UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

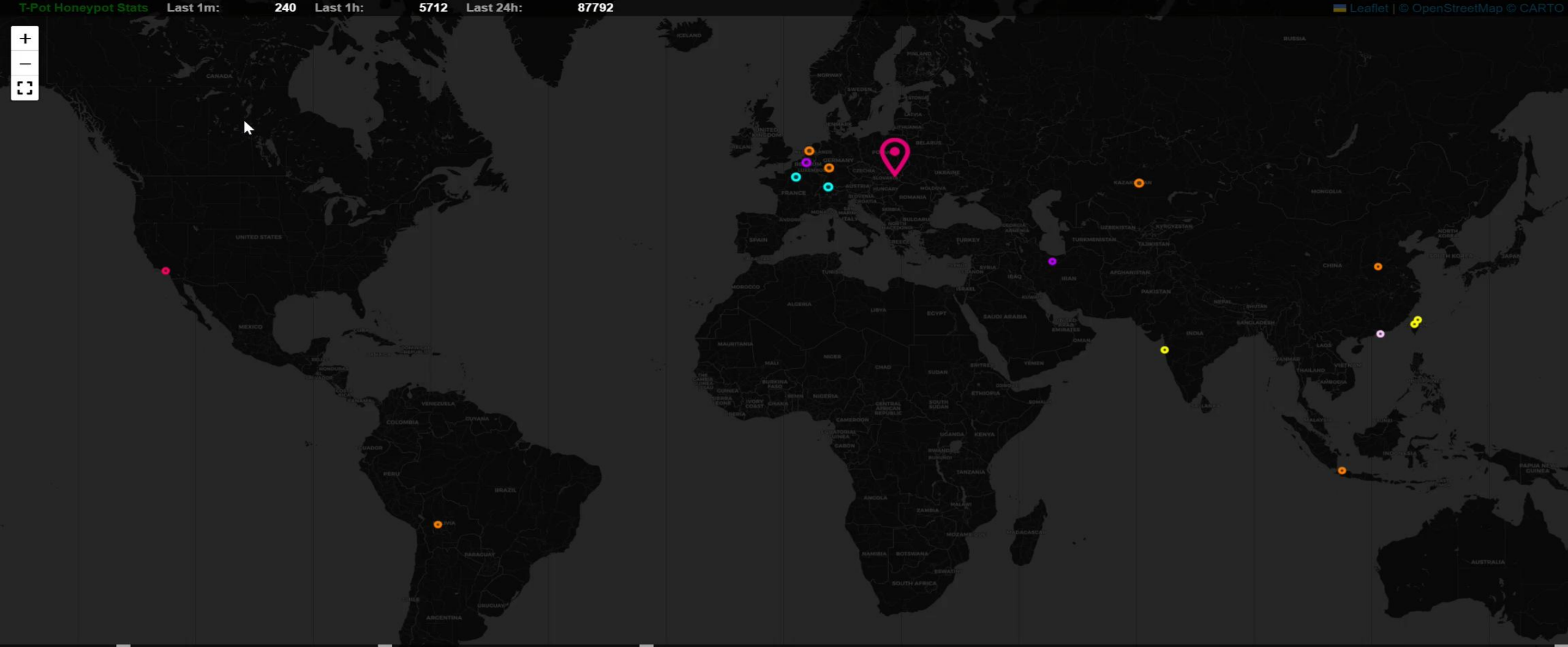
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Právna úprava kybernetickej bezpečnosti

Úvod do práva informačných a komunikačných technológií

Pavol Sokol

18.10.2025



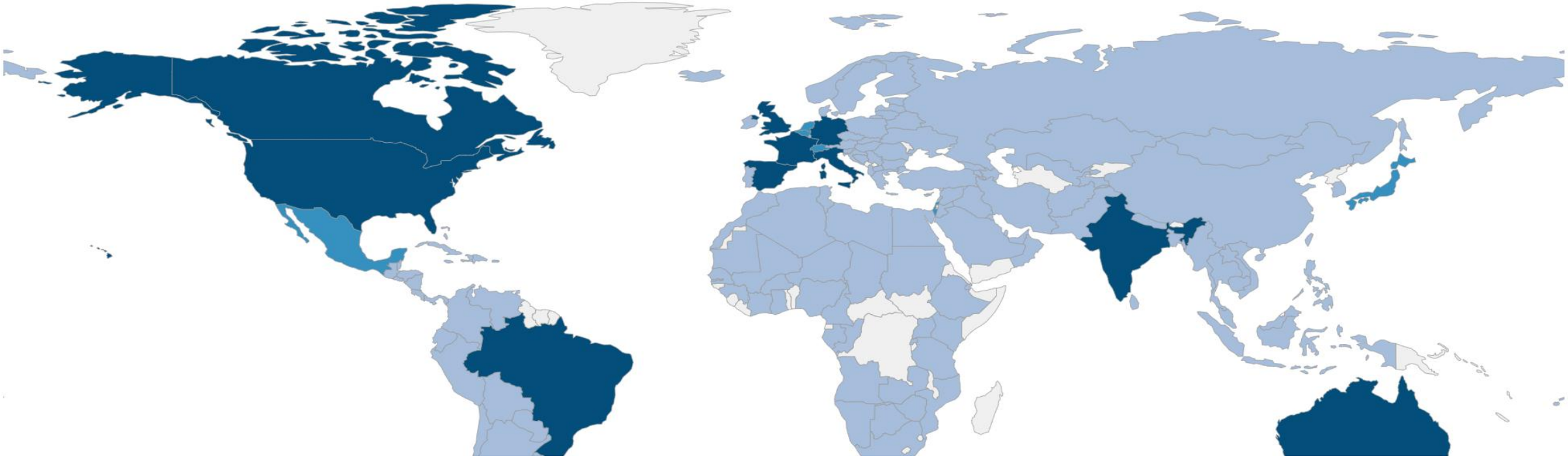
Color	Service
	FTP
	SSH
	TELNET
	EMAIL
	SQL
	DNS
	HTTP
	HTTPS

Hits	IP
4689	193.41.206.98
3672	193.37.69.157
3612	193.41.206.138
1993	193.37.69.205
236	170.64.199.171
235	209.38.30.136
108	54.89.203.179

Hits	Country
8380	France
5710	The Netherlands
565	United States
471	Australia
358	Taiwan
233	China
142	South Korea

Events	IP	Country	Honeypot	Service
2025-03-17 05:56:48	193.41.206.138	France	Tanner	HTTP
2025-03-17 05:56:48	193.41.206.138	France	Tanner	HTTP
2025-03-17 05:56:48	193.41.206.138	France	Tanner	HTTP
2025-03-17 05:56:47	193.41.206.138	France	Tanner	HTTP
2025-03-17 05:56:47	193.41.206.138	France	Tanner	HTTP
2025-03-17 05:56:48	193.41.206.138	France	Tanner	HTTP
2025-03-17 05:56:47	193.41.206.138	France	Tanner	HTTP

Svet okolo nás (I.)



Groups	Victims	This year	This month
268	20 315	3 829	291

Zdroj: https://www.ransomware.live/

Svet okolo nás (II.)

2024

22.3.2024 15:46 | Bezpečnosť

Hackeri udreli na Slovenskú národnú knižnicu. Nejdú prístupy k zdrojom ani kontakty

Zdroj: reprofoto Snk.sk, iStock a úprava redakcia

Rumunské nemocnice napadnuté ransomvérom

Vypublikované 13. 02. 2024

ransomware-nemocnice-860x360

Najmenej 25 rumunských nemocníc bolo odrezaných od online služieb po tom, čo útok ransomvéru znefunkčnil ich systém na správu zdravotnej starostlivosti. Cieľom útoku bol HIS, ktorý sa používa v nemocniciach na správu lekárskej činnosti a údajov o pacientoch. Útok, ktorý sa odohral počas noci z 11. na 12. februára 2024, zasiahol produkčné servery HIS a v dôsledku toho s**ystém prestal fungovať**, súbory a databázy boli zašifrované. **Rumunské ministerstvo zdravotníctva** uviedlo, že incident je predmetom vyšetrovania IT špecialistami, vrátane odborníkov na kybernetickú bezpečnosť z Národného riaditeľstva pre kybernetickú bezpečnosť (DNSC), a posudzujú sa možnosti obnovy. Zoznam zasiahnutých nemocníc bol aktualizovaný po zverejnení aktualizácie DNSC a zahŕňa nemocnice v rôznych regiónoch Rumunska vrátane centier pre regionálnu a onkologickú liečbu.

