KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

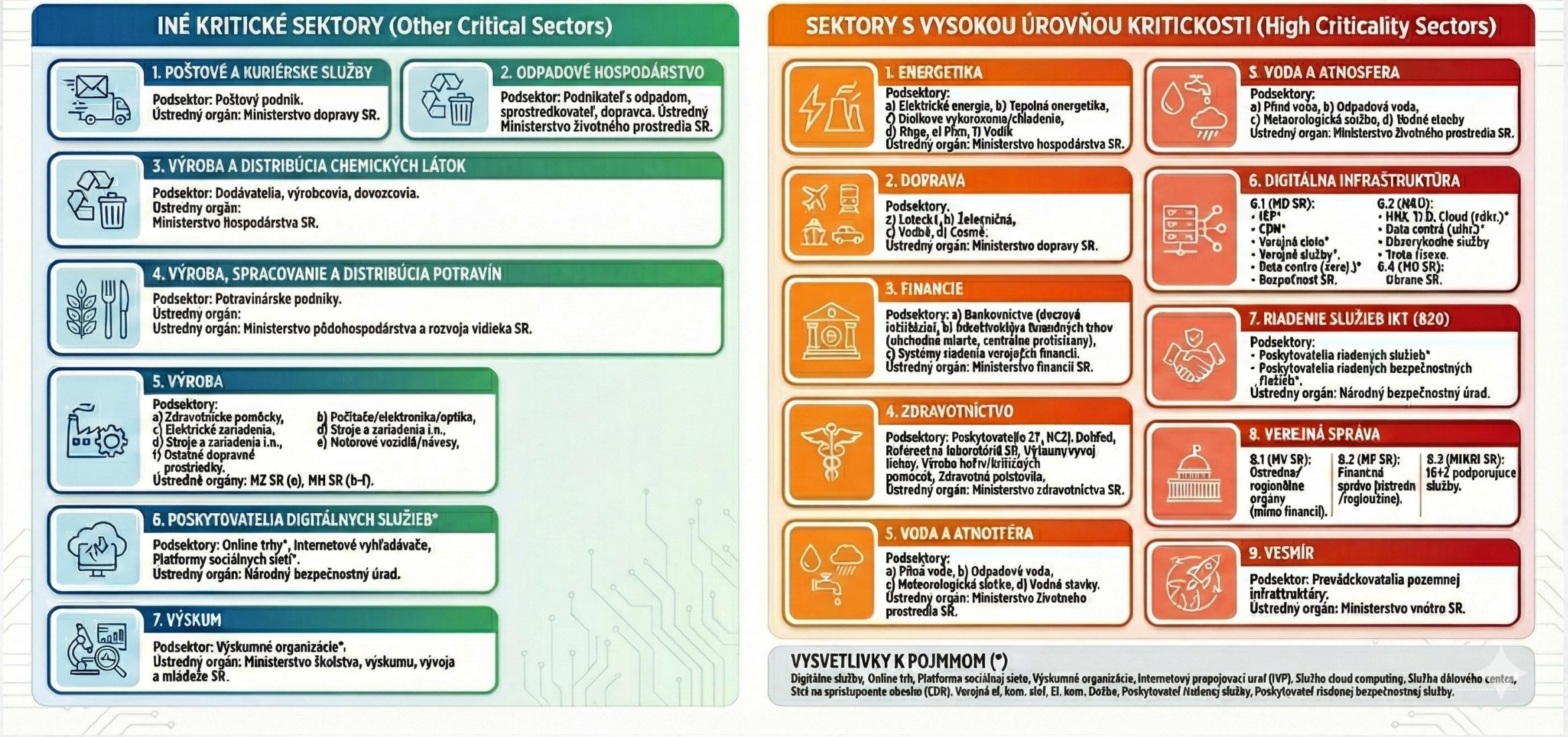
Subjekty v kybernetickej bezpečnosti

Meno a priezvisko

XX.XX.XXXX

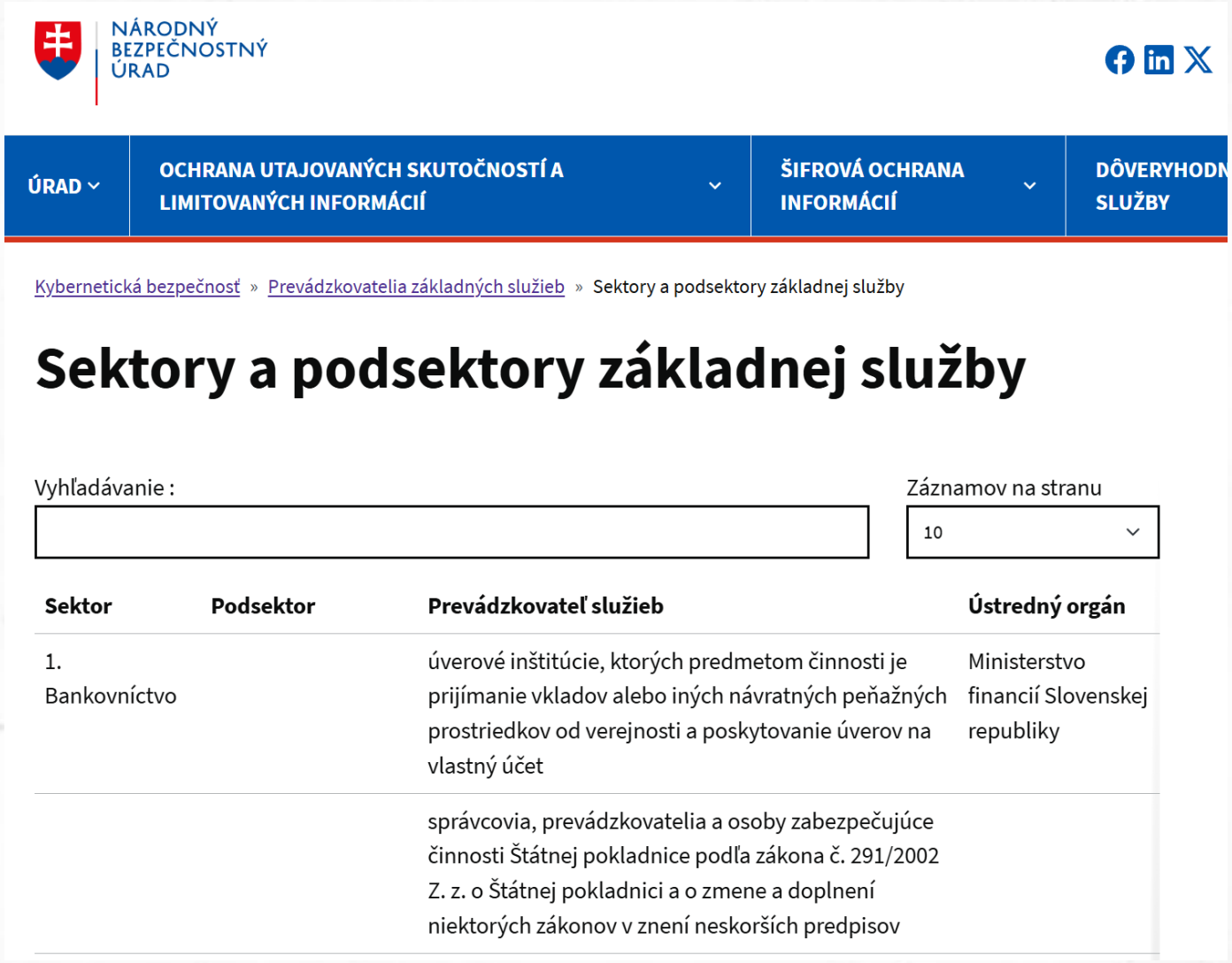
KCKB UPJS CSIRT UPJS

Sektory v kybernetickej bezpečnosti (I.)



Zdroj: Obrázok vygenerovaný AI: Gemini

Sektory v kybernetickej bezpečnosti (II.)



NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

ÚRAD | OCHRANA UTAJOVANÝCH SKUTOČNOSTÍ A LIMITOVANÝCH INFORMÁCIÍ | ŠIFROVÁ OCHRANA INFORMÁCIÍ | DÔVERYHODN SLUŽBY

Kybernetická bezpečnosť » Prevádzkovatelia základných služieb » Sektory a podsektory základnej služby

Sektory a podsektory základnej služby

Vyhľadávanie :

Záznamov na stranu 10

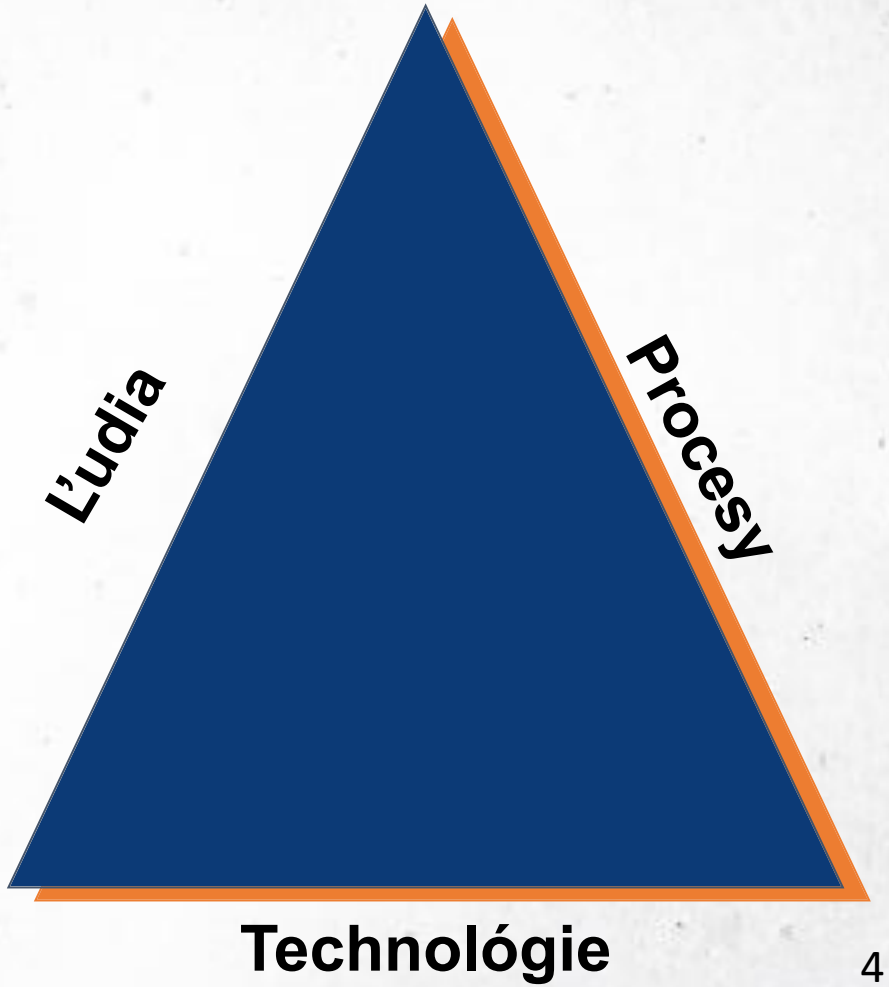
Sektor	Podsektor	Prevádzkovateľ služieb	Ústredný orgán
1. Bankovníctvo		úverové inštitúcie, ktorých predmetom činnosti je prijímanie vkladov alebo iných návratných peňažných prostriedkov od verejnosti a poskytovanie úverov na vlastný účet	Ministerstvo financií Slovenskej republiky
		správcovia, prevádzkovatelia a osoby zabezpečujúce činnosti Štátnej pokladnice podľa zákona č. 291/2002 Z. z. o Štátnej pokladnici a o zmene a doplnení niektorých zákonov v znení neskorších predpisov	

