Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Kryptografické opatrenia a zásady používania kryptografie

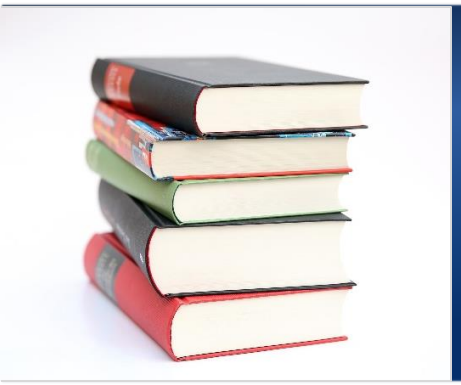
Technické opatrenia (Blok IV)

Kurz: Manažér kybernetickej bezpečnosti

Ing. Ladislav Mariš, PhD.

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

ladislav.maris@uniza.sk



- Základy kryptografických bezpečnostných mechanizmov
- Koncepcie a technológie vzdialeného prístupu
- Princípy zabezpečenia virtuálnych privátnych sietí (VPN)

Zákonný rámec pre kryptografické opatrenia

- **Zákonný rámec:** § 20 písm. h) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti
- **Zameranie:** Riadiace technické opatrenia v oblasti kryptografie a ich úloha pri ochrane dôvernosti, integrity a dostupnosti.
- **§ 20 Bezpečnostnými opatreniami** na účely tohto zákona sú **úlohy, procesy, role a technológie** v organizačnej, personálnej, fyzickej a technologickej oblasti, ktorých **cieľom je dosiahnutie, zaručenie a udržanie kybernetickej bezpečnosti** počas životného cyklu sietí a informačných systémov a operačných technológií.
- Bezpečnostné opatrenia sú realizované **na základe** vykonanej **analýzy rizík** a s prihliadnutím na bezpečnostné metodiky a politiky úradu, najnovšie bezpečnostné trendy a medzinárodné normy a v súlade s bezpečnostnými štandardami v oblasti kybernetickej bezpečnosti **s cieľom:**
  - **identifikovať zraniteľnosti** (…),
  - **chrániť preventívne aktíva** (…),
  - **detegovať kybernetické incidenty,**
  - **reagovať na identifikované zraniteľnosti a incidenty** (…)
  - a **obnoviť systémy** ().

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

Zákonný rámec pre kryptografické opatrenia

§ 20 (2) písm. h) zákona č. 69/2018 Z. z.

(2) Bezpečnostné opatrenia sa prijímajú aspoň pre

a) organizáciu a riadenie informačnej bezpečnosti a kybernetickej bezpečnosti,

b) správu zraniteľností a kybernetických hrozieb,

c) správu aktív a riadenie kybernetických hrozieb a rizík,

d) riadenie udalostí a kybernetických bezpečnostných incidentov,

e) riadenie kontinuity činností, zálohovanie, obnovu systémov po havárii a krízové riadenie,

f) bezpečnosť pri nadobúdaní, vývoji a údržbe siete, informačných systémov, aplikácií a konfigurácií,

g) postupy posudzovania účinnosti opatrení, riadenie súladu a kontrolné činnosti,

h) kryptografické opatrenia a zásady používania kryptografie,

i) bezpečnosť a spôsobilosti ľudských zdrojov,

j) správu identít a prístupov,

k) bezpečnosť pri prevádzke sietí a informačných systémov,

l) ochranu proti škodlivému kódu a nežiaducemu obsahu,

m) systémovú bezpečnosť, sieťovú bezpečnosť a komunikačnú bezpečnosť,

n) monitorovanie, zaznamenávanie a hlásenie udalostí,

o) fyzickú bezpečnosť, bezpečnosť prostredia a správu koncových zariadení,

p) ochranu záznamov, súkromia a označovanie informácií,

q) dodávateľský reťazec,

r) obstarávanie a využívanie certifikovaných produktov IKT, služieb IKT a procesov IKT.

(3) Bezpečnostné opatrenia sa prijímajú a realizujú v rozsahu a spôsobom podľa § 32 ods. 1 písm. b) alebo osobitného predpisu (pr. atómový zákon, úrad jadrového dozoru), ak je vydaný, a na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu.

§ 32 Úrad ustanoví všeobecne záväzným právnym predpisom ods. 1 písm. b):
obsah bezpečnostných opatrení, obsah a štruktúru bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (§ 20)

Súvislosť kryptografických opatrení

- § 7 Národná stratégia kybernetickej bezpečnosti a národný plán reakcie na rozsiahle kybernetické bezpečnostné incidenty a kybernetické krízy
  - (3) V rámci národnej stratégie kybernetickej bezpečnosti sa prijímajú politiky najmä na zabezpečenie:
    - b) zohľadňovania požiadaviek na kybernetickú bezpečnosť produktov IKT a služieb IKT vo verejnom obstarávaní, a to aj ak ide o certifikáciu kybernetickej bezpečnosti, **kryptografické opatrenia** a využívanie produktov s otvoreným zdrojovým kódom,

- **Národná stratégia kybernetickej bezpečnosti** je východiskový strategický dokument, ktorý komplexne určuje strategický prístup Slovenskej republiky k zabezpečeniu vysokej úrovne kybernetickej bezpečnosti
- https://www.nbu.gov.sk/612-sk/narodna-strategia-a-akcny-plan-kybernetickej-bezpecnosti/