Zdroj: https://www.nbu.gov.sk/rumunske-nemocnice-napadnute-ransomverom/, https://zive.aktuality.sk/clanok/1CGRx85/hackeri-udreli-na-slovensku-narodnu-kniznicu-nejdu-pristupy-k-zdrojom-ani-kontakty/

Svet okolo nás (III.)

2025

TREND Predplatiť

Hekeri po útoku na kataster žiadajú vysoké výkupné, štát nemusí disponovať zálohami dát

Daniel Ivančák
online editor

9.1. 7:35 | **Ak sa hekerský útok v takomto rozsahu potvrdí, na Slovensku môže nastať chaos**

živé Predplatné

TOP Kataster po mesiaci: Štát prelomil mlčanie. Čo radí a sľubuje ľuďom

Zdroj: iStock, reprofoto Zbgis.skgeodesy.sk, úprava redakcia

Lukáš Kosno

Filip Hanker

Zhrnuli sme novinky okolo katastra presne mesiac po útoku. Máme oficiálne vyjadrenia úradu.

Zdroj: https://www.trend.sk/spravy/hekeri-utoku-kataster-ziadaju-vysoke-vykupne-stat-nemusi-disponovat-zalohami-dat
https://zive.aktuality.sk/clanok/MkBBFdI/kataster-po-mesiaci-stat-prelomil-mlcanie-co-radi-a-slubuje-ludom/


100% bezpečnosť neexistuje

Kybernetická hrozba (I.)

- **kybernetická hrozba**
  - § 3 ods. 1 písm. j) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti – odkazuje sa na Nariadenie 2019/881 (akt o kybernetickej bezpečnosti)

  - je **každá potenciálna okolnosť**, **udalosť alebo činnosť**, ktorá by mohla poškodiť, narušiť alebo inak **negatívne ovplyvniť** siete a informačné systémy, užívateľov takýchto systémov a iné osoby;

Bezpečnostné hrozby (II.)

Zdroj: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-list-of-top-15-threats

Bezpečnostné hrozby (III.)

Zdroj: ENISA Landscape 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Bezpečnostné hrozby (IV.)

Zdroj: https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030

Kybernetická bezpečnosť (I.)

- **kybernetická bezpečnosť**
  - § 3 ods. 1 písm. h) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti:
    - stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje **dostupnosť, pravosť, integritu alebo dôvernosť** uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov,

  - Článok 2 ods. 1 Nariadenia 2019/881 (akt o kybernetickej bezpečnosti)
    - **sú činnosti** potrebné na ochranu sietí a informačných systémov, užívateľov takýchto systémov a iných osôb dotknutých kybernetickými hrozbami

Kybernetická bezpečnosť (II.)

Všetky vaše medicínske záznamy sme omylom zaslali úplne cudziemu človeku

Odkazuje, že ani on bohužiaľ nevie čo s vami vlastne je...

Kybernetická bezpečnosť (III.)

Vaše medicínske záznamy nám bohužiaľ stále nezaslali naspäť

Nepamätáte si náhodou Vašu celú medicínsku históriu?

Zdroj: https://www.newyorker.com/magazine/2018/11/12/why-doctors-hate-their-computers

Kybernetická bezpečnosť (IV.)

Vážený pane, vaše medicínske záznamy nám konečne zaslali späť a konečne poznáme príčinu vašich problémov

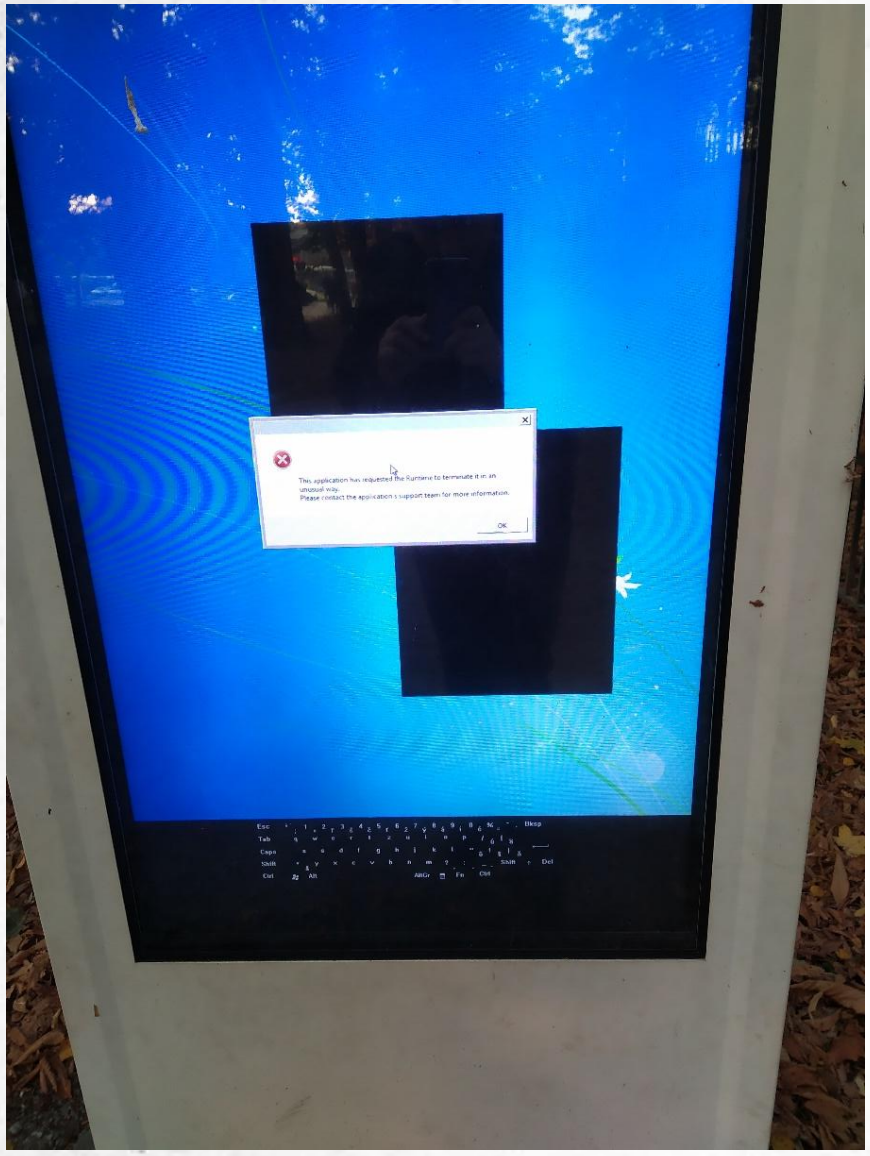
Ste tehotný!

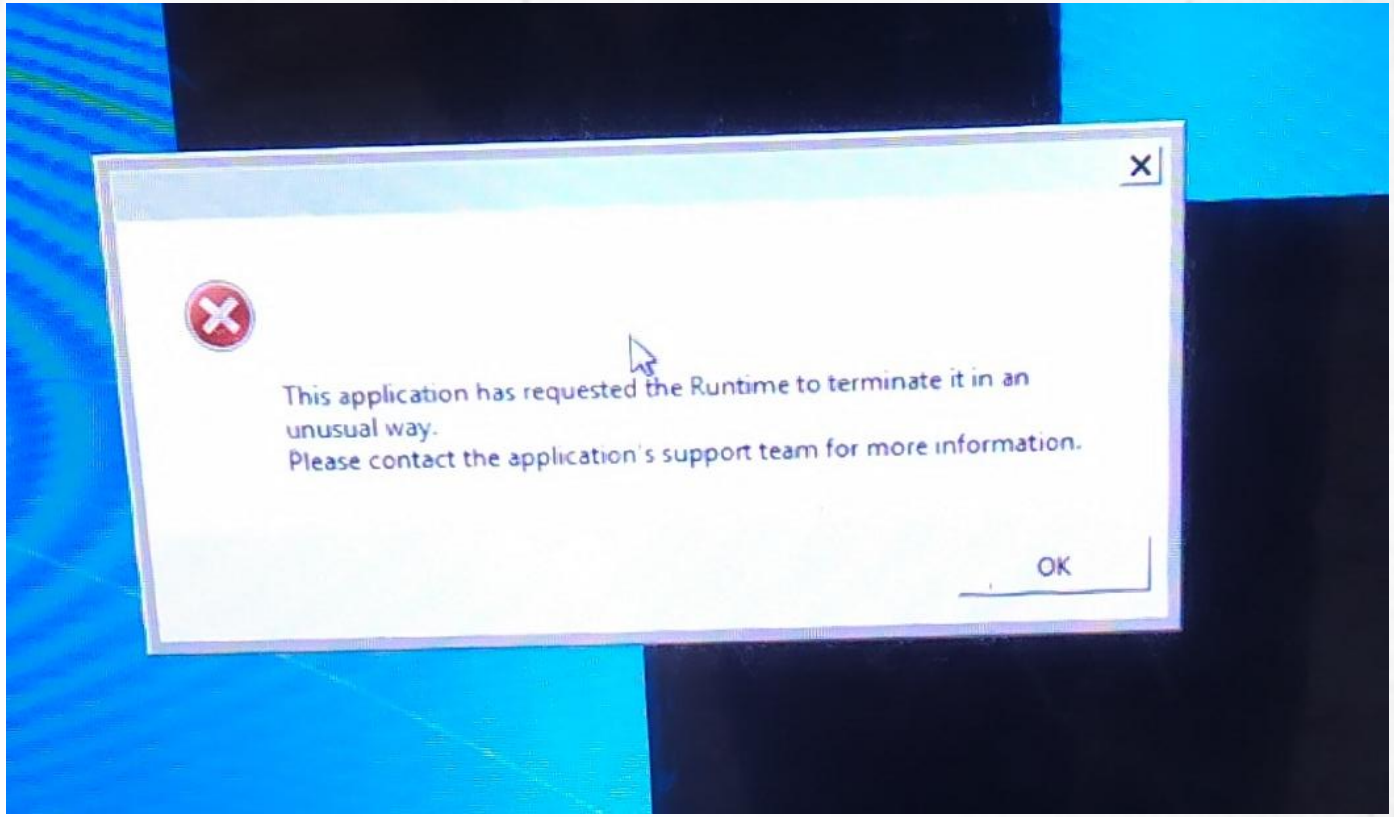
Zdroj: https://dribbble.com/shots/6278477-Composition-with-little-doctors