Zdroj: https://www.nbu.gov.sk/sektory-a-podsektory-zakladnej-sluzby/

Subjekty v oblasti kybernetickej bezpečnosti

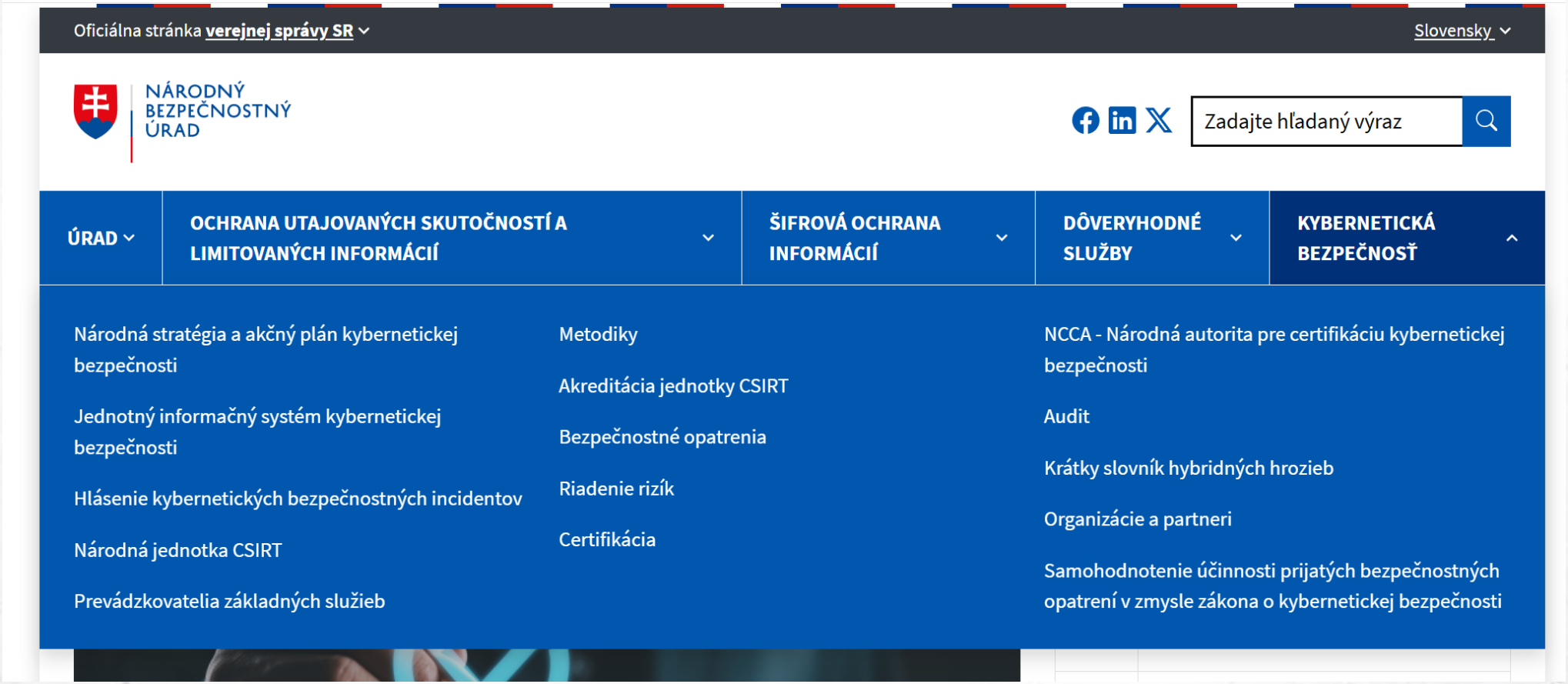
- kybernetická bezpečnosť - ide o prepojenie procesov, ľudí a technológií

- Národný bezpečnostný úrad (§ 5 ZoKB)
- Ústredný orgán (§ 9 ZokB)
- Jednotky CSIRT
  - Národná jednotka CSIRT (§ 6 ZoKB)
  - Vládna jednotka CSIRT (§ 11 ZokB)
  - Akreditovaná jednotka CSIRT (§ 14 ZoKB)
- Prevádzkovateľ základnej služby (§ 17 ZoKB)
- Prevádzkovateľ kritickej základnej služby



Národná bezpečnostný úrad (I.)

- Národný bezpečnostný úrad - § 5 ZoKB



Zdroj: https://www.nbu.gov.sk/

Národná bezpečnostný úrad (II.)

- **Národná stratégiu kybernetickej bezpečnosti**
- § 7 ZoKB
- východiskový strategický dokument, ktorý komplexne určuje strategický prístup Slovenskej republiky

Oficiálna stránka verejnej správy SR Slovensky

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Menu

Aktualita

Vláda SR prijala Národnú stratégiu kybernetickej bezpečnosti na roky 2026 – 2030

Vypublikované 4. 02. 2026

Vláda Slovenskej republiky v stredu schválila Národnú stratégiu kybernetickej bezpečnosti na roky 2026 až 2030, ktorú predložil Národný bezpečnostný úrad (NBÚ). Strategický dokument určuje smerovanie Slovenska v oblasti kybernetickej bezpečnosti na nasledujúcich päť rokov.

Zdroj: https://www.nbu.gov.sk/vlada-sr-prijala-narodnu-strategiu-kybernetickej-bezpecnosti-na-roky-2026-2030/

Ústredný orgán (I.)

- Ústredný orgán (§ 9 ZokB) - zodpovedá za zabezpečenie kybernetickej bezpečnosti v sektore tým, že:
  - plní úlohy jednotky CSIRT
  - poskytuje NBÚ požadovanú súčinnosť a informácie
  - spolupracuje s ostatnými ústrednými orgánmi a prevádzkovateľmi základnej služby
  - buduje bezpečnostné povedomie, koordinovanú spoluprácu
  - aplikuje bezpečnostné opatrenia a politiku správania sa v kybernetickom priestore,
  - identifikuje prevádzkovateľa základnej služby
  - spolupracuje so zahraničnou inštitúciou obdobného zamerania.

Ústredný orgán (II.)

Sektor	Podsektor / Špecifikácia	Ústredný orgán
Energetika	Elektrina, Plyn, Ropa, Teplo, Vodík	Ministerstvo hospodárstva SR
Doprava	Letecká, Železničná, Vodná, Cestná	Ministerstvo dopravy SR
Bankovníctvo	Úverové inštitúcie	Ministerstvo financií SR
Infraštruktúra fin. trhov	Obchodné miesta, centrálne protistrany	Ministerstvo financií SR
Zdravotníctvo	Poskytovatelia ZS, laboratóriá, výroba liekov	Ministerstvo zdravotníctva SR
Voda	Pitná voda, Odpadová voda	Ministerstvo životného prostredia SR
Digitálna infraštruktúra	DNS, TLD, Cloud, Data centrá, Dôveryhodné služby	Národný bezpečnostný úrad (NBÚ)
	Elektronické komunikácie	Ministerstvo dopravy SR
	Vládne systémy (Bezpečnosť štátu / Obrana)	Min. vnútra SR / Min. obrany SR
Riadenie služieb IKT	Managed Service Providers (B2B)	Národný bezpečnostný úrad (NBÚ)
Verejná správa	Ústredná a regionálna správa	Ministerstvo vnútra SR
	Finančná správa	Ministerstvo financií SR
	Informačné systémy verejnej správy (ISVS)	MIRRI SR
Vesmír	Pozemná infraštruktúra	Ministerstvo vnútra SR
Poštové služby	Kuriérske a poštové služby	Ministerstvo dopravy SR
Odpadové hospodárstvo	Nakladanie s odpadom (okrem bežného zberu)	Ministerstvo životného prostredia SR
Chemický priemysel	Výroba a distribúcia chemických látok	Ministerstvo hospodárstva SR
Potravinárstvo	Výroba, spracovanie a distribúcia	Min. pôdohospodárstva a rozvoja vidieka SR
Výroba	Zdravotnícke pomôcky	Ministerstvo zdravotníctva SR
	Elektronika, stroje, vozidlá, optika	Ministerstvo hospodárstva SR
Digitálne služby	Online trhoviská, vyhľadávače, soc. siete	Národný bezpečnostný úrad (NBÚ)
Výskum	Výskumné organizácie	Min. školstva, výskumu, vývoja a mládeže SR

Jednotky CSIRT (I.)

- **CSIRT** (computer security incident response team) – tím na riešenie počítačových bezpečnostných incidentov
  - Činnosti CSIRT/CERT tímov
    - reaktívne činnosti
    - proaktívne činnosti
  - Medzinárodné zoskupenia - TF-CSIRT, FIRST, CSIRT network

Jednotky CSIRT (II.)