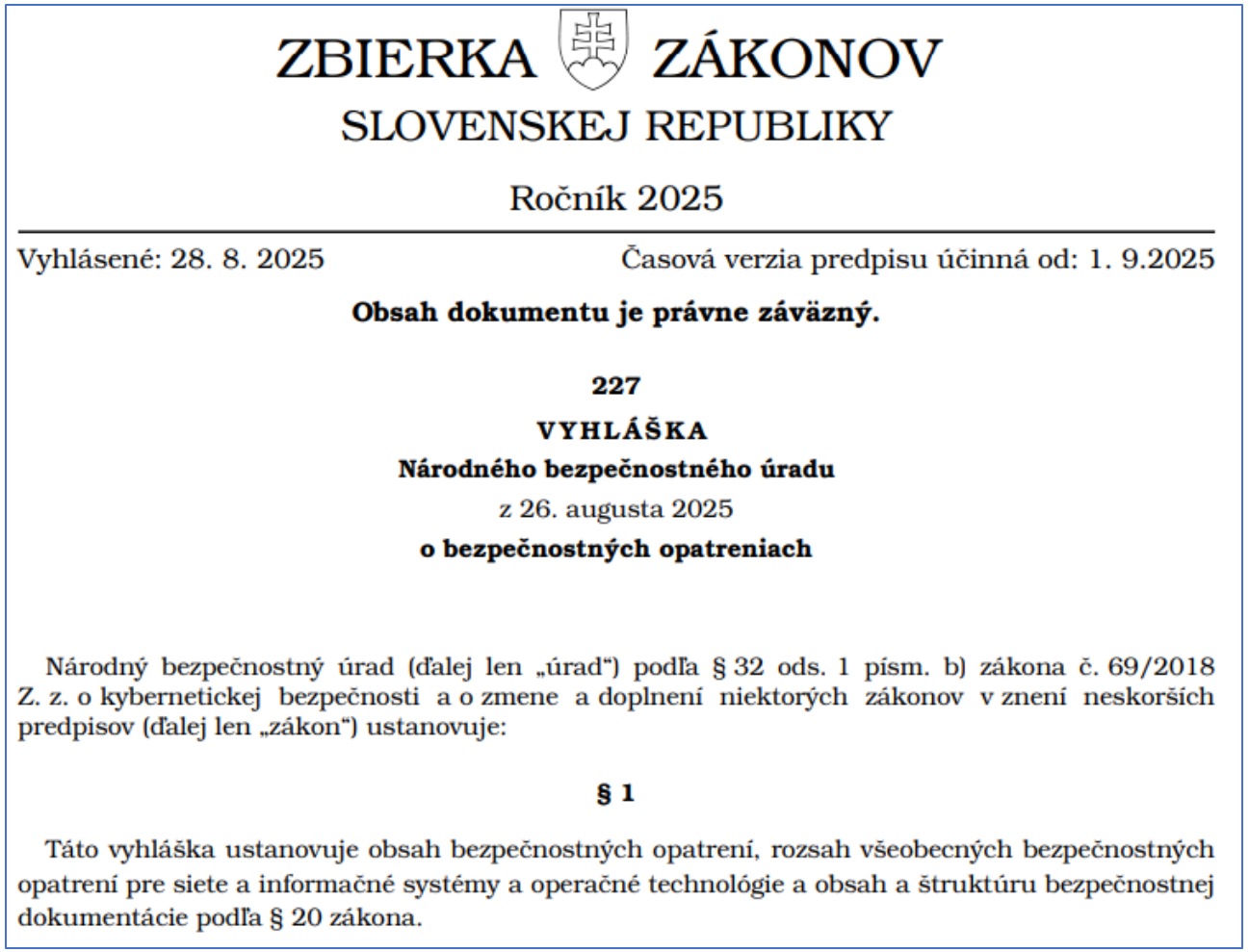
Vyhláška NBÚ o bezpečnostných opatreniach

Vyhláška NBÚ č. 227 z roku 2025 o bezpečnostných opatreniach

https://static.slov-lex.sk/pdf/SK/ZZ/2025/227/ZZ_2025_227_20250901.pdf

Príloha č. 1
k vyhláške č. 227/2025 Z. z.

Kryptografické opatrenia v Prílohe č. 1 Bezpečnostné opatrenia pre **kryptografické opatrenia a zásady používania kryptografie** podľa § 20 ods. 2 písm. h) zákona sú uvedené v **Položke 61 až 63** Prílohy č. 1 tejto vyhlášky.



ZBIERKA ZÁKONOV
SLOVENSKEJ REPUBLIKY

Ročník 2025

Vyhlásené: 28. 8. 2025 Časová verzia predpisu účinná od: 1. 9.2025

Obsah dokumentu je právne záväzný.

227

VYHLÁŠKA

Národného bezpečnostného úradu

z 26. augusta 2025

o bezpečnostných opatreniach

Národný bezpečnostný úrad (ďalej len „úrad") podľa § 32 ods. 1 písm. b) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon") ustanovuje:

§ 1

Táto vyhláška ustanovuje obsah bezpečnostných opatrení, rozsah všeobecných bezpečnostných opatrení pre siete a informačné systémy a operačné technológie a obsah a štruktúru bezpečnostnej dokumentácie podľa § 20 zákona.

Príloha č. 1 Vyhlášky NBÚ 227/2025 z pohľadu kryptografických opatrení

Prevádzkovateľ základnej služby (PZS) a prevádzkovateľ kritickej základnej služby (PKZS) ich musia prijať, pričom sa vzťahujú na informačné a komunikačné technológie (IKT) aj na operačné technológie (OT)

Položka	Bezpečnostné opatrenia pre kryptografické opatrenia a zásady používania kryptografie podľa § 20 ods. 2 písm. h) zákona prijíma prevádzkovateľ základnej služby tak, že:	Relevancia pre IKT		Relevancia pre OT	
		PZS	PKZS	PZS	PKZS
61.	**nastavením pravidiel pre použitie vhodných kryptografických metód je obmedzené potenciálne narušenie dôvernosti informácií vrátane osobných údajov** a sú dodržiavané požiadavky vyplývajúce zo všeobecne záväzných právnych predpisov, požiadavky vyplývajúce zo zmlúv alebo v prípade certifikovaného subjektu normatívne požiadavky týkajúce sa kybernetickej bezpečnosti	áno	áno	áno	áno
62.	sú definované a zavedené **pravidlá efektívneho používania kryptografických mechanizmov vrátane správy kryptografických kľúčov a postupov**	áno	áno	áno	áno
63.	sú prijaté a **aplikované postupy na pravidelné prehodnocovanie odolnosti zavedených kryptografických mechanizmov**; prehodnocovanie odolnosti zavedených kryptografických mechanizmov sa vykonáva **najmenej raz ročne a vyhotovuje sa o tom záznam**, ktorý sa uchováva najmenej na obdobie od ukončenia posledného auditu do ukončenia nasledujúceho auditu alebo samohodnotenia	áno	áno	áno	áno

Položka 61: Riadenie dôvernosti a súlad s legislatívou - **príklad**

- Položka 61 vyžaduje, aby ste
  - **nastavili jasné pravidlá** pre použitie vhodných kryptografických metód s cieľom obmedziť narušenie **dôvernosti informácií**, vrátane osobných údajov.