Search Google Maps
Stanične námestie
Košice, Košice Region
Google Street View
Apr 2024
See more dates
Košice
Stredná
škola že
Google
Image capture: Apr 2024
© 2024 Google
Slovakia
Terms
Privacy
Report a problem

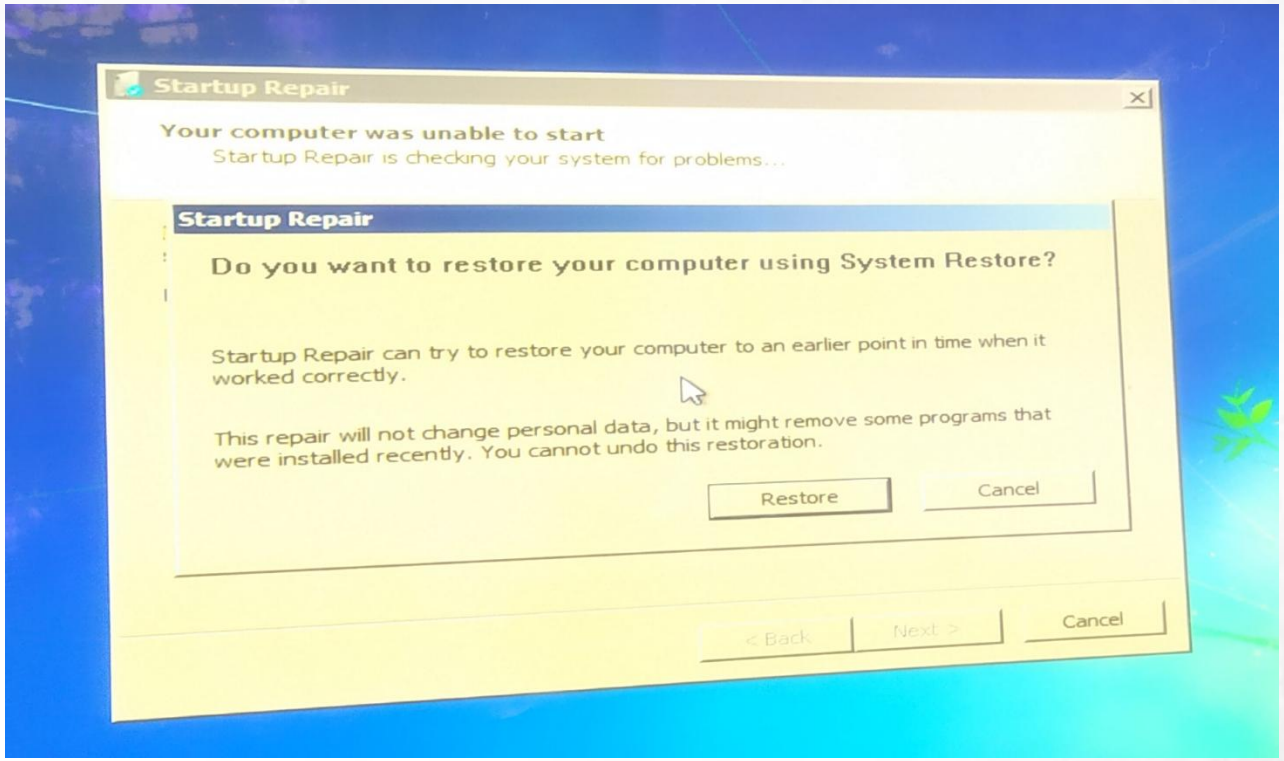
Kybernetická bezpečnosť (VI.)

Kybernetická bezpečnosť (VII.)



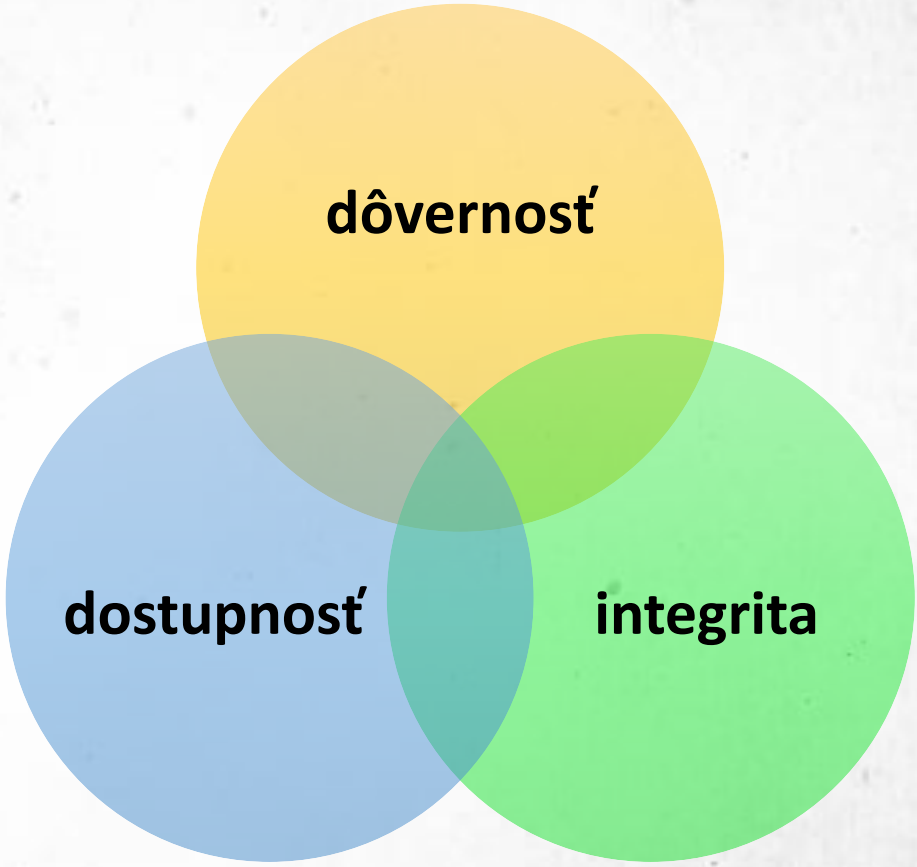


Kybernetická bezpečnosť (VIII.)



Kybernetická bezpečnosť (IX.)