- Jednotky CSIRT:
  - musia spĺňať podmienky akreditácie podľa § 14 ZoKB
  - musia plniť úlohy jednotky CSIRT podľa § 15 ZoKB

- **Akreditácia jednotky CSIRT** (§ 13 a 14 ZoKB) – jednotka CSIRT:
  - má požadované technické, technologické a personálne vybavenie
  - má vytvorené podmienky umožňujúce chránený prenos a spracovanie údajov
  - chráni informácie a údaje,
  - má umiestnenú dokumentáciu, informačné systémy a ostatné informačno-komunikačné technológie v zabezpečenom priestore

Jednotky CSIRT (III.)

- Vyhláška NBÚ č. 166/2018 Z. z. o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov

166

VYHLÁŠKA

Národného bezpečnostného úradu

z 1. júna 2018

o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov

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

§ 1

Táto vyhláška ustanovuje podrobnosti technického, technologického a personálneho vybavenia jednotky pre riešenie kybernetických bezpečnostných incidentov (ďalej len „jednotka CSIRT“), ktorých náležitosti a spôsob splnenia sa preukazujú na účely akreditácie jednotky CSIRT podľa **§ 13 zákona**.

§ 2

(1) Požadované vybavenie jednotky CSIRT podľa **§ 14 písm. a) zákona** sa preukazuje splnením

a) technických podmienok, ktoré zahŕňajú technicko-organizačné podmienky a technicko-procesné podmienky,

b) personálnych podmienok a

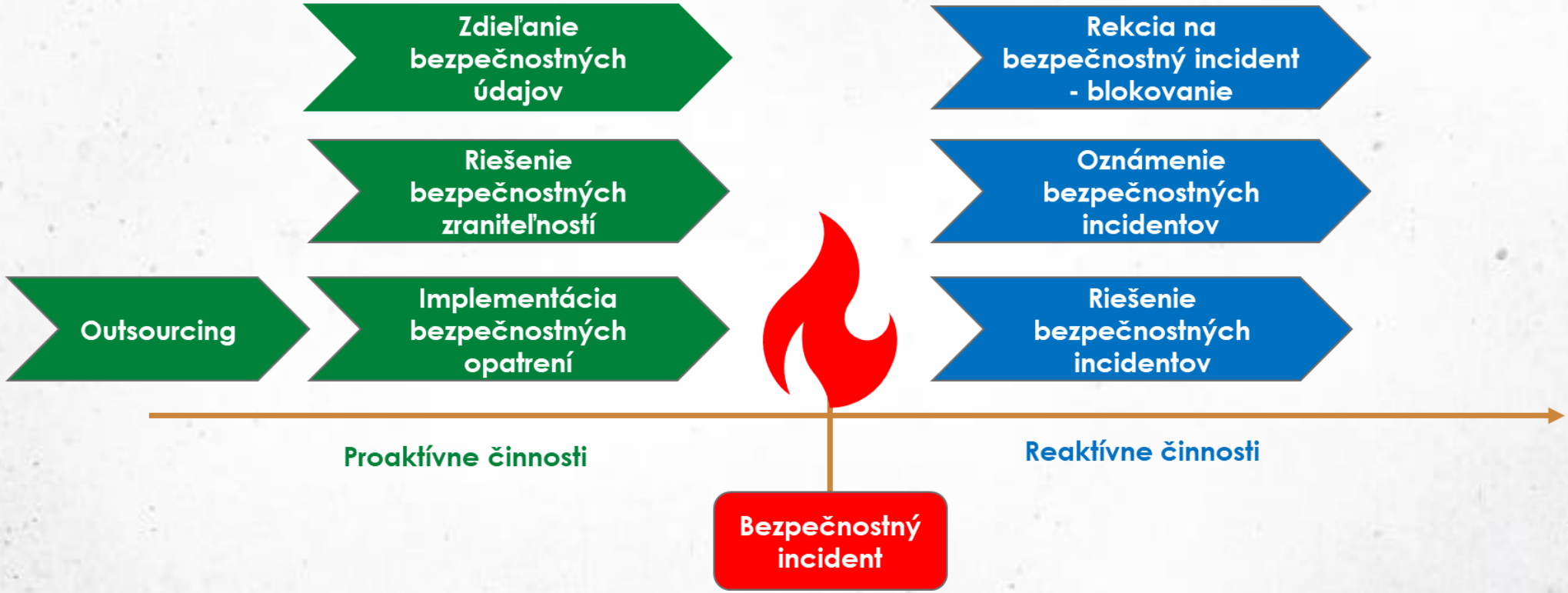
c) technologických podmienok.

(2) Splnenie podmienok podľa odseku 1 sa preukazuje dokumentom tak, že k takému dokumentu má prístup a je s ním preukázateľne oboznámený každý pracovník jednotky CSIRT, ktorý plní úlohy tejto jednotky CSIRT, a to vo forme záväzného interného predpisu vydaného orgánom verejnej moci podľa **§ 4 písm. b) zákona**.

(3) Dokument podľa odseku 2 je súčasťou dokumentácie preukazujúcej splnenie podmienok akreditácie jednotky CSIRT podľa **§ 14 zákona**.

Jednotky CSIRT (IV.)

- úlohy jednotky CSIRT podľa § 15 ZoKB
  - ten, kto plní úlohy jednotky CSIRT v rozsahu svojej pôsobnosti zodpovedá za riešenie kybernetických bezpečnostných incidentov
  - vykonáva preventívne služby a reaktívne služby



Jednotky CSIRT (V.)

- **preventívne služby** (§ 15 ods. 2 ZoKB):
  - vytváranie bezpečnostného povedomia, výcvik,
  - spolupráca, monitorovanie zraniteľností, kybernetických hrozieb, kríz a incidentov
  - ...

- **reaktívne služby** (§ 15 ods. 3 ZoKB):
  - Výstrahy a varovania
  - Detekcia, analýza, odozva, asistencia, reakcia na kybernetické bezpečnostné incidenty,
  - ...

Jednotky CSIRT (VI.)

Zoznam akreditovaných jednotiek CSIRT

Vyhľadávanie :

Záznamov na stranu 10

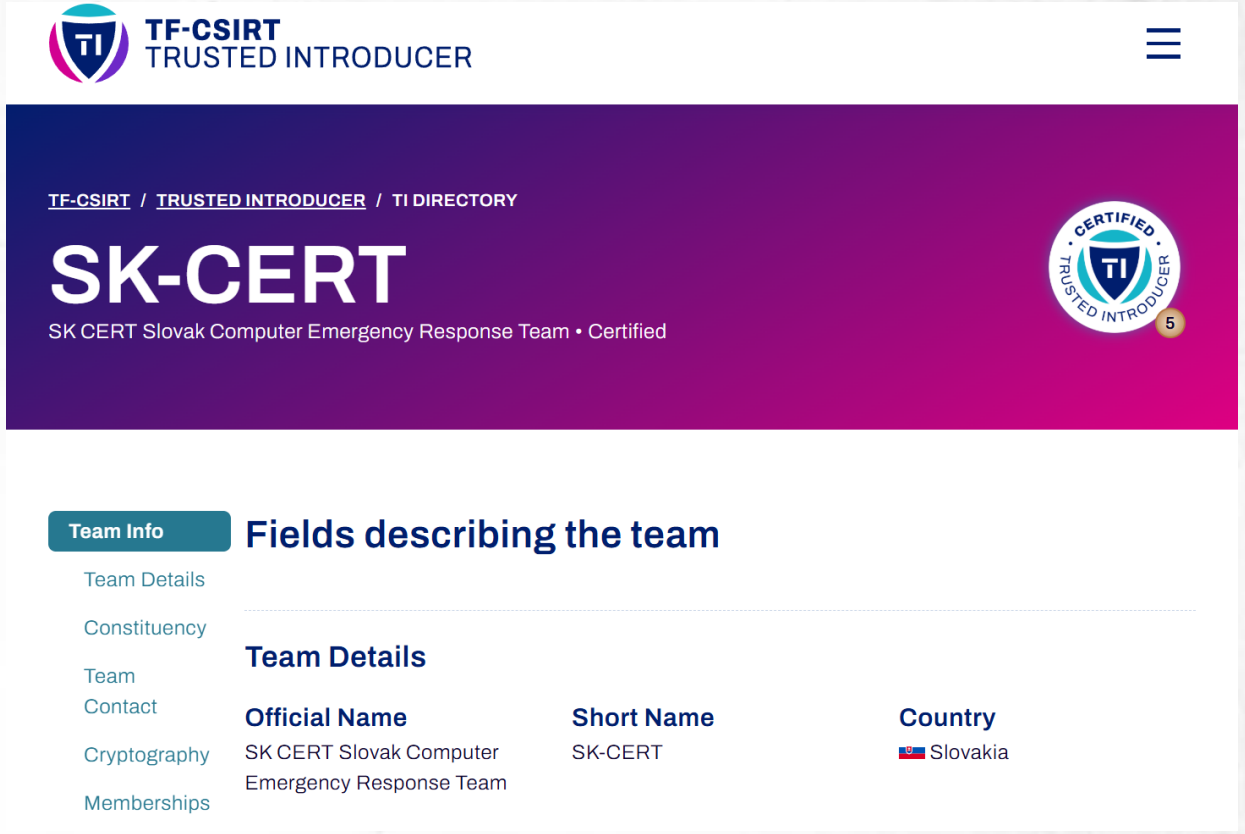
Prevádzkovateľ jednotky	Označenie jednotky	Typ jednotky	Sídlo	Telefón	Fax	e-mail	PGP komunikácia
Centrum pre kybernetickú obranu Slovenskej republiky	CSIRT.MIL.SK	Jednotka CSIRT	Kutuzovova 8, 832 47 Bratislava	421 960 11 22 33	421 960 314 688	cyber@mosr.sk	údaje pre PGP komunikáciu
Národný bezpečnostný úrad	SK-CERT	Národná jednotka CSIRT	Budatínska 30, 851 06 Bratislava	421 2 6869 1111	421 2 6869 1700	sk-cert(at)nbu.gov.sk	údaje pre PGP komunikáciu
Ministerstvo investícií, regionálneho rozvoja a informatizácie SR	CSIRT.SK	Vládna jednotka CSIRT	Pribinova 25, 811 09 Bratislava	421 2 2092 8786/421 2 2092 8804		info(at)csirt.gov.sk	údaje pre PGP komunikáciu

Zobrazuje sa 1 - 3 z 3 záznamov

Zdroj: https://www.nbu.gov.sk/7283-sk/zoznam-akreditovanych-jednotiek-csirt/

Jednotky CSIRT (VII.)