Najdôležitejšia pre manažment je požiadavka na

  - **súlad s právnymi predpismi a zmluvami**.

61.	**nastavením pravidiel pre použitie vhodných kryptografických metód je obmedzené potenciálne narušenie dôvernosti informácií vrátane osobných údajov** a sú dodržiavané požiadavky vyplývajúce zo všeobecne záväzných právnych predpisov, požiadavky vyplývajúce zo zmlúv alebo v prípade certifikovaného subjektu normatívne požiadavky týkajúce sa kybernetickej bezpečnosti

Manažérska perspektíva: Vašou primárnou úlohou je **vytvoriť a nechať schváliť Kryptografickú politiku** – dokument, ktorý stanovuje, aké šifrovacie protokoly (napr. minimálne verzie TLS) a algoritmy (napr. AES-256) sú povolené v celej organizácii (pre IKT aj OT).

- Musíte zabezpečiť, aby táto politika bola v súlade s požiadavkami, ktoré na vás kladú iné zákony (napr. GDPR pre osobné údaje) a všetky zmluvy s tretími stranami (dodávateľmi).
- Manažérsky výstupom je **preukázanie** (prostredníctvom auditu), že neexistuje žiadny systém, ktorý by používal zastarané (a teda ľahko prelomiteľné) šifrovanie a vystavoval tak dáta riziku.

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

Položka 62: Pravidlá efektívneho používania mechanizmov a správa kľúčov- **príklad**

- Položka 62 sa zameriava na definovanie a zavedenie pravidiel **efektívneho používania kryptografických mechanizmov**, pričom kľúčovou oblasťou je **správa kryptografických kľúčov a postupov**.
- *Ak sa skompromituje kľúč, celá snaha o šifrovanie je zbytočná !!!*

62.	sú definované a zavedené **pravidlá efektívneho používania kryptografických mechanizmov vrátane správy kryptografických kľúčov a postupov**

Manažérska perspektíva: Musíte riadiť celý **životný cyklus kľúčov** – od ich bezpečného generovania (napr. pomocou špecializovaných zariadení) až po ich definitívne a preukázateľné zničenie.

- To znamená nasadenie a riadenie **Systému riadenia kľúčov (KMS)**, aby kľúče neboli nikdy uložené na nechránenom disku. Pre vás je dôležité mať **procesy** pre:
  - **Rotáciu kľúčov:** Automatizovaná a pravidelná výmena kľúčov.
  - **Uchovávanie kľúčov:** Kľúče by mali byť izolované, ideálne v **hardvérových bezpečnostných moduloch (HSM)**.
  - **Incident Response – ! Reakcia !** Zavedenie postupu pre **okamžité zneplatnenie** kľúča v prípade, že **existuje podozrenie na jeho kompromitáciu**. V kontexte OT to chráni riadiace systémy pred prevzatím kontroly útočníkom cez neoprávnený kľúč.

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

Položka 63: Pravidelné prehodnocovanie odolnosti a auditná stopa - **príklad**

- Položka 63 ukladá povinnosť prijímať a aplikovať postupy na **pravidelné prehodnocovanie odolnosti** zavedených kryptografických mechanizmov **najmenej raz ročne**.
- Vyžaduje sa aj **vyhotovenie záznamu** o tomto prehodnotení, ktorý slúži pre potreby následného auditu.

63.	sú prijaté a **aplikované postupy na pravidelné prehodnocovanie odolnosti zavedených kryptografických mechanizmov**; prehodnocovanie odolnosti zavedených kryptografických mechanizmov sa vykonáva **najmenej raz ročne a vyhotovuje sa o tom záznam**, ktorý sa uchováva najmenej na obdobie od ukončenia posledného auditu do ukončenia nasledujúceho auditu alebo samohodnotenia

Manažérska perspektíva: Táto položka je o **trvalej udržateľnosti a overovaní**. Nestačí len šifrovanie zaviesť; musíte aktívne testovať svoju bezpečnosť.

- **Plánovanie testov:** Zabezpečte, aby sa každý rok vykonal **technický test** (audit sily šifrovania) na všetkých kritických systémoch. Výsledky testov musia explicitne hovoriť o sile (alebo slabosti) kryptografickej ochrany.
- **Auditná stopa:** Musíte zabezpečiť, že **záznam o ročnom prehodnotení** je nielen vypracovaný, ale aj **schválený** príslušnou vedúcou osobou a riadne archivovaný. Tento záznam je kľúčovým dôkazom pre NBÚ, že svoju povinnosť plníte.
- **Náprava rizík:** Ak prehodnotenie zistí, že kryptografická odolnosť je nízka (napr. používa sa slabý kľúč), musíte zistenú zraniteľnosť ihneď zaradiť do **procesu riadenia rizík** a prijať nápravné opatrenia.

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

Zhrnutie kryptografických opatrení z pozície manažéra KB

Pre manažéra kybernetickej bezpečnosti predstavujú položky 61-63 komplexný balík pre **riadenú kryptografiu**:

- **(61)** nastaví pravidlá a súlad,
- **(62)** chráni kľúče a mechanizmy a
- **(63)** zabezpečuje, že ochrana je trvalo odolná a auditovateľná.