- **dôvernosť**
  - záruka, že údaj alebo informácia nie je prezradená neoprávneným subjektom alebo procesom (§3 ods. 1 písm. e) ZoKB)
- **integrita**
  - záruka, že bezchybnosť, úplnosť alebo správnosť údaja neboli narušené (§3 ods. 1 písm. g) ZoKB)
- **Dostupnosť**
  - záruka, že údaj alebo poskytovaná služba sú pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď sú potrebné a požadované (§3 ods. 1 písm. f) ZoKB)



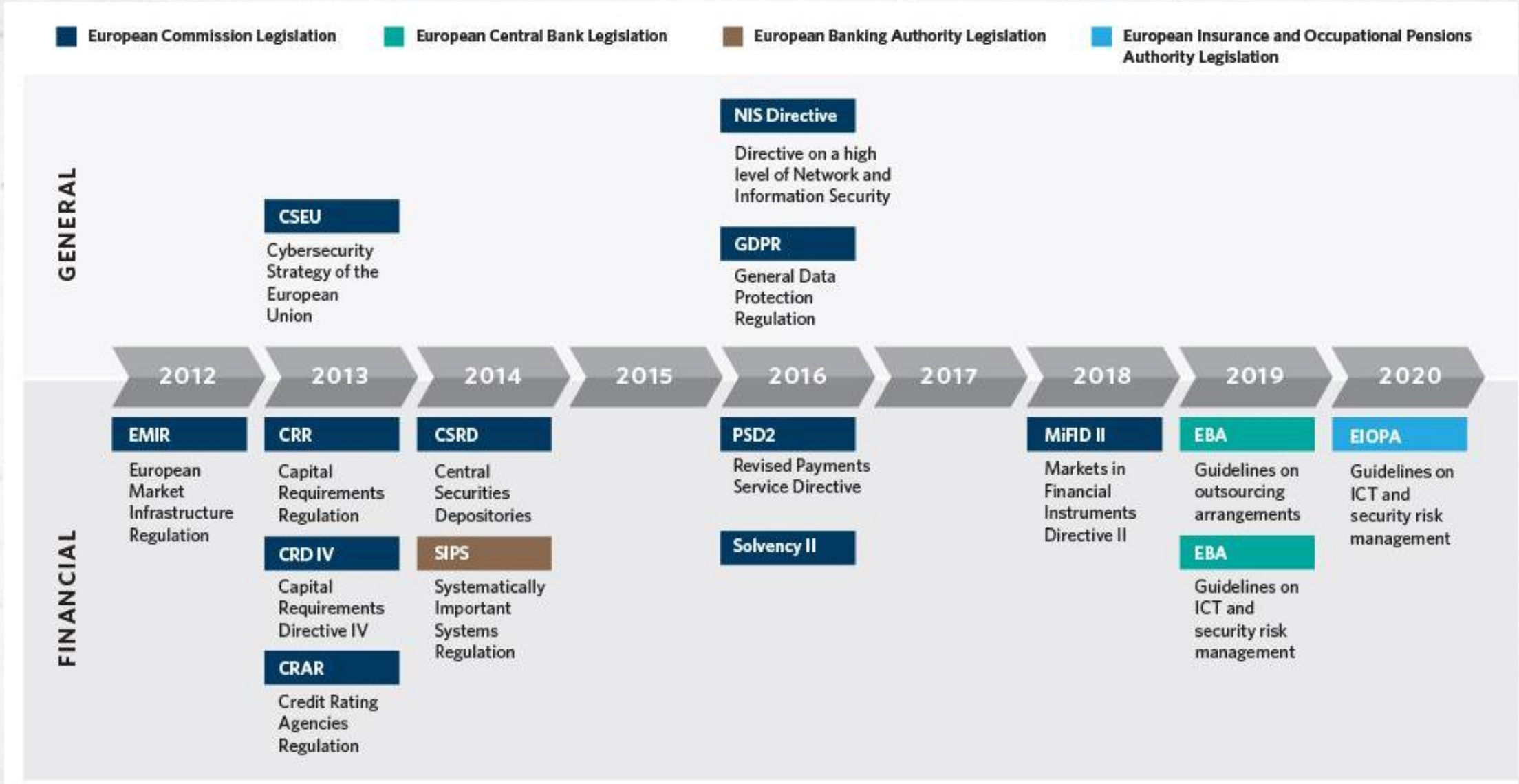
ODOLNOSŤ VOČI KYBERNETICKÝM HROZBÁM

„Skutočná odolnosť nespočíva v tom, že zabránime každému útoku, ale v tom, ako rýchlo a efektívne sa dokážeme zotaviť.“

Kybernetická Hrozba

Základné pojmy

Právna úprava KB (I.)



Európska právna úprava (I.)

- Zmluva o EÚ a Zmluva o fungovaní EÚ
- Charta základných práv EÚ

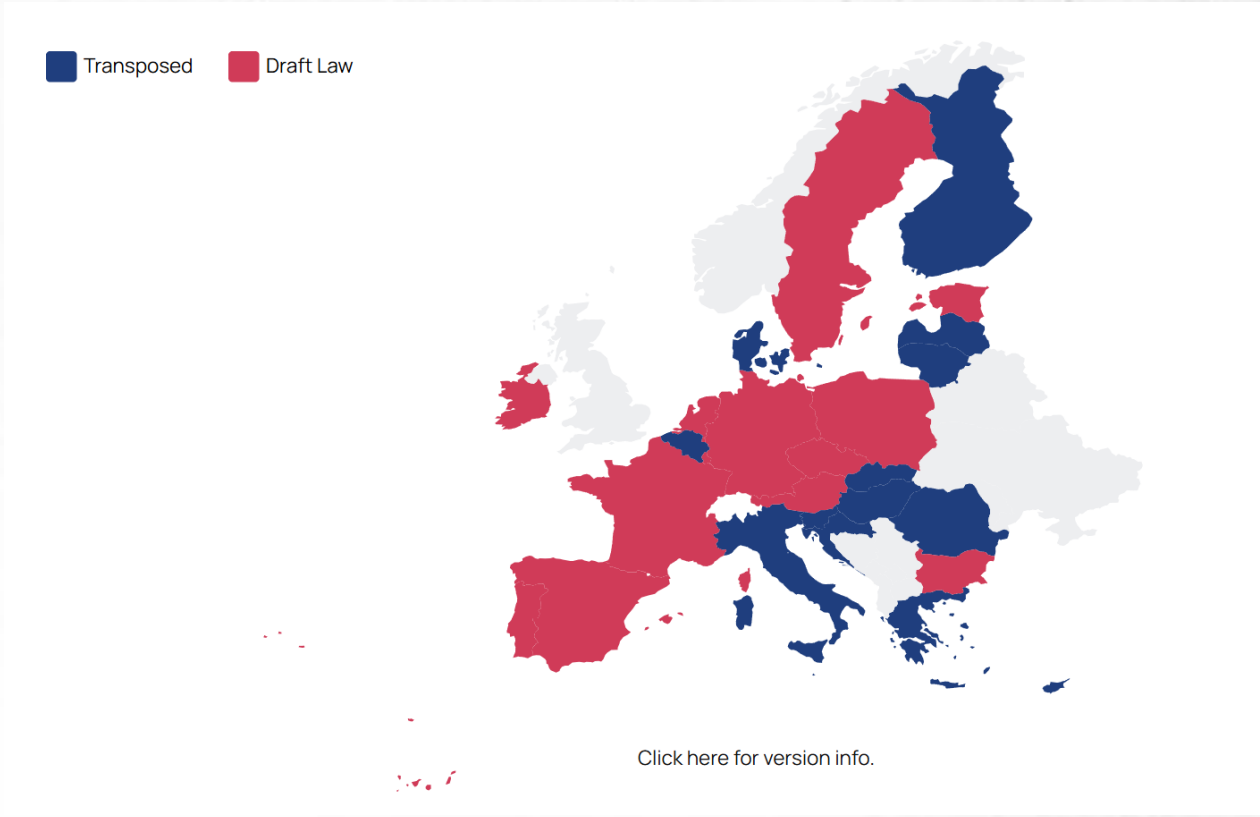
- NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (**všeobecné nariadenie o ochrane údajov - GDPR**)

- SMERNICA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2022/2555 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (**smernica NIS 2**)

Európska právna úprava (II.)