- **Národná jednotka CSIRT - Národné centrum kybernetickej bezpečnosti (§ 6 ZoKB)**
  - organizačná zložka NBÚ
  - postavenie národnej jednotky CSIRT s pôsobnosťou pre SR
  - SK-CERT
  - pre všetky sektory a podsektory uvedené v prílohe č. 1 alebo v prílohe č. 2 ZoKB okrem tých sektorov a podsektorov, pre ktoré plní úlohy jednotky CSIRT ústredný orgán.
  - plní úlohu ústredného orgánu, ak tento orgán túto úlohu nezabezpečí



Zdroj: https://www.trusted-introducer.org/trusted-introducer/directory/teams/sk-cert/

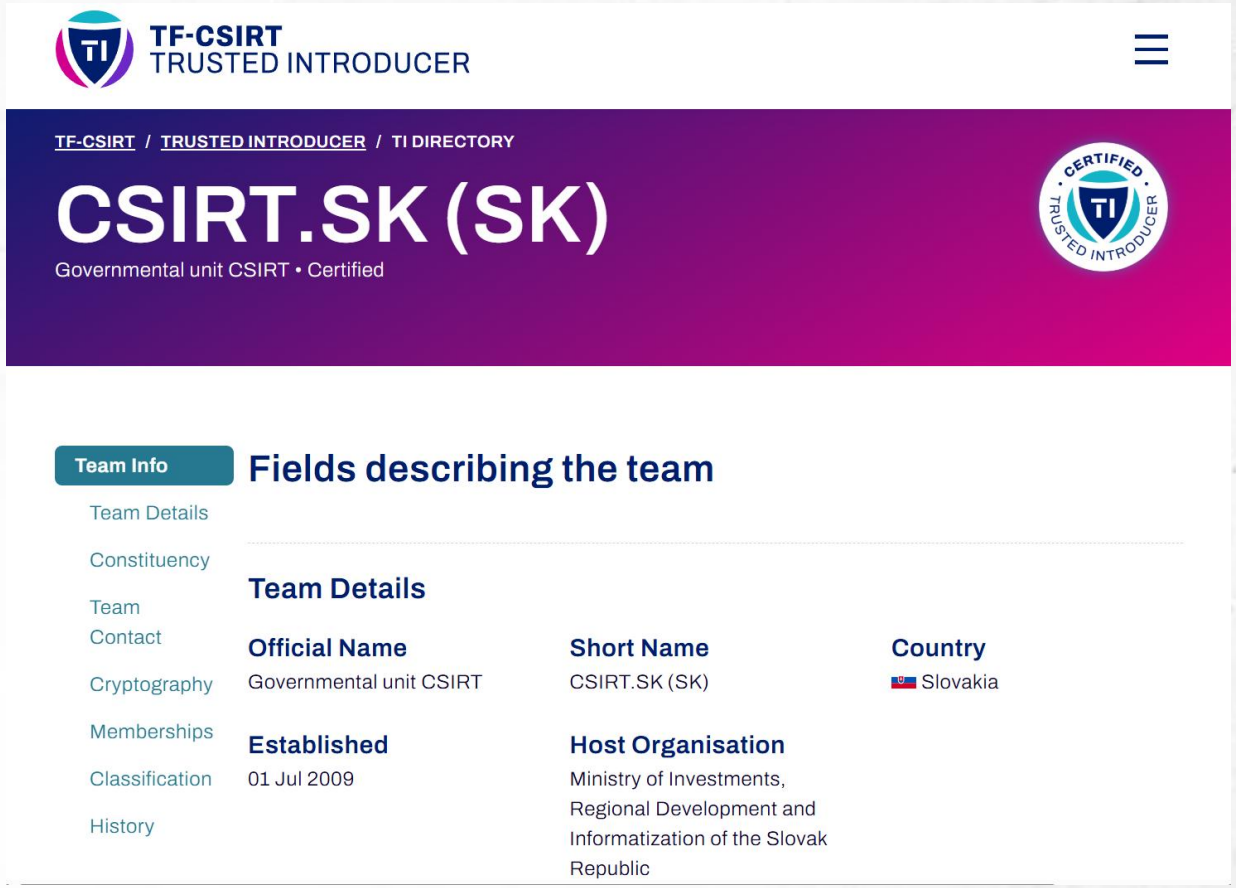
Jednotky CSIRT (VIII.)

- **Sieť národných jednotiek CSIRT**
  - smernica NIS2 (čl. 15)
  - prispieť k zvyšovaniu dôvery a podporiť rýchlu a účinnú operačnú spoluprácu medzi členskými štátmi sa zriaďuje
  - skladá sa zo zástupcov jednotiek CSIRT, orgánoch a agentúrach Únie (CERT-EU).
  - agentúra ENISA zabezpečuje sekretariát a aktívne pomáha so spoluprácou medzi jednotkami CSIRT.

Zdroj: https://csirtsnetwork.eu/#about

Jednotky CSIRT (IX.)

- **Vládna jednotka CSIRT (§ 11 ZoKB)**
  - CSIRT.SK
  - v pôsobnosti Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky
  - pre podsektor informačné systémy verejnej správy.
  - zaraďuje do zoznamu akreditovaných jednotiek CSIRT.



Zdroj: https://www.trusted-introducer.org/trusted-introducer/directory/teams/csirtsk-sk/

Prevádzkovateľ základnej služby (I.)

- **Subjekty v smernici NIS 2**
  - rozdelenie subjektov podľa rozsahu, v akom sú kritické, pokiaľ ide o ich odvetvie alebo druh služieb, ktoré poskytujú, ako aj ich veľkosti
  - dôležitý subjekt – ostatné významné sektory
  - kľúčový subjekt – dôležitejšie, kritické sektory

- **Zákon o KB**
  - prevádzkovateľ základnej služby (= dôležitý subjekt)
  - prevádzkovateľ kritickej základnej služby (= kľúčový subjekt)

Prevádzkovateľ základnej služby (II.)

- **Prevádzkovateľom základnej služby** je ten, kto je zapísaný v registri prevádzkovateľov základnej služby (§ 3 ods. 2 ZoKB)

- Do **registra prevádzkovateľov základnej služby** sa zapisuje (§ 17 ods. 1 ZoKB):
  - a) **ústredný orgán štátnej správy** a iný štátny orgán s celoštátnou pôsobnosťou
  - b) **kritický subjekt**,
  - c) osoba bez ohľadu na splnenie podmienok veľkosti pre stredný podnik, ktorá vykonáva činnosť v niektorom zo sektorov podľa prílohy č. 1 alebo prílohy č. 2 a ktorá
  - d) **štátny orgán vykonávajúci pôsobnosť v najmenej dvoch okresoch** a **vyšší územný celok**, ak by narušenie ich činnosti mohlo mať významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie

Prevádzkovateľ základnej služby (III.)

- Do registra prevádzkovateľov základnej služby sa zapisuje (§ 17 ods. 1 ZoKB):
  - e) osoba, ktorá spĺňa **najmenej podmienky veľkosti pre stredný podnik** a vykonáva činnosť v niektorom zo sektorov podľa prílohy č. 1 alebo prílohy č. 2,
  - f) mesto, ak by narušenie výkonu jeho pôsobnosti mohlo mať **významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie**,
  - g) **správca informačnej technológie verejnej správy**
  - h) osoba, ktorá poskytuje službu **registrácie názvu domény** bez ohľadu na splnenie podmienok veľkosti pre stredný podnik
  - i) **tretia strana, ktorá má významný vplyv** pri zabezpečovaní kybernetickej bezpečnosti, a má uzatvorenú zmluvu s prevádzkovateľom základnej služby, ktorý prevádzkuje kritickú základnú službu.

Prevádzkovateľ základnej služby (IV.)

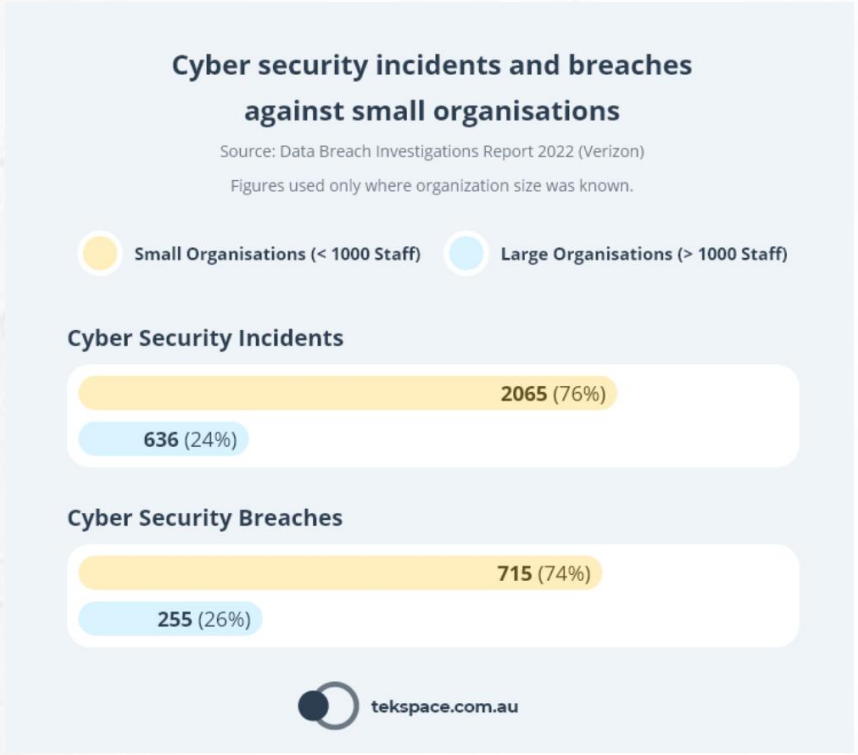
- § 17 ods. 1 písm. c) ZoKB - osoba bez ohľadu na splnenie podmienok veľkosti pre stredný podnik, ktorá vykonáva činnosť v niektorom zo sektorov podľa prílohy č. 1 alebo prílohy č. 2 a ktorá
  - 1. je podnikom poskytujúcim verejnú elektronickú komunikačnú sieť alebo verejnú elektronickú komunikačnú službu,
  - 2. je poskytovateľom dôveryhodnej služby (certifikáty, elektronické podpisy, ...),
  - 3. je správcom TLD (domény najvyššej úrovne),
  - 4. poskytuje službu DNS,
  - 5. je v SR jediným poskytovateľom služby, ktorá je kľúčovou službou,
  - 6. poskytuje službu, ktorej narušenie by mohlo mať významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie,
  - 7. poskytuje službu alebo má také postavenie, že narušenie poskytovania služby alebo zásah do postavenia by mohli vyvolať významné systémové riziko
  - 8. je vzhľadom na svoj osobitný význam na vnútroštátnej alebo regionálnej úrovni kritická pre konkrétny sektor, alebo
  - 9. je subjektom hospodárskej mobilizácie, ktorému bolo uložené opatrenie podľa osobitného predpisu,

Prevádzkovateľ základnej služby (V.)