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

Čiastočný presah kryptografie podľa písm. **m)** bezpečnostné opatrenia pre **systémovú bezpečnosť, sieťovú bezpečnosť a komunikačnú bezpečnosť,**

Položka	Bezpečnostné opatrenia pre systémovú bezpečnosť, sieťovú bezpečnosť a komunikačnú bezpečnosť podľa § 20 ods. 2 písm. m) zákona prijíma prevádzkovateľ základnej služby tak, že:	Relevancia pre IKT*		Relevancia pre OT*	
		PZS*	PKZS*	PZS*	PKZS*
101.	sú vypracované a zavedené postupy na prenos informácií v rámci organizácie ako aj s tretími stranami pre všetky typy technických prostriedkov a médií	ÁNO	ÁNO	ÁNO	ÁNO
102.	je používané šifrovanie na zabezpečenie údajov pri prenose vybraných údajov medzi systémami OT; identifikácia vybraných údajov prebieha pomocou klasifikácie informácií	-	-	ÁNO	ÁNO
103.	je používané šifrovanie na zabezpečenie vybraných údajov pri prenose medzi a v rámci rôznych úrovní systémov OT; identifikácia vybraných údajov prebieha pomocou klasifikácie informácií – toto opatrenie je relevantné pre komponenty zaradené do vrstiev* pre operačné technológie 3 a vyššie	-	-	-	ÁNO

Položky 102 a 103 - príklady

- **102 - Manažérska zodpovednosť:** Zabezpečiť, aby bol proces klasifikácie dát v OT prostredí **realistický a funkčný**. Manažér musí schváliť, ktoré dáta sú *vybrané* na šifrovanie a prečo. Nesprávna klasifikácia vedie k nedostatočnej ochrane kritickej prevádzky.
- **Architektonické rozhodnutia:** Manažér musí schváliť nasadenie technológií, ktoré umožňujú šifrovanie dátového toku medzi priemyselnými zariadeniami (napr. PLC a SCADA servery). Kvôli požiadavkám na nízku latenciu a výkon musí zabezpečiť, že zvolené šifrovacie riešenia (napr. *IPsec tunely*, alebo šifrované *MQTT protokoly*) **nezhoršia stabilitu a časovú odozvu** kritickej technológie.
- **Metrika:** Sledovanie percenta kritických OT dát, ktoré sú prenášané bez šifrovania, a udržanie tohto percenta na nule.

- **103 - Strategická segmentácia:** Manažér túto položku využíva na posilnenie **sieťovej segmentácie** medzi rôznymi OT vrstvami (napr. medzi Vrstvou 3 – riadiace servery a Vrstvou 4 – podnikové systémy). Šifrovanie tu funguje ako **dodatočná kontrola dôveryhodnosti** prechodu medzi segmentmi.
- **Izolácia riadiacich príkazov:** Manažér musí zabezpečiť, že riadiace príkazy prenášané v rámci alebo medzi kritickými vrstvami sú šifrované. Tým sa **chráni integrita** prevádzky – ak by útočník modifikoval nešifrovaný príkaz, mohol by spôsobiť výpadok. Šifrovanie s digitálnymi podpismi túto zmenu odhalí.
- **Politika nulovej dôvery (Zero Trust):** V koncepte nulovej dôvery táto položka zaisťuje, že komunikácia medzi dvoma entitami, aj keď sú už *vnútri* dôveryhodnej siete OT, musí byť chránená. Tým sa manažér vyhýba spoliehaniu sa na "bezpečnú sieť".
- **Metrika:** Auditné záznamy potvrdzujúce šifrovanie všetkých dátových tokov s klasifikovanými dátami prechádzajúcimi hranice Vrstvy 3 a 4.

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

Základy kryptografických bezpečnostných mechanizmov

Zameranie kryptografie v oblasti KB

- **Zameranie:** Riadiace technické opatrenia v oblasti kryptografie a ich úloha pri ochrane dôvernosti, integrity a dostupnosti.

Kryptografia je základným pilierom technických opatrení, ktoré zabezpečujú:

- **Dôvernosť (Confidentiality):** Informácie sú čitateľné len oprávneným osobám.
- **Integrita (Integrity):** Ochrana pred neautorizovanou zmenou obsahu.
- **Autentifikácia (Authentication):** Overenie identity komunikujúcich strán.
- **Nezapierateľnosť (Non-repudiation):** Zaručenie, že odosielateľ nemôže poprieť odoslanie správy.

Dôvernosť

"E-mail s dôvernými dokumentmi je šifrovaný" → Dôvernosť

- **Šifrovanie** zabezpečuje, že obsah e-mailu môžu čítať len oprávnení príjemcovia.
- Ak niekto e-mail zachytí (napr. počas prenosu cez internet), **neuvidí zrozumiteľný text**, ale len nezmyselné znaky.

Integrita

"Obsah je kontrolovaný hashom" → Integrita

- **Hashovacia funkcia** vytvorí „odtlačok“ obsahu e-mailu.
- Príjemca si vie overiť, či bol tento odtlačok (napr. SHA-256 hodnota) zhodný s tým, ktorý bol podpísaný.
- Ak by niekto e-mail **po ceste zmenil** (napr. zmenil prílohu), hash by nesedel a integrita by bola porušená.

Overenie identity

Overenie identity znamená, že systém si **overí, kto konkrétne posiela alebo prijíma e-mail**.

- V kryptografii sa to deje najčastejšie pomocou:
  - **Digitálneho certifikátu** (napr. kvalifikovaný certifikát občianskeho preukazu)
  - **Prihlásenia sa so súkromným kľúčom**, ktorý je jedinečný pre konkrétneho používateľa.

Odosielateľ používa certifikát vystavený dôveryhodnou certifikačnou autoritou (CA), ktorý je viazaný na jeho meno a e-mail.

- Príjemca môže tento certifikát overiť a **spoľahlivo identifikovať** odosielateľa.
- Overenie identity prebieha ešte **pred tým**, ako príjemca dôveruje obsahu správy alebo podpisu.

Nezapierateľnosť

"Podpísaný digitálnym podpisom" → Nezapierateľnosť

- Digitálny podpis **overuje totožnosť odosielateľa** – potvrdzuje, že e-mail naozaj poslal.
- Vzniká použitím **súkromného kľúča odosielateľa**, príjemca overí verejným kľúčom.
- **Nezapierateľnosť** znamená, že odosielateľ nemôže tvrdiť, že správu neposlal – podpis je právne a technicky dôkazom.

Všetky 4 základné vlastnosti

Odosielateľ podpíše dokument (nezapierateľnosť), zašifruje ho pre príjemcu (dôvernosť), pridá hash (integrita), a identifikuje sa pomocou certifikátu (autentifikácia).

Prijímateľ má istotu:

- **Kto** mu správu poslal (autentifikácia),
- Že obsah **nebol pozmenený** (integrita),
- Že obsah **vidí len on** (dôvernosť),
- A že odosielateľ to **nemôže poprieť** (nezapierateľnosť).