- smernica sa musí transponovať do právneho poriadku (nariadenie platí priamo)
- členské štáty mali transponovať smernicu do 17. októbra 2024 (SR – od 1.1.2025)
- implementácia do právnej úpravy v členských štátoch - organizácie sa musia prispôsobiť až po prijatí v danej krajine

- spolupráca pri zvládaní incidentov
- koordinované zverejňovanie zraniteľností
- riadenie kybernetických rizík



Zdroj: https://ecs-org.eu/activities/nis2-directive-transposition-tracker/

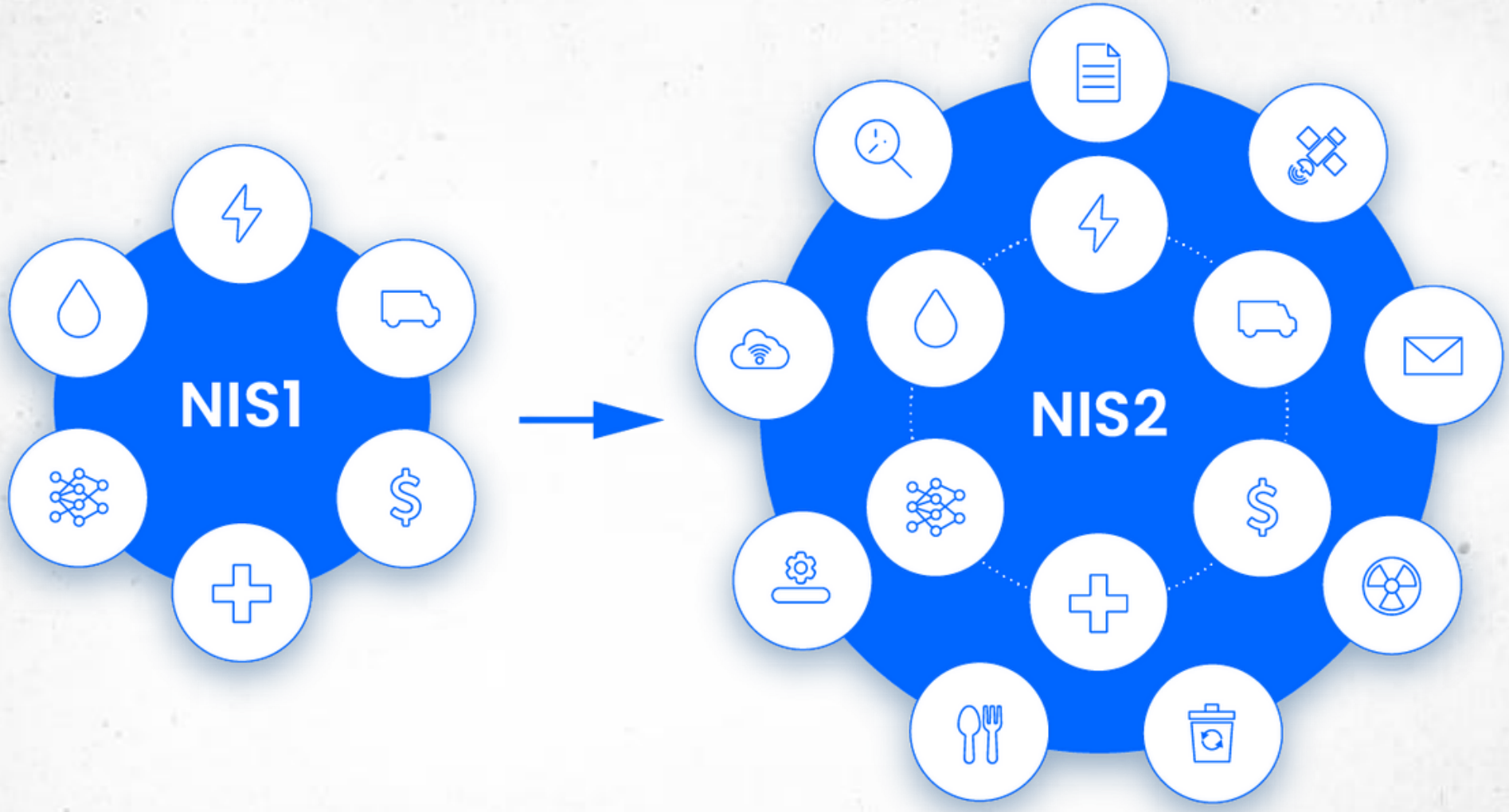
Európska právna úprava (III.)

Ciele:

- členské štáty boli primerane vybavené. Napríklad s tímom reakcie na incidenty počítačovej bezpečnosti (CSIRT)
- spoluprácu medzi všetkými členskými štátmi
- kultúra bezpečnosti v sektoroch, ktoré sú životne dôležité pre naše hospodárstvo a spoločnosť

- sprísniť uložené bezpečnostné požiadavky,
- riešiť bezpečnosť dodávateľského reťazca,
- zefektívniť ohlasovanie incidentov,
- posilniť opatrenia v oblasti dohľadu,
- zaviesť požiadavky na vymáhanie práva s harmonizovanými sankciami vo všetkých členských štátoch EÚ.

Európska právna úprava (IV.)



Zdroj: https://nis2directive.eu/

28.11.2024 12:05 | Bezpečnosť

Úroveň kybernetickej bezpeč sa zvýši

Zdroj: istock

TASR

Novela bude účinná od 1. januára 2

Zvýšenie úrovne kybernetickej bezpečnosti

rizík, ktoré sú spôsobené rýchlym technologickým vývojom a

platná od 16. januára 2023.

Ako ovplyvní smernica NIS2 možnosť používať druhotný softvér?

redakcia touchIT 25. februára 2025

Tento článok je tlačová správa a je publikovaný bez redakčných úprav.

V decembri 2022 schválila Európska únia smernicu NIS2 (Network and Information System Directive 2), ktorá stanovuje pravidlá a požiadavky na kybernetickú bezpečnosť ICT systémov a sietí. Členské štáty EÚ mali implementovať NIS2 do svojich právnych poriadkov do 18. októbra 2024. Na Slovensku smernica nadobudla účinnosť 1. januára 2025. Ovplyvnia nové prísnejšie pravidlá [illegible]žnosť používania druhotného softvéru?

nyc digitalizáciou. To sú hlavné ciele novely zákona o kybernetickej

rodnej úrovni a

ologickým vývoj

Zdroj: https://zive.aktuality.sk/clanok/zpNPdfB/uroven-kybernetickej-bezpecnosti-na-slovensku-sa-zvysi/, https://touchit.sk/ako-ovplyvni-smernica-nis2-moznost-pouzivat-druhotny-softver/698207, https://touchit.sk/je-vasa-firma-pripravena-na-nis2/620047, https://zive.aktuality.sk/clanok/JExEku3/prezident-podpisal-novelu-zakona-o-kybernetickej-bezpecnosti-co-sa-meni/

Slovenská právna úprava (I.)

- Zákon č. 69/2018 Z. z. o **kybernetickej bezpečnosti** a o zmene a doplnení niektorých zákonov
  - Prevádzkovatelia základných služieb a prevádzkovatelia kritických základných služieb

- Zákon č. 95/2019 Z. z. o **informačných technológiách vo verejnej správe** a o zmene a doplnení niektorých zákonov (ZoITVS)
  - verejná správa – ministerstvá, mestá, obce, školy ...

- Zákon č. 18/2018 Z. z. o **ochrane osobných údajov** a o zmene a doplnení niektorých zákonov
  - Prevádzkovateľ, ktorý spracúva osobné údaje

- zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (**zákon o e-Governmente**)
- zákon č. 452/2021 Z. Z. **o elektronických komunikáciách**
- zákon č. 215/2004 Z. z. o **ochrane utajovaných skutočností**

Slovenská právna úprava (II.)

- novela zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti

- rozšírenie povinných subjektov
- zrušenie dopadových a špecifických kritérií
- bezpečnosť dodávateľského reťazca

- neboli novelizované vykonávacie právne predpisy, resp. osobitná právna úprava

13.12.2024 18:40 | Bezpečnosť

Prezident podpísal novelu zákona o kybernetickej bezpečnosti, čo sa mení

Zdroj: istock

živě

TASR

Novela bude účinná od 1. januára 2025.

Zdroj: https://zive.aktuality.sk/clanok/JExEku3/prezident-podpisal-novelu-zakona-o-kybernetickej-bezpecnosti-co-sa-meni/

Slovenská právna úprava (III.)

- § 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

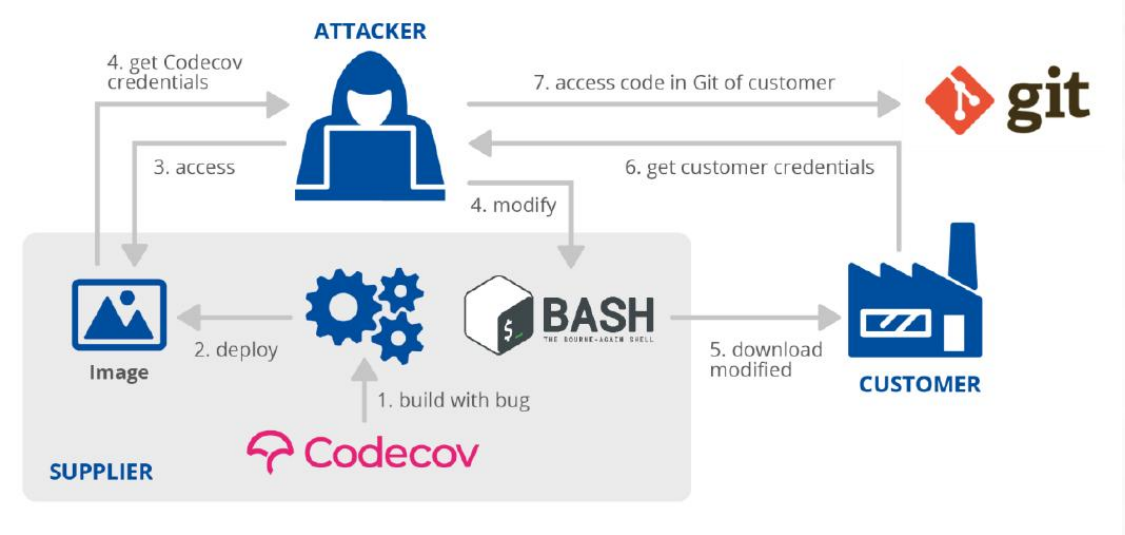
- odporúčanie Komisie 2003/361/ES
- **viac ako 50** zamestnancov a
- obrat alebo súvaha **nad 10 mil. €**

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

Slovenská právna úprava (IV.)