- **Prevádzkovateľom kritickej základnej služby** - ak prevádzkovateľ základnej služby vykonáva aspoň 1 z kritických základných služieb:
  - a) výkon pôsobnosti ústredného orgánu štátnej správy alebo iného štátneho orgánu s celoštátnou pôsobnosťou,
  - b) činnosť v sektore podľa prílohy č. 1, okrem sektoru verejná správa, ak ju vykonáva osoba, ktorá prekračuje limity veľkosti určené pre stredný podnik,
  - c) kvalifikovaná dôveryhodná služba,
  - d) správa TLD,
  - e) služba DNS,
  - f) poskytovanie verejnej elektronickej komunikačnej siete alebo verejnej elektronickej komunikačnej služby osobou, ktorá dosahuje najmenej podmienky veľkosti pre stredný podnik,
  - g) vykonávanie činnosti alebo existencia postavenia podľa § 17 ods. 1 písm. c) piateho až deviateho bodu,
  - h) poskytovanie základnej služby kritickým subjektom, alebo
  - i) informačná činnosť a elektronické služby, vykonávané s použitím informačnej technológie verejnej správy, určených NBÚ.

Prevádzkovateľ základnej služby (VI.)

- menšie podniky sú tiež cieľmi útokov
- útočníci sa zameriavajú na každého z nás



Zdroj: https://tekspace.com.au/articles/cyber-security-myths-misconceptions/, https://tvnoviny.sk/domace/clanok/932340-novy-typ-podvodu-cieli-na-seniorov-na-vylakanie-penazi-zneuzivaju-telefony

Prevádzkovateľ základnej služby (VII.)

- aj menšie podniky spadajú pod regulácie smernice NIS 2 a zákona o KB

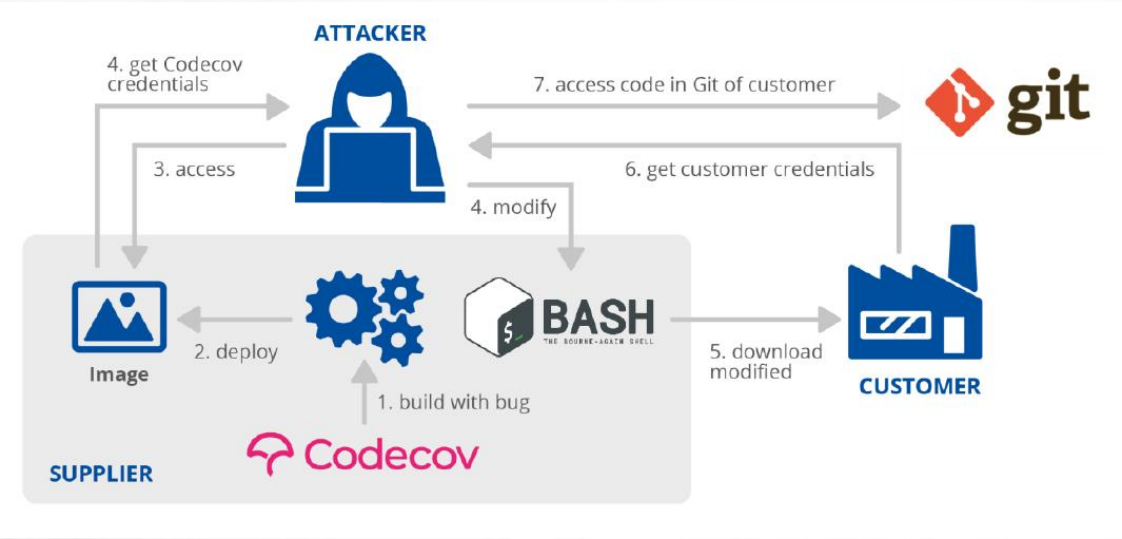
- § 17 ods. 1 písm. e) zákona o KB - osoba, ktorá spĺňa najmenej podmienky **veľkosti pre stredný podnik** a vykonáva činnosť v niektorom zo sektorov podľa prílohy č. 1 alebo prílohy č. 2 zákona o KB

- odporúčanie Komisie 2003/361/ES
- **viac ako 50** zamestnancov a
- obrat alebo súvaha **nad 10 mil. €**

Zdroj: https://www.nbu.gov.sk/novela-kyberzakona-je-predo-dvermi-nbu-zverejnil-pomocku-pre-organizacie/

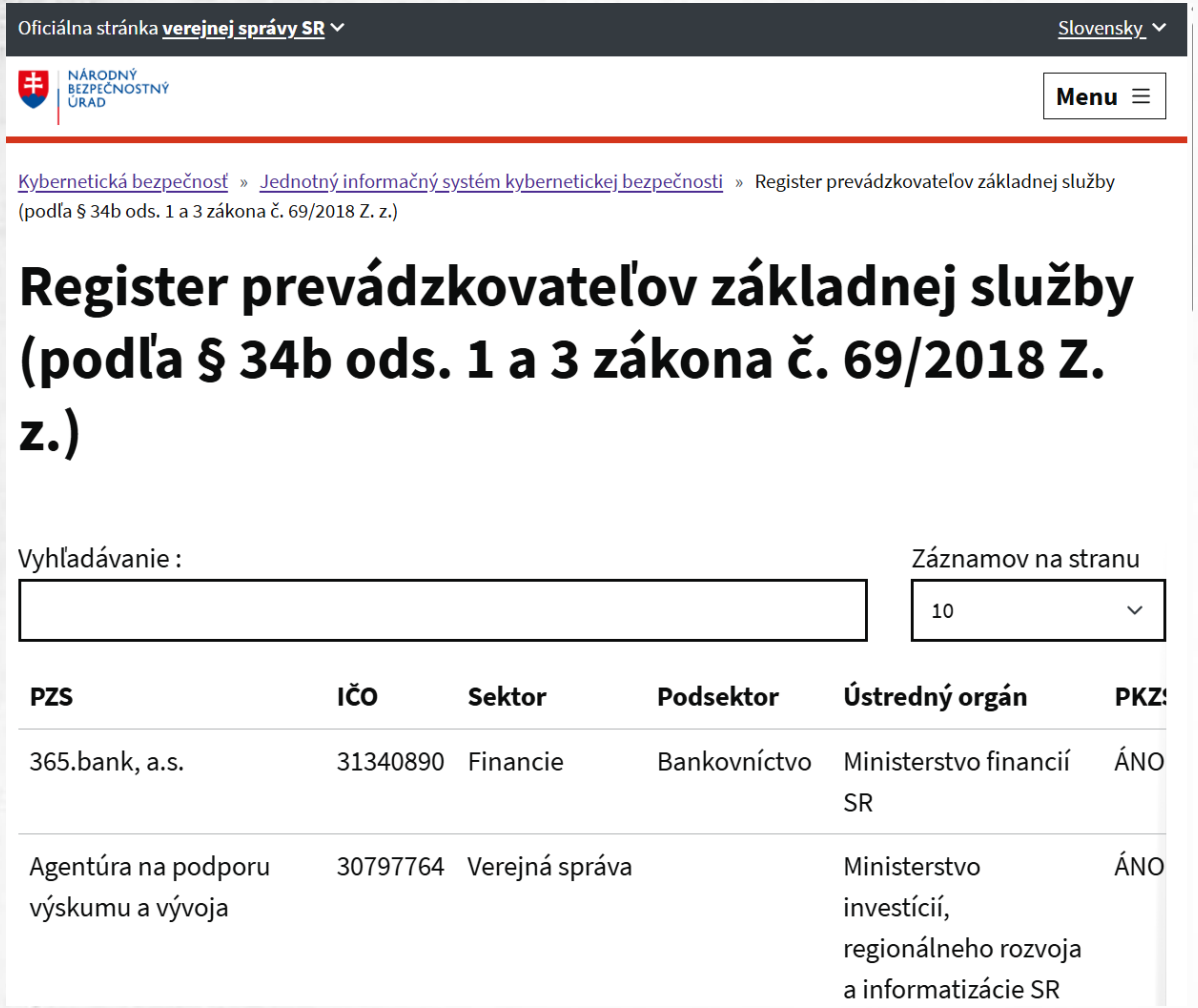
Prevádzkovateľ základnej služby (VIII.)

- rozšírenie pôsobnosti na **dodávateľské reťazce (riešenie hrozby dodávateľského reťazca)**
- § 17 ods. 1 písm. i) zákona o KB - tretia strana, ktorá má významný vplyv pri zabezpečovaní kybernetickej bezpečnosti, a má uzatvorenú zmluvu s prevádzkovateľom základnej služby, ktorý prevádzkuje kritickú základnú službu



Zdroj: https://thehackernews.com/2021/05/rapid7-source-code-breached-in-codecov.html, https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030

Register PZS



Oficiálna stránka verejnej správy SR — Slovensky

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD — Menu

Kybernetická bezpečnosť » Jednotný informačný systém kybernetickej bezpečnosti » Register prevádzkovateľov základnej služby (podľa § 34b ods. 1 a 3 zákona č. 69/2018 Z. z.)