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

Symetrické vs. asymetrické šifrovanie

Symetrické šifrovanie

- Rovnaký kľúč pre šifrovanie aj dešifrovanie.
- Rýchle a efektívne.
- Vyžaduje bezpečný prenos kľúčov.

Asymetrické šifrovanie

- Dvojica verejný / súkromný kľúč.
- Ideálne na výmenu kľúčov a digitálne podpisy.
- Pomalšie ako symetrické.

V praxi sa používa aj **hybridné šifrovanie.**

HASH

- **Prečo sú dôležité pre organizáciu**
- **Integrita dát = dôveryhodnosť informácií.**
  - Ak organizácia nevie garantovať, že dáta **neboli pozmenené**, nemôže sa na ne spoľahnúť – čo ohrozuje rozhodovanie, procesy aj povesť.
- **Hash zabezpečuje, že systém odhalí neoprávnený zásah.**
  - To je kľúčové pri evidencii, zmluvách, účtovníctve, systémoch spracúvajúcich osobné alebo zdravotné údaje.

- Z manažérskeho hľadiska je dôležité, aby vedenie organizácie **rozumelo významu hashovacích funkcií nielen technicky, ale aj strategicky**, tzn. ako prispievajú k ochrane informačných aktív a napĺňaniu zákonných požiadaviek (napr. podľa § 20 písm. h) zákona č. 69/2018 Z. z.).

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

Overujeme ako sa tieto funkcie nasadzujú

Manažérske rozhodnutia:

- **Výber bezpečného algoritmu (napr. SHA-256, SHA-3)**
  - **Manažér musí zabezpečiť, že IT oddelenie nepoužíva zastarané alebo prelomené funkcie (algoritmy, šifry)** (napr. MD5 alebo SHA-1).

- **Stanovenie politík pre ukladanie hesiel**
  - **Heslá musia byť v databázach hashované -** nikdy neuložené ako čistý text. Nesprávna implementácia môže viesť k úniku citlivých údajov.

- **Auditovanie a kontrola integrity systémov a dát**
  - **Hashy môžu byť súčasťou automatizovaných kontrol**, ktoré overujú, či sú súbory, databázy alebo konfigurácie nezmenené (napr. po aktualizáciách alebo incidente).

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

Príklady

Distribúcia softvéru:
Ak organizácia sťahuje softvér alebo aktualizácie (napr. z dodávateľského portálu), hash zabezpečí, že sa súbor nepoškodil alebo nezmenil *pri prenose – čím sa predchádza* ***malvéru alebo útokom dodávateľského reťazca****.*

Overenie elektronických dokumentov:
Digitálne podpisy pracujú s hashmi. Bezpečný podpis faktúry alebo zmluvy *znamená, že dokument je originál a nebol upravený.*

Zákonné povinnosti (kybernetický zákon, vyhlášky):
Implementácia hashovania je technické opatrenie*, ktoré sa považuje za* ***primeraný spôsob zabezpečenia integrity****, ako to vyžaduje § 20 písm. h).*

Dôsledky

Dôsledky zanedbania hashovania

- Úniky dát alebo **podvrhnutie dokumentov** bez možnosti odhalenia.
- Porušenie legislatívy (napr. Zákon o KB).
- **Strata dôvery** voči zákazníkom, partnerom alebo audítorom.
- Možné **finančné sankcie alebo právna zodpovednosť.**

Súčasnosť/budúcnosť

- 2026 mnohé certifikačné autority (napr. I.CA v EÚ) prestávajú podporovať 2048-bitové kľúče a vyžadujú minimálne 4096-bitové kľúče pre digitálne podpisy (RSA 4096),
- 2026 potreba kombinovania, súčasných algoritmov s novými (PQC)
- Digitálna identita, digitálna mena, digitálna banka (EU peňaženka), nové hrozby.
- 2026-2030? plán prechodu na nové, odolnejšie kryptografické algoritmy, aby sa ochránili dáta a systémy pred budúcimi kvantovými počítačmi, ktoré by mohli rozlúsknuť dnešné šifrovanie
- testovanie, certifikácia, spolupráca s priemyslom a cieľ dokončiť prechod do roku 2035 (týka sa hlavne PZS a PKZS!)

Kvantová výpočtová technika bola identifikovaná ako hrozba pre mnohé kryptografické algoritmy používané na ochranu dôvernosti a pravosti údajov. Proti tejto hrozbe možno bojovať včasným, komplexným a koordinovaným prechodom na postkvantovú kryptografiu (PCQ).

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

Rôzne

- **Krypto-agilita:** Schopnosť systému rýchlo nahradiť jeden algoritmus iným bez nutnosti meniť celú infraštruktúru (*kritická požiadavka, služba funguje*).
- **Hybridná implementácia:** Kombinovanie klasických a post-kvantových (napr. ML-KEM) algoritmov na zabezpečenie ochrany pred súčasnými aj budúcimi hrozbami.
- Šifrovacie algoritmy súčasnosti nebudú po roku 2030 považované za dostačujúce (kryptografický audit)
- **Regulačná zhoda:** Súlad s normami a nariadeniami EÚ o digitálnej odolnosti (napr. **NIS2**), ktoré od r. 2026 prísnejšie tlačia na bezpečnú kryptografiu – resp. Každým rokom to bude prísnejšie, dynamický vývoj.
- **Dátová životnosť:** Pre dáta, ktoré musia zostať tajné 10 a viac rokov, je použitie **AES-256** a **ML-KEM** v roku 2026 už povinnosťou.

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

Včasná adaptácia na postkvantovú kryptografiu

- Nové bezpečnostné štandardy ukladajú štátu a jeho dodávateľom povinnosť prejsť na certifikované šifrovanie a preukázateľne bezpečné dodávateľské reťazce.
- Zhoda sa netýka len technológií (HW/SW), ale vyžaduje aj revíziu procesov: ***od správy kľúčov a auditov až po zvyšovanie kvalifikácie zamestnancov.***
- Strategickým cieľom je včasná adaptácia **na postkvantovú kryptografiu.**

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

Koncepcie a technológie vzdialeného prístupu a princípy zabezpečenia (VPN)

Nezabezpečený vzdialený prístup je právne aj bezpečnostne neakceptovateľný!