- rozšírenie pôsobnosti na **dodávateľské reťazce**

- § 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

Mýtus – KB je súčasný fenomén

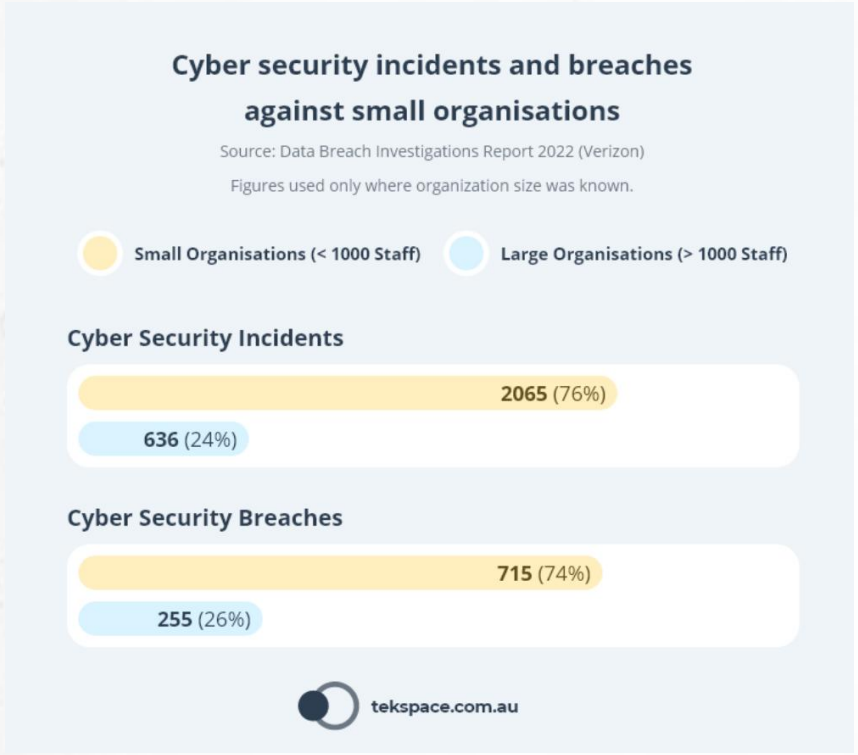
- bezpečnostné hrozby a bezpečnostné opatrenia existovali aj pred smernicou NIS, smernicou NIS 2 a zákonom o kybernetickej bezpečnosti

- povinnosť venovať sa informačnej a kybernetickej bezpečnosti bola už predtým
- rok 2000 - ISO/IEC 17799:2000
- rok 2022 - ISO/IEC 27002:2022

Zdroj: https://advisera.com/27001academy/explanation-of-11-new-iso-27001-2022-controls/

Mýtus – KB je problém veľkých a známych (I.)

- 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

Mýtus – KB je problém veľkých a známych (II.)

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

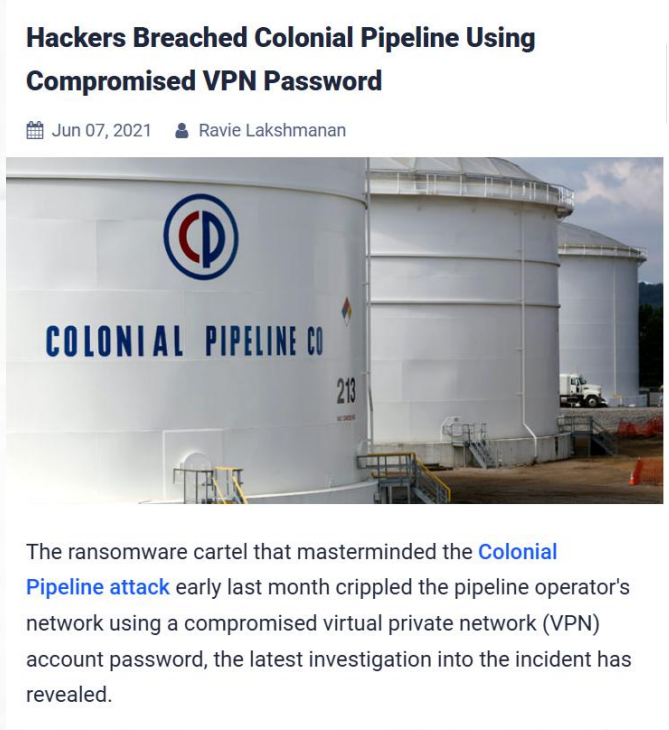
- § 17 ods. 1 písm. e) zákona o KB - osoba, ktorá spĺňa najmenej podmienky **veľkosti pre stredný podnik** a vykonáva činnosť v niektorom zo sektorov podľa prílohy č. 1 alebo prílohy č. 2 zákona o KB

- 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/

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

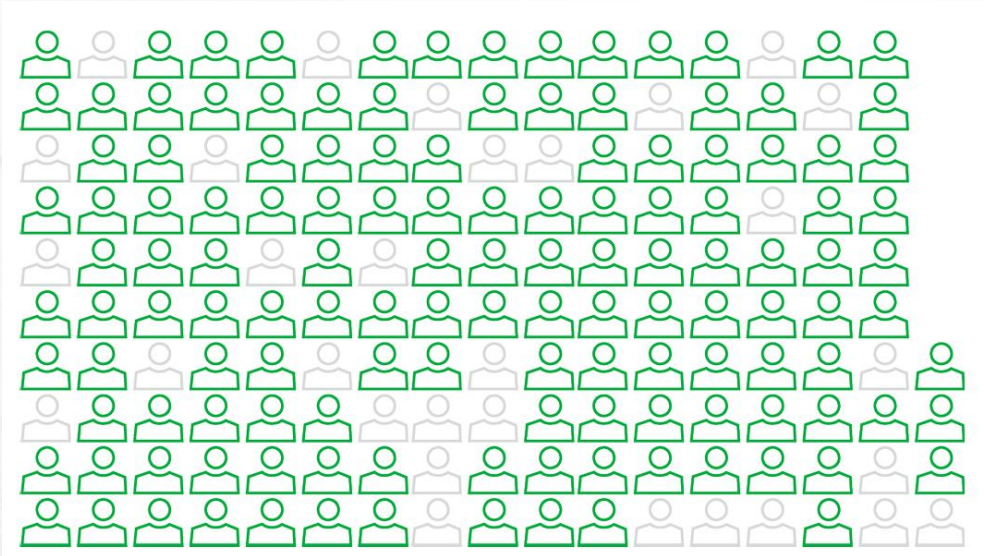
The ransomware cartel that masterminded the Colonial Pipeline attack early last month crippled the pipeline operator's network using a compromised virtual private network (VPN) account password, the latest investigation into the incident has revealed.