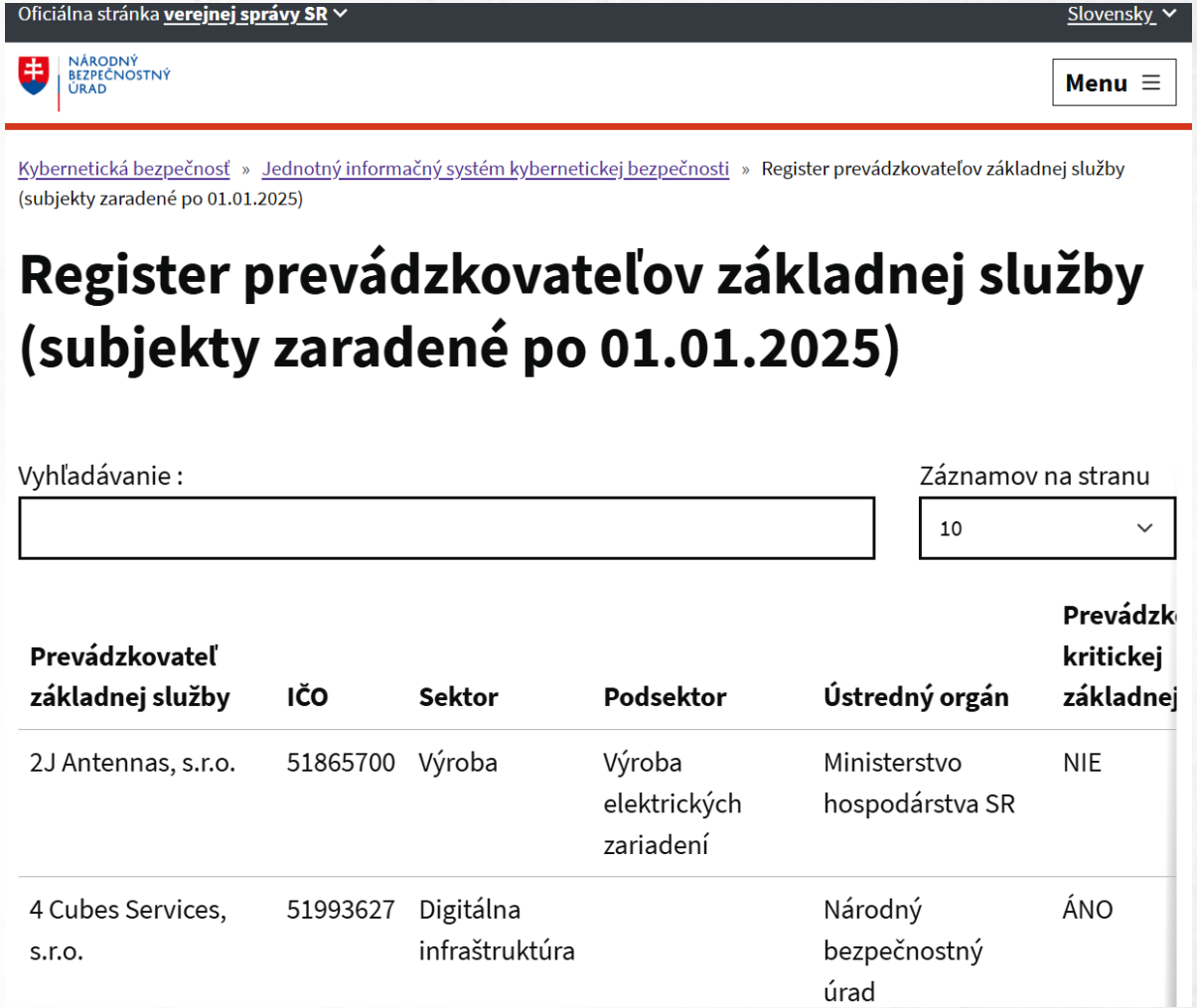
Register prevádzkovateľov základnej služby (podľa § 34b ods. 1 a 3 zákona č. 69/2018 Z. z.)

Vyhľadávanie :

Záznamov na stranu: 10

PZS	IČO	Sektor	Podsektor	Ústredný orgán	PKZ
365.bank, a.s.	31340890	Financie	Bankovníctvo	Ministerstvo financií SR	ÁNO
Agentúra na podporu výskumu a vývoja	30797764	Verejná správa		Ministerstvo investícií, regionálneho rozvoja a informatizácie SR	ÁNO

Zdroj: https://www.nbu.gov.sk/register-prevadzkovatelov-zakladnej-sluzby-podla-34b-ods-1-a-3-zakona-c-692018-z-z/



Oficiálna stránka verejnej správy SR — Slovensky

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD — Menu

Kybernetická bezpečnosť » Jednotný informačný systém kybernetickej bezpečnosti » Register prevádzkovateľov základnej služby (subjekty zaradené po 01.01.2025)

Register prevádzkovateľov základnej služby (subjekty zaradené po 01.01.2025)

Vyhľadávanie :

Záznamov na stranu: 10

Prevádzkovateľ základnej služby	IČO	Sektor	Podsektor	Ústredný orgán	Prevádzk kritickej základnej
2J Antennas, s.r.o.	51865700	Výroba	Výroba elektrických zariadení	Ministerstvo hospodárstva SR	NIE
4 Cubes Services, s.r.o.	51993627	Digitálna infraštruktúra		Národný bezpečnostný úrad	ÁNO

Zdroj: https://www.nbu.gov.sk/register-prevadzkovatelov-zakladnej-sluzby-subjekty-zaradene-po-01012025/

Prechodné ustanovenia k PZS/PKZS

- Prevádzkovateľ základnej služby podľa ZoKB v znení účinnom do 31. decembra 2024 sa **považuje za prevádzkovateľa kritickej základnej služby** podľa tohto zákona v znení účinnom od 1. januára 2025 (§34b ods. 1 ZoKB)

- NBÚ môže do 31. decembra 2026 aj z vlastnej iniciatívy rozhodnúť, ktorá z osôb nie je prevádzkovateľom kritickej základnej služby z dôvodu, že nespĺňa podmienky podľa § 18 ods. 1 v znení účinnom od 1. januára 2025.

Bezpečnostné opatrenia (I.)

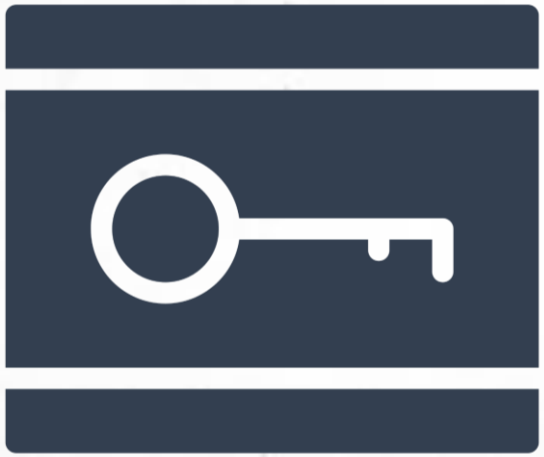
- Prevádzkovateľ základnej služby zaradený do registra prevádzkovateľov základnej služby je povinný do 2 rokov odo dňa účinnosti tohto zákona prijať bezpečnostné opatrenia

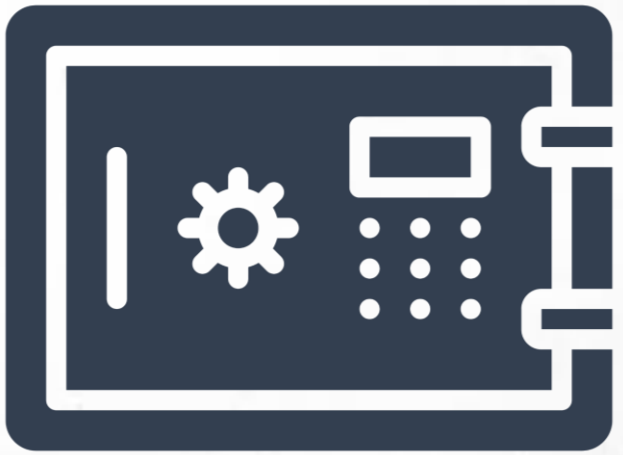
- **Bezpečnostné opatrenia**
  - sú úlohy, procesy, role a technológie v organizačnej, personálnej, fyzickej a technologickej oblasti, ktorých cieľom je dosiahnutie, zaručenie a udržanie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov a operačných technológií. Bezpečnostné 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 a prijímajú sa s cieľom (§ 20 ods. 1 ZoKB)

Bezpečnostné opatrenia (II.)

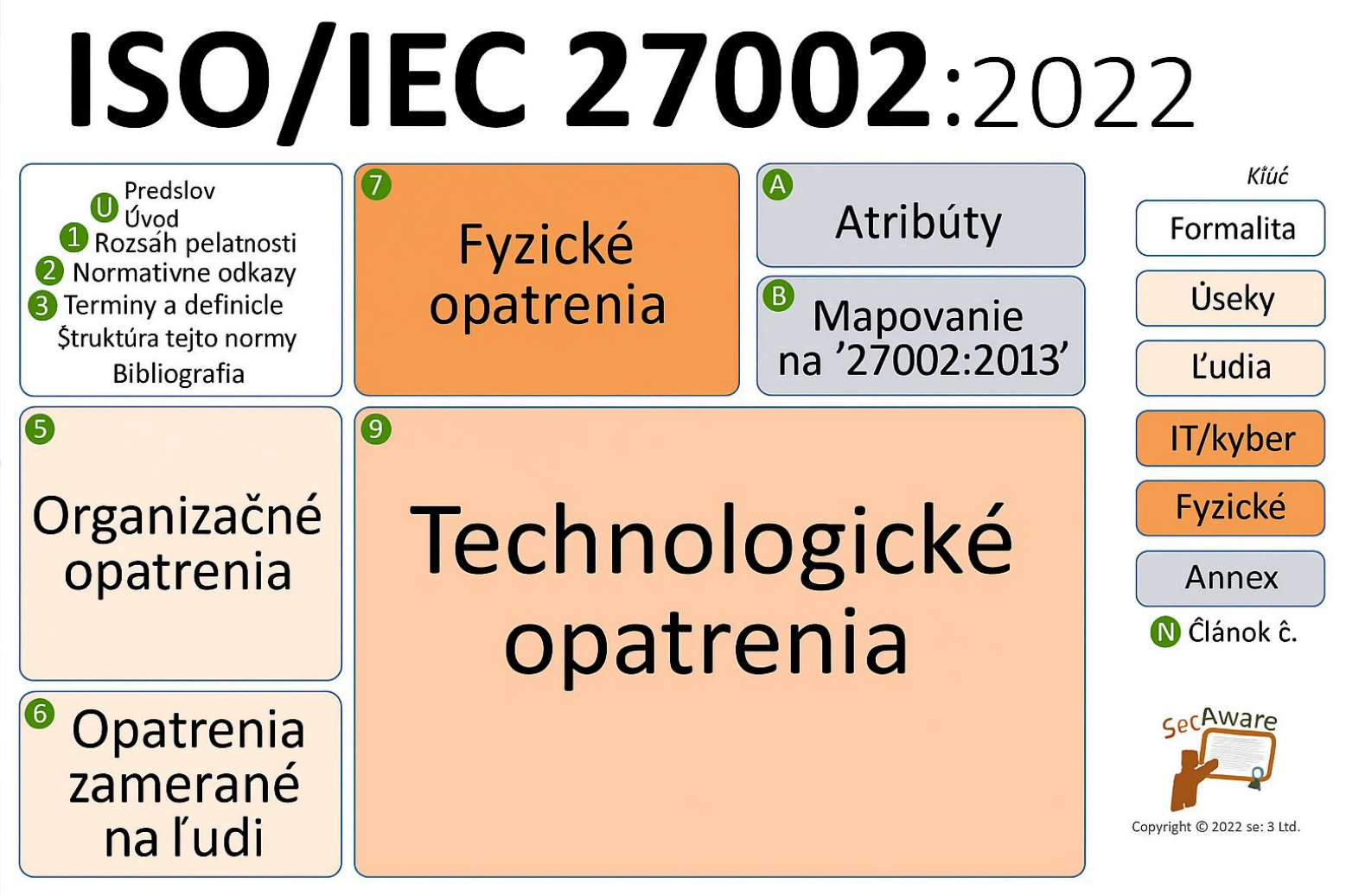
- akákoľvek činnosť, technické zariadenie, proces, mechanizmus, alebo čokoľvek, čo chráni informačný systém a jeho časti (aktíva) pred pôsobením konkrétnych hrozieb alebo hrozby.

