentu s počiatočným posúdením.
 - **Do 1 mesiaca:** Záverečná správa.

ZHRNUTIE OHLASOVACÍCH POVINNOSTÍ

Predpis	Typ incidentu	Časová lehota	Slovenský orgán
GDPR	Narušenie osobných údajov	Do 72 hodín	Úrad na ochranu osobných údajov SR (ÚOOÚ SR)
NIS2/ZoKB	Významný kybernetický bezpečnostný incident	Včasné varovanie: Do 24h	Národný bezpečnostný úrad (NBÚ)
		Oznámenie: Do 72h	
		Záverečná správa: Do 1 mesiaca	

ZÁVER: ZHRNUTIE KLÚČOVÝCH POZNATKOV

- **Pre bežného používateľa:**
 - Základom je **povedomie** o hrozbách (phishing, malvér).
 - Klúčová je **prevencia**: silné heslá, MFA, aktualizácie, opatrnosť.
 - V prípade útoku je nutná **rýchla prvá pomoc**: odpojenie od siete, zmena hesiel.
- **Pre organizáciu:**
 - Riadenie incidentov je **nepretržitý cyklus**, nie jednorazová úloha.
 - Základom je **príprava**: IRP, školenia, testovanie, zálohy.
 - Kľúčom k zlepšeniu je **fáza po incidente** (RCA, Lessons Learned).
 - Nevyhnutný je **súlad s legislatívou** (GDPR, NIS2).

ZÁVER: PROAKTÍVNY PRÍSTUP A SPOLUPRÁCA

- **Adaptácia na meniace sa hrozby:**
 - Kybernetické hrozby sa neustále vyvíjajú.
 - Proces riadenia incidentov musí byť dynamický a založený na neustálom zlepšovaní (cyklus Plan-Do-Check-Act).
- **Význam spolupráce a zdieľania informácií:**
 - Kybernetická bezpečnosť je kolektívne úsilie.
 - Efektívna spolupráca je nutná interne (IT, právne, PR) aj externe (orgány, komunita).
 - Zdieľanie poznatkov o hrozbách posilňuje celú komunitu.