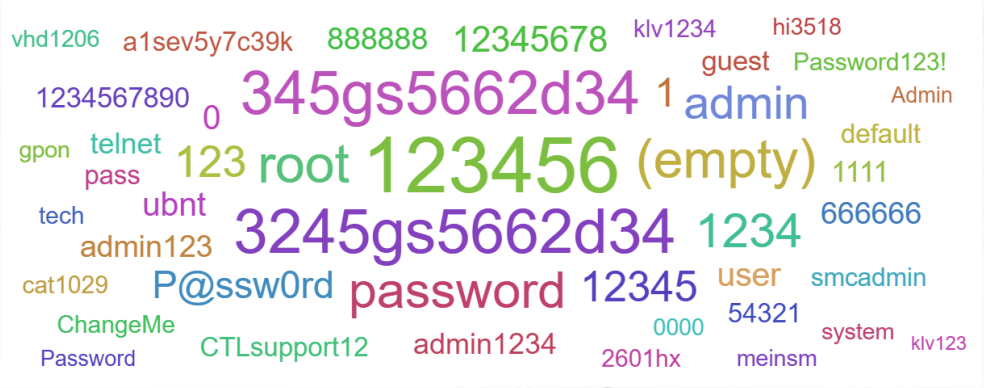
Zdroj: https://thehackernews.com/2021/06/hackers-breached-colonial-pipeline.html

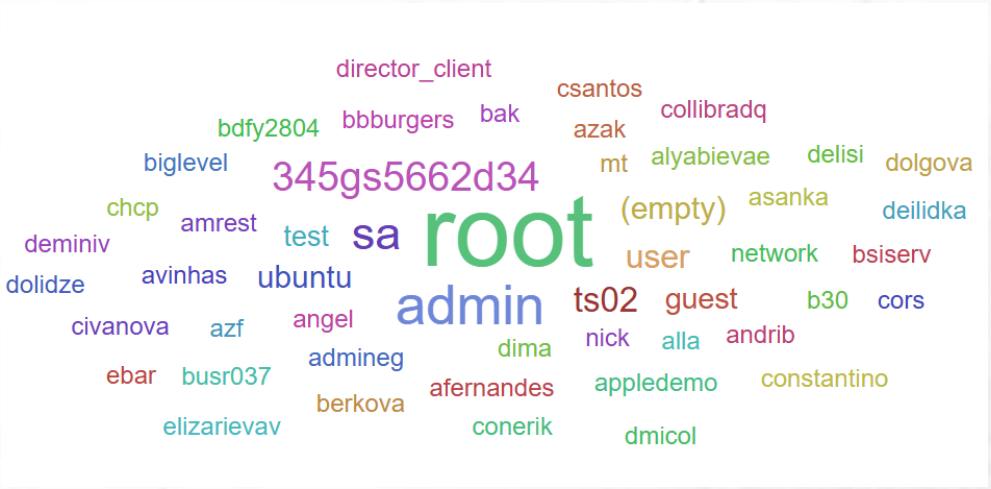
Mýtus – KB je zodpovednosť len IT a MKB (II.)

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

82 %



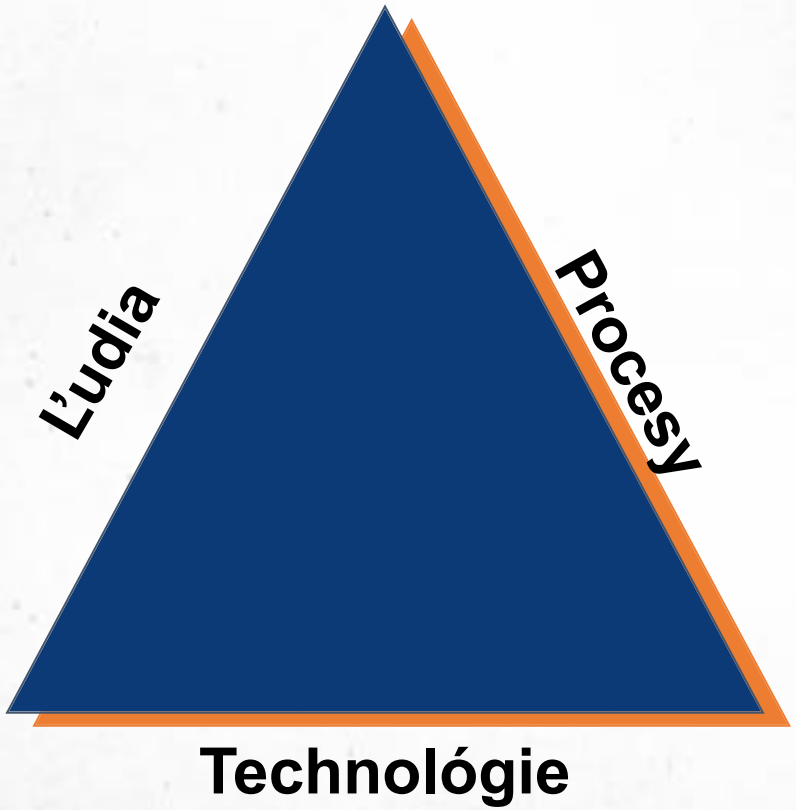


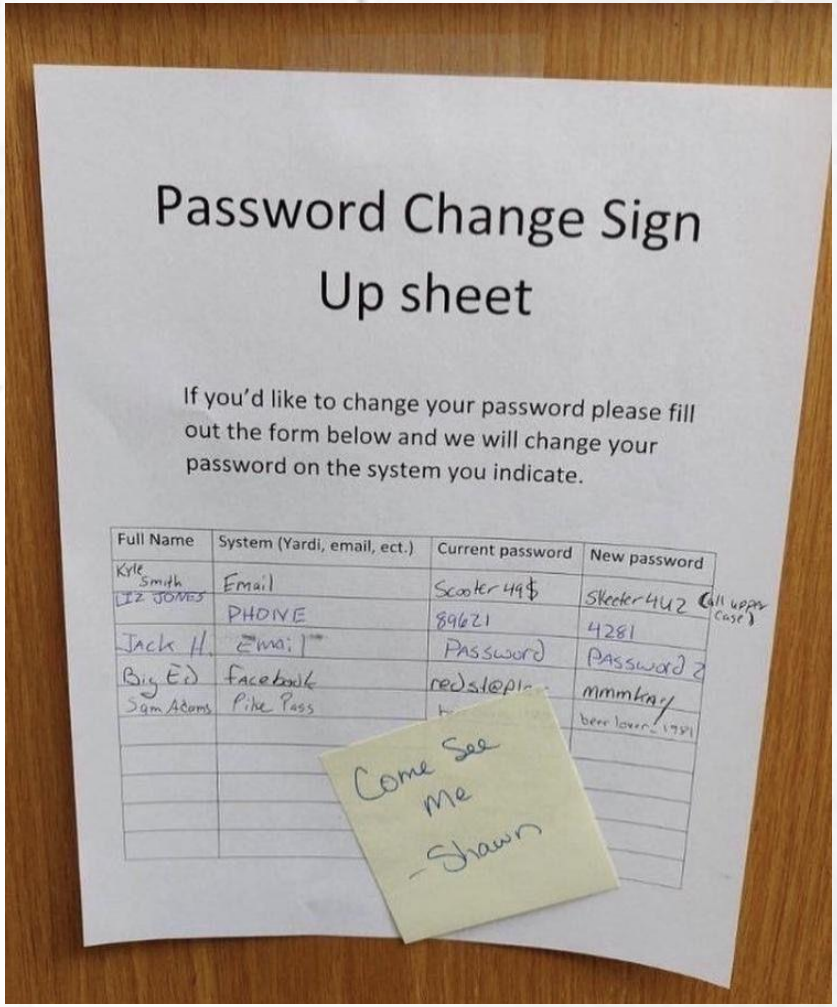


Zdroj: Verizon: DBIR Data Breach Investigations Report, 2022.

Mýtus – KB je jednorazový projekt (I.)