- **Administratívne** – napr. politiky, odporúčania, štandardy
- **Fyzické** – napr. uzamykateľné dvere, náhradný zdroj napájania
- **Logické** – napr. heslá, firewally, prístupové zoznamy





Bezpečnostné opatrenia (III.)



Zdroj: https://www.iso27001security.com/html/27002.html

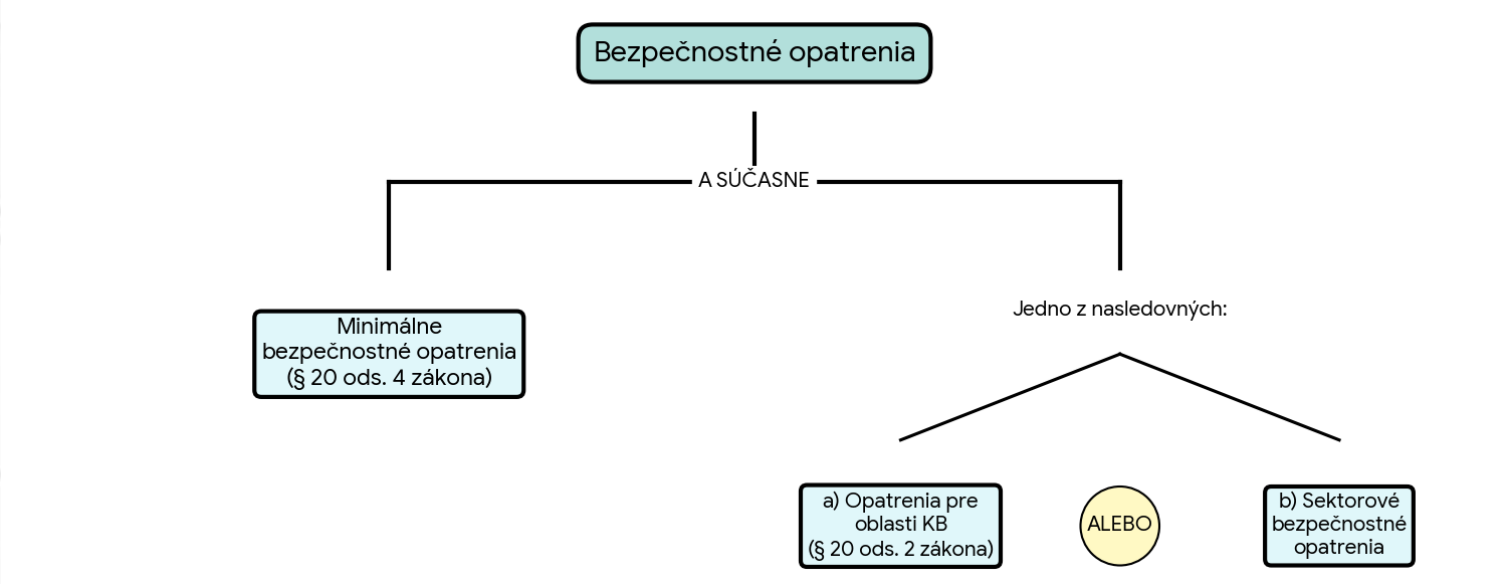
Bezpečnostné opatrenia (IV.)

- § 20 ods. 3 ZoKB
  - bezpečnostné opatrenia sa **prijímajú a realizujú v rozsahu a spôsobom** podľa § 32 ods. 1 písm. b) alebo osobitného predpisu, ak je vydaný, a na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu.
  - § 32 ods. 1 písm. b) -> **Vyhláška NBÚ č. 227/2025 Z. z. o bezpečnostných opatreniach**

- § 20 ods. 5 ZoKB
  - bezpečnostné opatrenia sa prijímajú a realizujú na **základe analýzy rizík** kybernetickej bezpečnosti, ktorá určuje pravdepodobnosť vzniku škodlivej udalosti.
  - súčasťou analýzy rizík je aj **analýza politického rizika tretej strany**

Bezpečnostné opatrenia (V.)

- vyhláška NBÚ č. 227/2025 Z. z. o bezpečnostných opatreniach (§ 3 ods. 1):
  - bezpečnostné opatrenia = minimálne bezpečnostné opatrenia (§ 20 ods. 4 ZoKB) AND (všeobecné bezpečnostné opatrenia (§ 20 ods. 2 ZoKB + vyhláška 227/2025) OR sektorové bezpečnostné opatrenia)
  - sektorové opatrenia – verejná správa



Zdroj: Obrázok vygenerovaný AI - Gemini

Minimálne bezpečnostné opatrenia (I.)

- **Minimálne bezpečnostné opatrenia**
  - § 20 ods. 4 ZoKB - bezpečnostné opatrenia musia zahŕňať najmenej

- a) určenie **manažéra kybernetickej bezpečnosti**, ktorý je pri návrhu, prijímaní a presadzovaní bezpečnostných opatrení nezávislý od štruktúry riadenia prevádzky a vývoja služieb informačných technológií a ktorý spĺňa znalostné štandardy pre výkon roly manažéra kybernetickej bezpečnosti,
- b) **detekciu** kybernetických bezpečnostných incidentov,
- c) **evidenciu** kybernetických bezpečnostných incidentov,
- d) **postupy riešenia** a riešenie kybernetických bezpečnostných incidentov,
- e) **určenie kontaktnej osoby** pre prijímanie a evidenciu hlásení,

Minimálne bezpečnostné opatrenia (II.)

- f) **pripojenie do komunikačného systému pre hlásenie a riešenie** kybernetických bezpečnostných incidentov a centrálneho systému včasného varovania,
- g) **určenie a pridelenie úloh, rolí a zodpovednosti** podľa podmienok prevádzkovateľa základnej služby a zabezpečenie primeraného vzdelávania a preškoľovania pre všetky zavedené roly,
- h) určenie konkrétnej osoby alebo konkrétnych osôb zodpovedných za **schvaľovanie bezpečnostných opatrení, dohľad, kontrolu** a audit, zabezpečenie primeranosti zdrojov na riadenie kybernetickej bezpečnosti a za vzdelávanie,
- i) **vzdelávanie a budovanie bezpečnostného povedomia** v oblasti kybernetickej bezpečnosti.

Manažér kybernetickej bezpečnosti

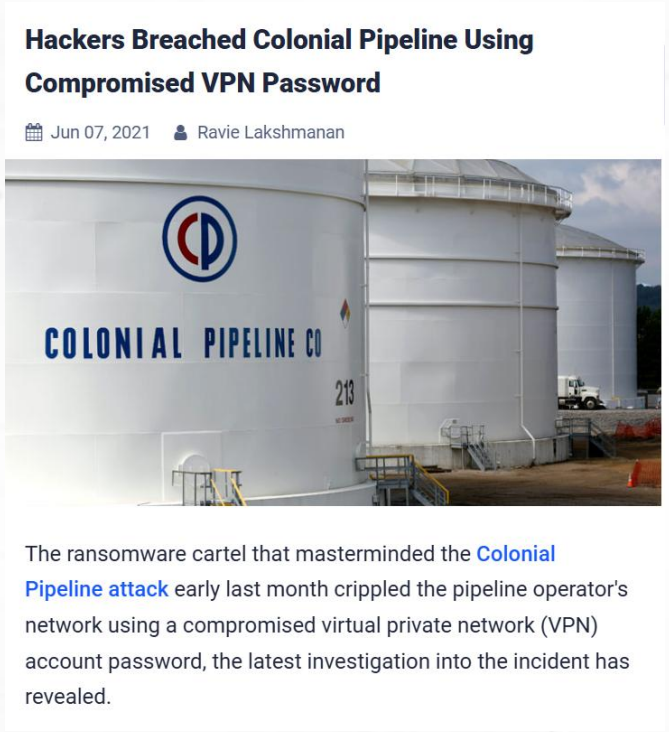
- **manažér kybernetickej bezpečnosti**
- je pri návrhu, prijímaní a presadzovaní bezpečnostných opatrení
- nezávislý od štruktúry riadenia prevádzky a vývoja služieb informačných technológií
- spĺňa **znalostné štandardy** pre výkon roly manažéra kybernetickej bezpečnosti
  - Vyhláška NBÚ č. 492/2022 Z. z. ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti – príloha č. 5

Stupeň vzdelania:	Úplné stredné všeobecné alebo úplné stredné odborné	Vysokoškolské I. stupňa	Vysokoškolské II. a III. stupňa
Odborná prax:	• najmenej **7 rokov** praxe v oblasti informačných technológií • z toho najmenej **5 rokov** praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT • medzinárodný certifikát sa považuje za započítateľnú odbornú prax 1 rok	• najmenej **5 rokov** praxe v oblasti informačných technológií • z toho najmenej **3 roky** praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT • medzinárodný certifikát sa považuje za započítateľnú odbornú prax 1 rok	• najmenej **3 roky** praxe v oblasti informačných technológií • z toho najmenej **1 rok** praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT • medzinárodný certifikát sa považuje za započítateľnú odbornú prax 1 rok
Špecifické kľúčové kompetencie	a) schopnosť prijímať rozhodnutia b) schopnosť myslieť a konať v súvislostiach c) schopnosť riešiť konflikty d) schopnosť poskytovať spätnú väzbu e) schopnosť delegovať úlohy f) schopnosť podporovať procesy vzdelávania a odovzdávania znalostí g) schopnosť viesť pracovný tím h) schopnosť organizovania a plánovania práce i) analytické myslenie j) strategické a koncepčné myslenie k) tvorivosť (kreativita) l) prezentačná zručnosť		

Požiadavky označené * sú odvetvovo závislé. Pre príslušnú rolu sú posudzované v kontexte kompetencií, potrebných na vykonávanie určitej pracovnej činnosti v konkrétnom odvetví.