Čo je VPN

VPN (Virtual Private Network) je technológia, ktorá umožňuje bezpečne prepojiť vzdialeného používateľa so sieťou organizácie. Zabezpečuje:

- **šifrovanie prenášaných dát** – zabráni odpočúvaniu a manipulácii,
- **autentifikáciu používateľa** – overuje, že ide o oprávnenú osobu,
- **ochranu integrity spojenia** – zabezpečuje, že dáta počas prenosu neboli pozmenené.

Z pohľadu manažéra ide o **nevyhnutný prvok informačnej bezpečnosti** v organizáciách, ktoré umožňujú prácu na diaľku.

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

Manažérsky kontext vzdialeného prístupu

- **Zamestnanci často pracujú mimo organizácie** – *home office, služobné cesty, externí dodávatelia.*
- Vzdialený prístup **otvára cestu k systémom organizácie z vonkajšieho prostredia** → vysoké bezpečnostné riziko.
- Cieľom je umožniť **bezpečný, kontrolovaný a auditovateľný prístup** len oprávneným osobám (chrániť prenášané dáta pred odpočúvaním, manipuláciou alebo falšovaním, ako aj zabezpečiť, že prístup získajú len oprávnené osoby. **To sa dosahuje primárne vďaka kryptografickým technológiám**).

- Zabezpečenie vzdialeného prístupu nie je len technickou otázkou. Predstavuje **strategické rozhodnutie**, ktoré ovplyvňuje celkovú odolnosť organizácie voči kybernetickým hrozbám, plnenie zákonných povinností a pripravenosť na krízové situácie (*napr. pandémia, výpadky infraštruktúry*).

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

VPN

- **Virtuálne privátne siete (VPN)**: Najčastejšie využívaná technológia.
- Vytvára **šifrovaný tunel** cez verejnú sieť (internet), čím sa prenášané dáta stanú nečitateľnými pre tretie strany.
- Z hľadiska kryptografie sú kľúčové nasledujúce protokoly:
  - IPsec (AES)
  - SSL/TLS

- **IPsec (Internet Protocol Security)**: Sada protokolov na zabezpečenie komunikácie na sieťovej vrstve (3. vrstva).
- Zabezpečuje **autentizáciu**, **dôvernosť** a **integritu** dát. Využíva šifrovanie AES (Advanced Encryption Standard) a rôzne metódy výmeny kľúčov.
- **SSL/TLS (Secure Sockets Layer/Transport Layer Security)**: Protokoly, ktoré zabezpečujú webovú komunikáciu (používajú sa napríklad pri HTTPS) - 4. vrstva (transport).
- V kontexte VPN vytvárajú bezpečné spojenie prostredníctvom webového prehliadača alebo špeciálneho klienta. Bežne sa používa napríklad **OpenVPN**, ktorý je postavený práve na SSL/TLS.

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

Šifrovanie dát

- Všetky spomínané technológie využívajú šifrovanie. Dôležité je pochopiť rozdiel medzi symetrickou a asymetrickou kryptografiou
- Kryptografická ochrana citlivých údajov **musí vychádzať z verejných štandardov**, zahŕňať bezpečné generovanie kľúčov a zabezpečenie prenosu dát proti konvenčným aj pokročilým vektorom útoku.

- **Symetrické šifrovanie**: Používa ten istý kľúč na šifrovanie aj dešifrovanie dát (napr. AES). Je veľmi rýchle a efektívne, preto sa používa na **šifrovanie samotného dátového prenosu** v rámci VPN tunela.
- **Asymetrické šifrovanie (verejný/súkromný kľúč)**: Používa pár kľúčov – verejný na šifrovanie a súkromný na dešifrovanie. Je pomalšie, preto sa využíva hlavne na **výmenu šifrovacích kľúčov** (napr. pri SSL/TLS) alebo na **digitálne podpisy** a **autentizáciu**.

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

Autentizácia

- Zabezpečuje, že prístup má len oprávnený užívateľ. Vzdialený prístup by mal vždy vyžadovať silnú autentizáciu, ideálne **viacfaktorovú autentizáciu (MFA)**.
- **Tokeny a certifikáty**: Kryptografické certifikáty vydané certifikačnou autoritou sa používajú na overenie identity užívateľa alebo zariadenia.
- Tieto certifikáty obsahujú verejný kľúč, ktorý sa spáruje so súkromným kľúčom uloženým na zariadení používateľa.
- **Protokoly na autentizáciu**: Na overenie prístupových údajov a autorizáciu sa používajú protokoly ako, ktoré komunikujú s centrálnymi databázami užívateľov.

Prečo zabezpečiť vzdialený prístup?

- Zabezpečenie vzdialeného prístupu nie je len technickým opatrením, ale predovšetkým strategickým rozhodnutím, ktoré určuje, ako bude organizácia chrániť svoje informačné aktíva mimo vlastných fyzických priestorov.
  - **Výber vhodnej technológie**: Rozhodnúť, či je pre potreby organizácie vhodnejšia technológia A,B,C alebo kombinácia.
  - **Politiky a pravidlá**: Nastavenie prístupových pravidiel, napríklad, ktoré zariadenia môžu byť použité, aké sú požiadavky na heslá, a aké zdroje sú dostupné.
  - **Správa certifikátov a kľúčov**: Zabezpečenie správnej správy životného cyklu kryptografických kľúčov a certifikátov, vrátane ich generovania, distribúcie, a revokácie.
  - **Audity a monitorovanie**: Pravidelná kontrola a auditovanie pripojení na vzdialený prístup s cieľom odhaliť anomálie alebo podozrivú aktivitu.
  - **Plánovanie reakcie na incidenty**: Pripravenosť na to, čo robiť v prípade, že dôjde k narušeniu bezpečnosti vzdialeného prístupu.

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

Bezpečnostné princípy vzdialeného prístupu

- **Silná autentifikácia používateľa**
  - Minimálne dvojfaktorová (2FA), ideálne s použitím **certifikátu, tokenu alebo biometrie**.
  - Nepostačuje len používateľské meno a heslo.
- **Šifrovaná komunikácia**
  - Všetky dáta musia byť prenášané cez **šifrovaný kanál**.
  - Zabraňuje odpočúvaniu citlivých informácií (napr. prihlasovacích údajov).
- **Segmentácia a obmedzenie prístupových práv**
  - Používateľ z domu nemá mať rovnaké práva ako v kancelárii.
  - Princíp **najmenších potrebných oprávnení (least privilege)**.
- **Monitorovanie a audit**
  - Každý vzdialený prístup má byť **zaznamenaný**, logy sa pravidelne kontrolujú.
  - Pomáha pri detekcii podozrivej aktivity.