Mýtus – KB je zodpovednosť len IT a MKB (I.)

- manažér kybernetickej bezpečnosti a zamestnanci IT nedokážu zabezpečiť všetko sami
- právna úprava vyžaduje integráciu kybernetickej bezpečnosti do riadenia organizácie
- zodpovednosť – štatutárny orgán



Hackers Breached Colonial Pipeline Using Compromised VPN Password

Jun 07, 2021 Ravie Lakshmanan

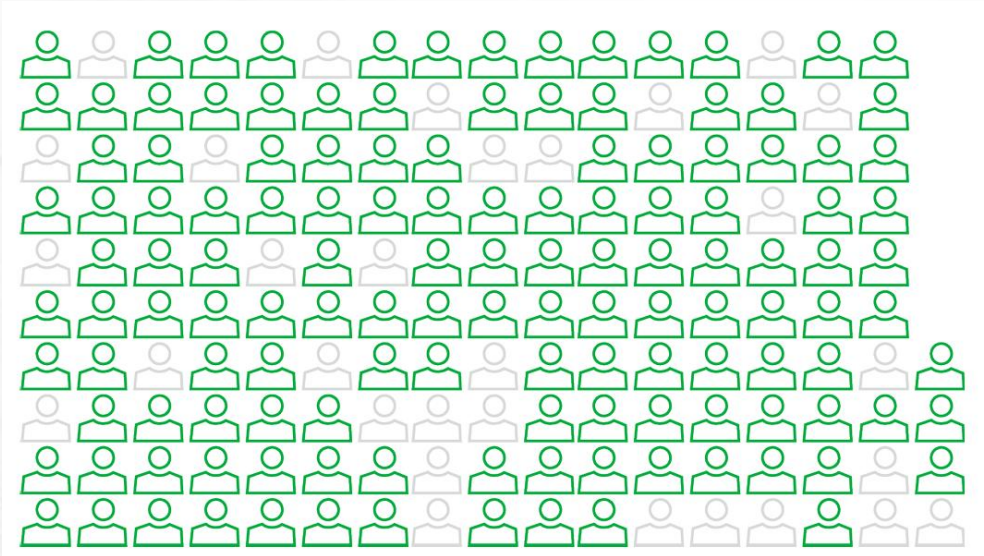
The ransomware cartel that masterminded the Colonial Pipeline attack early last month crippled the pipeline operator's network using a compromised virtual private network (VPN) account password, the latest investigation into the incident has revealed.

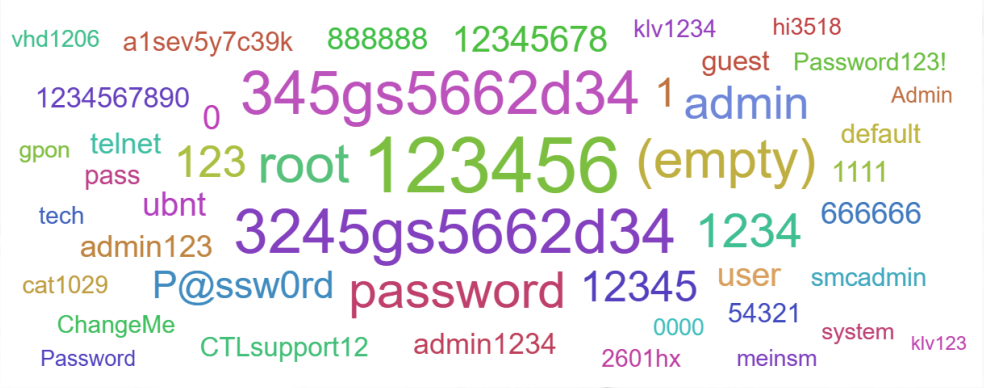
Zdroj: https://thehackernews.com/2021/06/hackers-breached-colonial-pipeline.html

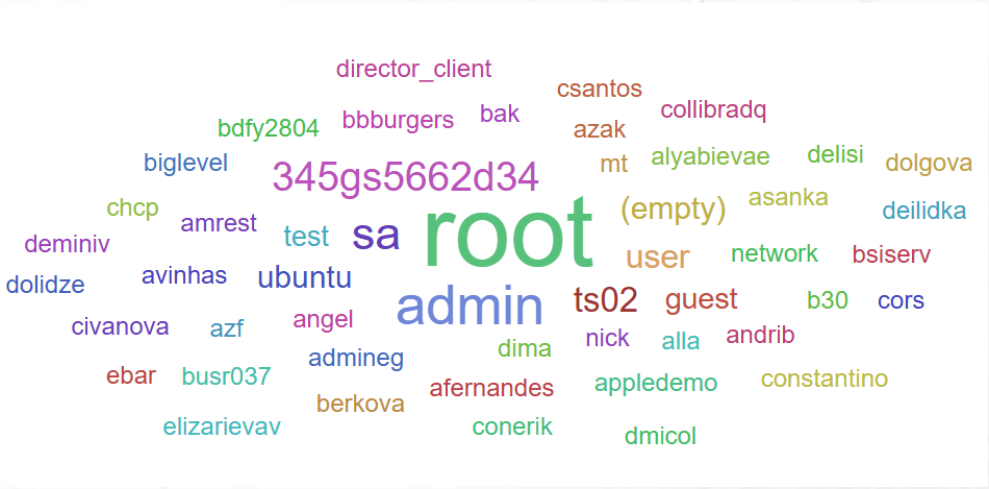
Mýtus – KB je zodpovednosť len IT a MKB (II.)

- každý zamestnanec nesie svoju mieru zodpovednosti.
- prevencia cez pravidelné školenia a budovanie bezpečnostnej kultúry.

82 %







Zdroj: Verizon: DBIR Data Breach Investigations Report, 2022.

Všeobecné bezpečnostné opatrenia (I.)

- **Všeobecné bezpečnostné opatrenia:**
  - § 20 ods. 2 ZoKB - Bezpečnostné opatrenia sa prijímajú aspoň pre (**oblasti bezpečnostných opatrení**):

- 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,

Všeobecné bezpečnostné opatrenia (II.)

- 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.

Všeobecné bezpečnostné opatrenia (III.)

- **Vyhláška NBÚ č. 227/2025 Z. z. o bezpečnostných opatreniach**

ROZSAH BEZPEČNOSTNÝCH OPATRENÍ PRE OBLASTI KYBERNETICKEJ BEZPEČNOSTI PODĽA § 20 ODS. 2 ZÁKONA

Položka	Bezpečnostné opatrenia pre organizáciu a riadenie informačnej bezpečnosti a kybernetickej bezpečnosti podľa § 20 ods. 2 písm. a) zákona prijíma prevádzkovateľ základnej služby tak, že:	Relevancia pre IKT*		Relevancia pre OT*	
		PZS*	PKZS*	PZS*	PKZS*
1.	manažér kybernetickej bezpečnosti predkladá návrhy bezpečnostných opatrení a oznamuje informácie v oblasti kybernetickej bezpečnosti priamo štatutárnemu orgánu prevádzkovateľa základnej služby	ÁNO	ÁNO	ÁNO	ÁNO
2.	je určená osoba zodpovedná za riadenie prístupu používateľov do siete a k informačnému systému a za prideľovanie a odoberanie prístupových práv používateľom, ich evidenciu a vedenie prevádzkových záznamov o každom prístupe do siete a informačného systému podľa príslušnej bezpečnostnej politiky	ÁNO	ÁNO	ÁNO	ÁNO
3.	je definovaná a schválená štruktúra pre zavedenie, prevádzku a riadenie kybernetickej bezpečnosti vrátane pridelenia úloh, rolí ako aj určenie zodpovedností podľa právomocí na schvaľovanie bezpečnostných opatrení, dohľad, kontrolu, audit a vzdelávanie	ÁNO	ÁNO	ÁNO	ÁNO
4.	je zabezpečená primeranosť zdrojov na riadenie kybernetickej bezpečnosti a vzdelávanie v oblasti kybernetickej bezpečnosti	ÁNO	ÁNO	ÁNO	ÁNO
5.	je definovaný a zavedený systém vzdelávania a preškoľovania pre všetky roly týkajúce sa kybernetickej bezpečnosti	ÁNO	ÁNO	ÁNO	ÁNO
6.	je uplatnená zásada najnižších privilégií, podľa ktorej sú každému používateľovi obmedzené privilégiá v najväčšom rozsahu potrebnom na splnenie pridelených úloh	ÁNO	ÁNO	ÁNO	ÁNO
7.	je uplatnená zásada oddeľovania zodpovedností, podľa ktorej žiaden používateľ nemá oprávnenie upravovať alebo používať aktíva prevádzkovateľa základnej služby bez autorizácie alebo overenia identity	ÁNO	ÁNO	ÁNO	ÁNO
8.	je uplatnená zásada vymedzenia právomoci, povinnosti a zodpovednosti, ktoré sú súčasťou pracovnej náplne alebo obdobného opisu pracovných činností	ÁNO	ÁNO	ÁNO	ÁNO
9.	je uplatnená zásada sprístupňovania informácií podľa zásady aktuálnej potreby poznať, podľa ktorej prístup k informáciám a ich vlastníctvo je obmedzené len na tie osoby, ktoré	ÁNO	ÁNO	ÁNO	ÁNO

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

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť

pavol.sokol@upjs.sk

https://cyberawareness.sk