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

Príklady z hľadiska typov prístupu

Vzdialený prístup bez kryptografie = porušenie zákona.
Zákon predpokladá, že **vzdialený prístup je riadený, autentifikovaný a šifrovaný**.

Typ prístupu	Príklady technológií	Využitie
VPN	IPsec, SSL VPN	Pripojenie celého zariadenia do siete
Remote Desktop	RDP, VNC, Citrix	Práca na vzdialenej ploche bez prenosu dát
Cloud Access	M365, Google Workspace	Prístup cez prehliadač s centrálnou správou
Zero Trust Network Access (ZTNA)	Zscaler, Cloudflare Access	Dynamické overovanie identity a kontextu

Manažéri by mali:
- Určiť **politiku vzdialeného prístupu** – kto, kam, kedy, ako a prečo sa pripája.
- Zabezpečiť používanie **overených nástrojov** a **aktualizovaných klientov**.
- Vyžadovať **logovanie a revíziu prístupov** (v spolupráci s IT oddelením).

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

Príklady a chyby

Praktické scenáre

- **Home office zamestnanec:**
  - Pripojí sa cez VPN, autentifikuje sa smart kartou, získa len prístup na e-mail a interný portál.
  - Organizácia má záznam o každom pripojení.
- **Externý IT konzultant:**
  - Má pridelený izolovaný účet s časovo obmedzeným prístupom na vybrané servery.
  - Po ukončení spolupráce sa jeho certifikát okamžite revokuje.

Najčastejšie chyby v praxi

- Vzdialený prístup povolený bez šifrovania
- Prístup z osobných, nezabezpečených zariadení
- Neexistuje politika vzdialeného prístupu
- Chýba logovanie a detekcia anomálií

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

Príklady

Situácia: Firma má obchodného zástupcu, ktorý sa pripája z domu a potrebuje prístup k CRM systému.

Riešenie:

- Používa SSL VPN,
- autentifikuje sa pomocou certifikátu a hesla s MFA (aspoň 2 overenia – heslo, HW token, biometria) + overenie koncových bodov - overené PC s antivírusovým balíkom/aktualizáciami SW/šifrovaním disku/(Endpoint Security)
- má prístup len do CRM, nie do celej siete (Architektúra nulovej dôvery - ZeroTrust – ZTA) - znižuje riziko vstupu do iných aplikácií.

Výsledok: bezpečný, overený, šifrovaný prístup – súlad so zákonom aj s požiadavkami na dôvernosť údajov.

Čo sa máte pýtať?

- **Máme formálne schválenú VPN politiku?**
- **Používame moderné, podporované VPN protokoly (napr. WireGuard, IPsec, SSL VPN)?**
- **Je každý prístup monitorovaný a auditovaný?**
- **Sú prístupové práva a certifikáty pravidelne kontrolované a obnovované?**
- **Zvládne náš VPN systém nárast počtu používateľov v prípade krízového režimu (napr. lockdown)?**

Kritérium	IPsec VPN	SSL VPN	WireGuard
Šifrovanie	Silné	Silné	Najmodernejšie
Použitie	Sieťové prepojenia	Webové aplikácie	Všestranné
Zložitosť nasadenia	Vyššia	Nižšia	Nižšia
Výkon	Dobrý	Dobrý	Veľmi dobrý
Podpora zariadení	Široká	Široká	Rastúca

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

Zásady bezpečnej VPN z pohľadu manažéra - zhrnutie

- Pripojiť sa môže len známy používateľ (autentifikácia).
- Pristupuje len tam, kam má (segmentácia).
- Všetko, čo robí, sa zaznamenáva - logy (monitorovanie).
- Komunikácia je šifrovaná (dôvernosť).
- Prístup vie byť okamžite zrušený (správa).

Na záver príklady pre samohodnotenie

- Pri reálnom audite je stĺpec **„Dôkaz / Poznámka“** najdôležitejší.
- Audítorovi *by nemalo stačiť* vaše ústne „Áno“.
- Bude chcieť vidieť konkrétny **názov dokumentu**, **záznam, skeny,** alebo **screenshot konfigurácie/nastavení/výpisu**, na ktorý sa odvolávate a sú verifikovateľné.
- *Čo nie je zdokumentované, to sa nestalo.*

- *Tip: Vytvoriť digitálnu štruktúru priečinkov, ktorá kopíruje štruktúru vyhlášky.*

Príklady na samohodnotenie

61 – Pravidlá a metódy → *Cieľ: Zabezpečiť, aby organizácia mala stanovené, čo a ako sa šifruje. Poriadok v dokumentácii.*

Kontrolná otázka	Stav	Dôkaz / Poznámka (Príklad z praxe)
1. Existuje schválená Kryptografická politika?	**ÁNO**	Smernica ISMS_05_Kryptografia_v2.pdf schválená dňa 1.2.2025. Definuje povinné použitie AES-256 pre dáta v pokoji a TLS 1.3 pre prenos.
2. Sú zakázané zastarané algoritmy?	**ÁNO**	V kap. 4 smernice je explicitný **zákaz** používania MD5, SHA-1 a DES. Audit z 03/2025 potvrdil odstránenie posledného výskytu na starom file serveri.
3. Sú pokryté požiadavky legislatívy a tretích strán?	**ÁNO**	Politika odkazuje na čl. 32 GDPR (šifrovanie osobných údajov). V zmluve s dodávateľom cloudu je vynútené šifrovanie na strane klienta.
4. Je vynútená dôvernosť pri prenose dát? **.....**	**ÁNO** **.....**	Emailová brána automaticky šifruje odchádzajúce maily s príznakom „Dôverné“. Interný webový portál beží výhradne na HTTPS. ……

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

Príklady na samohodnotenie

62 – Efektívne používanie a kľúče → *Cieľ: Zabezpečiť, aby "kľúče od aktíva" boli v bezpečí.*

Kontrolná otázka	Stav	Dôkaz / Poznámka (Príklad z praxe)
5. Je zavedený systém správy kľúčov (KMS)?	**ÁNO**	Nasadený centrálny KMS (napr. HashiCorp Vault / AWS KMS). Kľúče nie sú hard-codeované v zdrojovom kóde aplikácií.
6. Existuje proces pre rotáciu kľúčov?	**ÁNO**	Automatizovaná rotácia SSL certifikátov každých 90 dní. Hlavné šifrovacie kľúče (Master Keys) sa rotujú ročne (posledná rotácia: 15.9.2025).
7. Sú kľúče bezpečne generované?	**ÁNO**	Pre generovanie kľúčov sa používa certifikovaný Hardvérový bezpečnostný modul (HSM), nie softvérový generátor na bežnom PC.
8. Existuje plán reakcie na kompromitáciu kľúča? **……..**	**ÁNO** **……..**	Súčasťou Incident Response Plan je scenár č. 4: „Únik privátneho kľúča“. Test revokácie (zneplatnenia) prebehol úspešne dňa 10.10.2025. ……

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

Príklady na samohodnotenie

63 – Prehodnocovanie -> Cieľ: Preukázať, že bezpečnosť je trvalá a kontrolovaná.

Kontrolná otázka	Stav	Dôkaz / Poznámka (Príklad z praxe)
9. Bolo vykonané prehodnotenie za posledných 12 mesiacov?	**ÁNO**	Externý penetračný test a audit kryptografie prebehol v marci 2025. Overovala sa sila šifier na verejných rozhraniach.
10. Existuje formálny záznam o prehodnotení?	**ÁNO**	Záznam Audit_Report_Crypto_2025_FINAL je podpísaný CISO a archivovaný v DMS systéme pre potreby kontroly.
11. Boli odstránené zistené nedostatky? **.....**	**ÁNO** **....**	Audit zistil slabú konfiguráciu na VPN bráne. Riziko bolo zaevidované a oprava (patch + zmena konfigurácie) prebehla do 48 hodín. .....

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

Príklady na samohodnotenie

Praktická aplikácia (VPN a OT)

Príklad pre organizáciu s hybridnou prácou a priemyselnými technológiami.

Kontrolná otázka	Stav	Dôkaz / Poznámka (Príklad z praxe)
12. Je VPN prístup šifrovaný a silne autentifikovaný?	**ÁNO**	Používame IPsec VPN klienta. Vyžaduje sa certifikát zariadenia (stroj) + heslo používateľa + mobilný token (MFA).
13. Sú heslá v databázach hashované?	**ÁNO**	Kontrola DB admina potvrdila, že stĺpec s heslami obsahuje reťazce SHA-256 (alebo Argon2) so soľou (salt). Žiadny plain-text.
14. Je v OT prostredí klasifikácia dát pre šifrovanie?	**ÁNO**	Dokument OT_Data_Classification určuje, že dáta z SCADA servera do cloudu musia ísť cez šifrovaný MQTT tunel.
15. Sú riadiace príkazy v OT chránené proti zmene?	**ÁNO**	Príkazy pre PLC na úrovni L3 sú digitálne podpísané. Ak by útočník zmenil príkaz „Stop“ na „Start“, systém to odmietne pre zlý podpis.

Príklad digitálnej štruktúry pre účel časti 61,62,63

- 01_Riadenie_a_Politiky_(Polozka_61)
  - 01_Kryptograficka_Politika.pdf
  - 02_Smernica_Spravy_Klucov.pdf
  - 03_Klasifikacia_Informacii_IKT_a_OT.pdf
- 02_Technicka_Implementacia_a_Konfiguracie_(Polozka_61_a_102)
  - A_Web_a_Prenos_(TLS_HTTPS)
  - B_Vzdialeny_Pristup_(VPN)
  - C_OT_Systemy_(SCADA_PLC)
- 03_Sprava_Klucov_a_Certifikatov_(Polozka_62)
  - A_Inventar_Klucov
  - B_Zaznamy_o_Rotacii
  - C_Revokacia_a_Likvidacia
- 04_Previerky_a_Testy_Odolnosti_(Polozka_63)
  - 01_Rocne_Prehodnotenie_Kryptografie_2025.pdf
  - 02_Vysledky_Pentestov_a_Skenov.pdf
  - 03_Zaznam_o_Odstraneni_Zranitelnosti.pdf
- 05_Logy_a_Prevadzka_(Auditna_Stopa)
  - 01_Logy_VPN_Pristupov.csv
  - 02_Logy_KMS_Systemu.csv

Ďalšie relevantné zdroje

- IBM Technology (videá – rôzne témy v oblasti Cybersecurity, AI, ...) https://www.youtube.com/@IBMTechnology/playlists
  - Kyberbezpečnosť a trendy (2025) https://www.youtube.com/watch?v=kqaMIFEz15s
- Základy kryptografie (videá) https://www.youtube.com/playlist?list=PL7d8iOq_0_CWAfs_z4oQnCuVc6yr7W5Fp
- Medium.com – Cybersecurity - https://medium.com/tag/cybersecurity
- https://www.bleepingcomputer.com/
- https://thehackernews.com/
- https://www.darkreading.com/
- https://krebsonsecurity.com/
- https://blogs.cisco.com/security
- .....
- https://csirt.sk/ aktuálne správy v SR / mesačné správy

Ostatné

- ODPORÚČANIE KOMISIE z 11. 4. 2024 o Pláne koordinovaného vykonávania prechodu na postkvantovú kryptografiu (súvis s plánovaným zákonom o kvantovej regulácii)

https://ec.europa.eu/newsroom/dae/redirection/document/104251

- European Union Agency for Cybersecurity - https://www.enisa.europa.eu/
- EU certifikácia v kyberbezpečnosti (napr. HW) https://www.enisa.europa.eu/publications/voices-of-eu-cybersecurity-certification
- https://certification.enisa.europa.eu/certificates_en?prefLang=sk
- Quantum Readiness https://quantumready.eu/

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

Kryptografické opatrenia a zásady používania kryptografie

Technické opatrenia (Blok IV)

Kurz: Manažér kybernetickej bezpečnosti

Ing. Ladislav Mariš, PhD.

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

ladislav.maris@uniza.sk