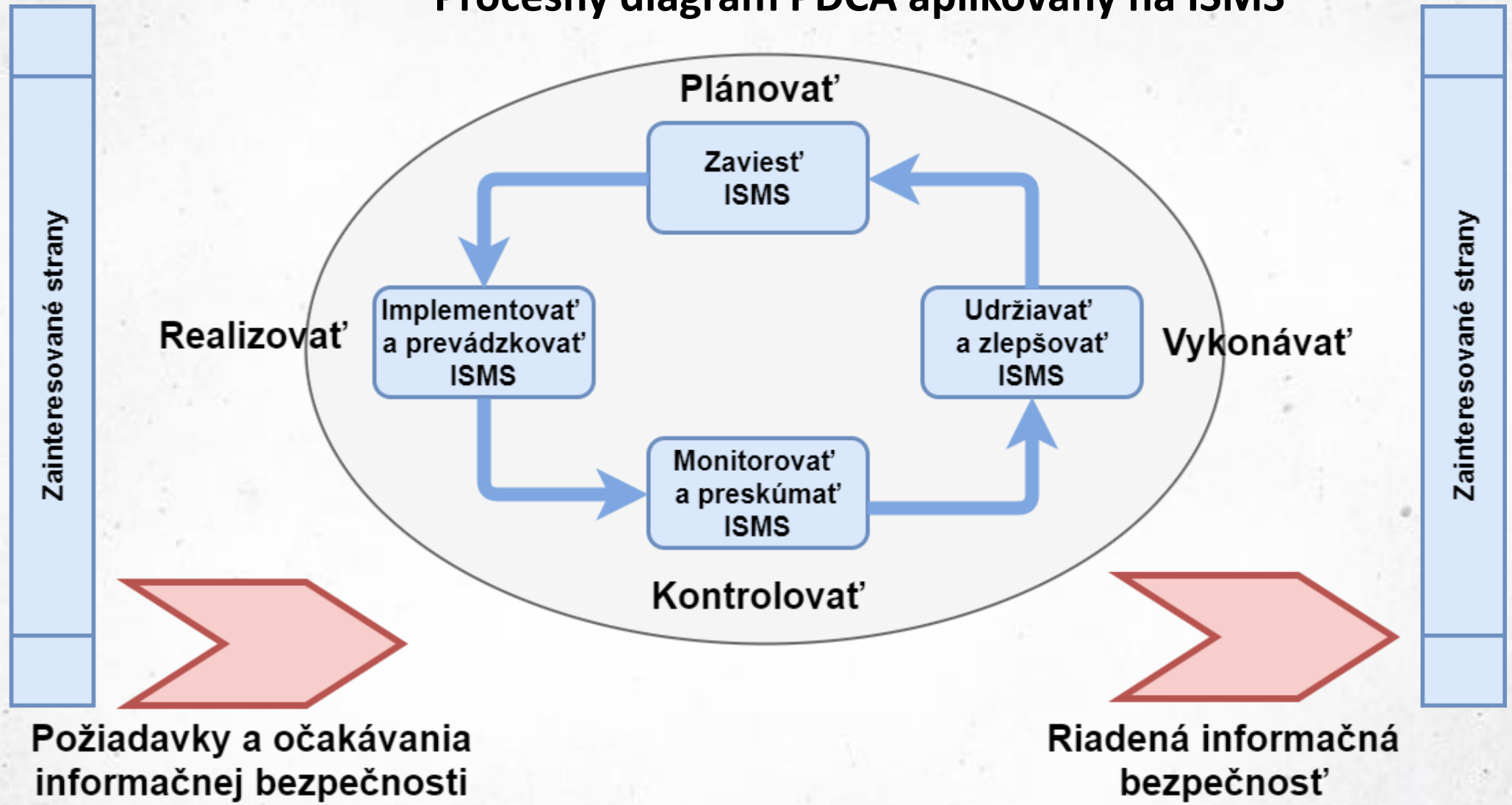
- kybernetická bezpečnosť je neustály proces, nie stav
- ide o prepojenie procesov, ľudí a technológií
- požadujte kvalitu a nenechajte sa odbiť zložitými pojmami (BIA, RTO, RPO, threat hunting, CTI, ...)





Mýtus – KB je jednorazový projekt (II.)

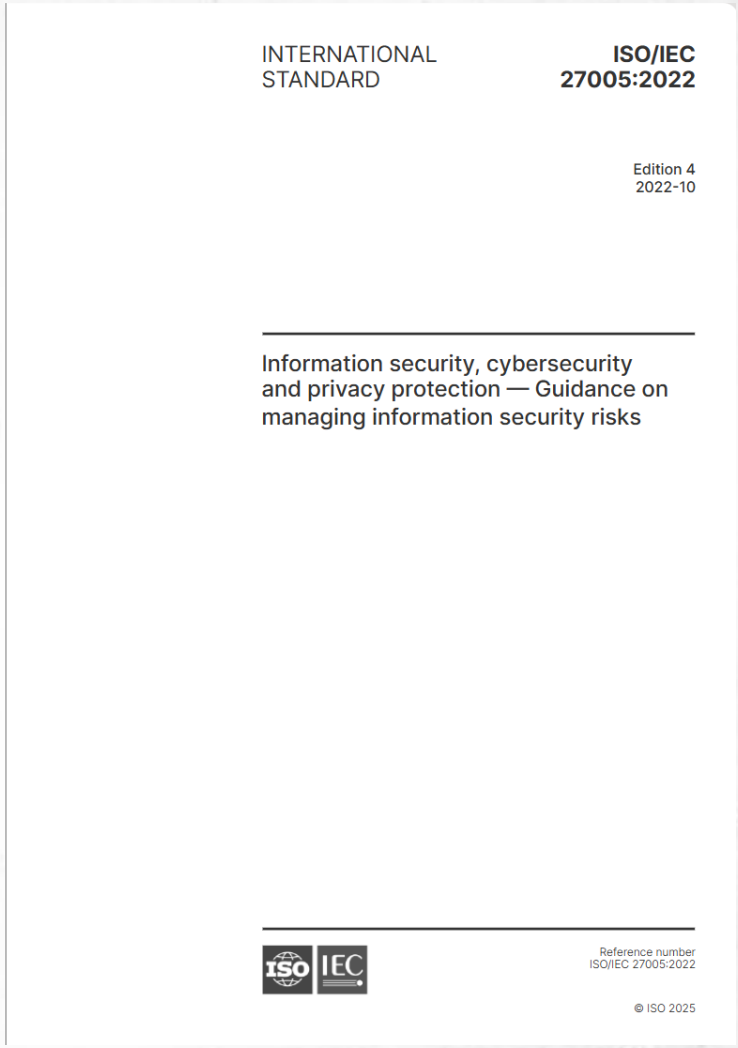
Procesný diagram PDCA aplikovaný na ISMS



Riadenie kybernetickej bezpečnosti (I.)

- **riziko**
  - potenciál straty alebo narušenia v dôsledku kybernetického bezpečnostného incidentu vyjadrený ako kombinácia rozsahu takejto straty alebo narušenia a pravdepodobnosti výskytu kybernetického bezpečnostného incidentu (§3 ods. 1 písm. i) ZoKB)

- Riadenie rizika - ISO/IEC 27005:2022 Informačné technológie – Bezpečnostné metódy – Riadenie rizík informačnej bezpečnosti


INTERNATIONAL STANDARD

ISO/IEC 27005:2022

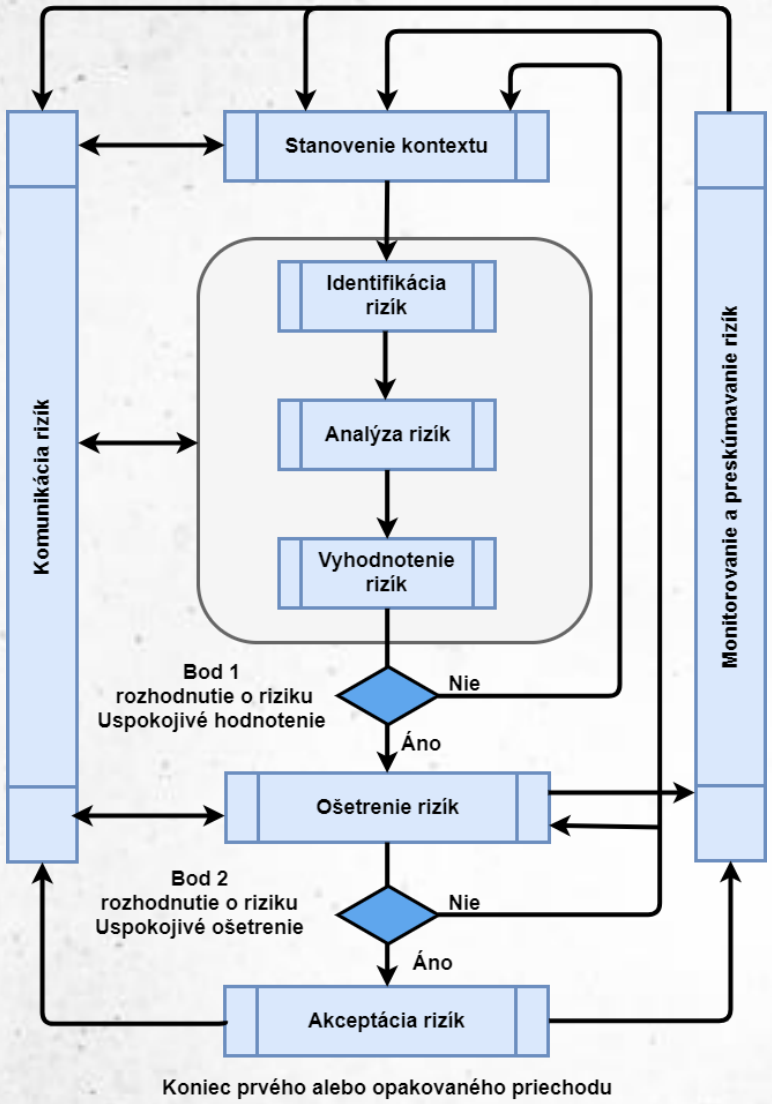
Edition 4
2022-10

Information security, cybersecurity and privacy protection — Guidance on managing information security risks

Reference number
ISO/IEC 27005:2022

© ISO 2025

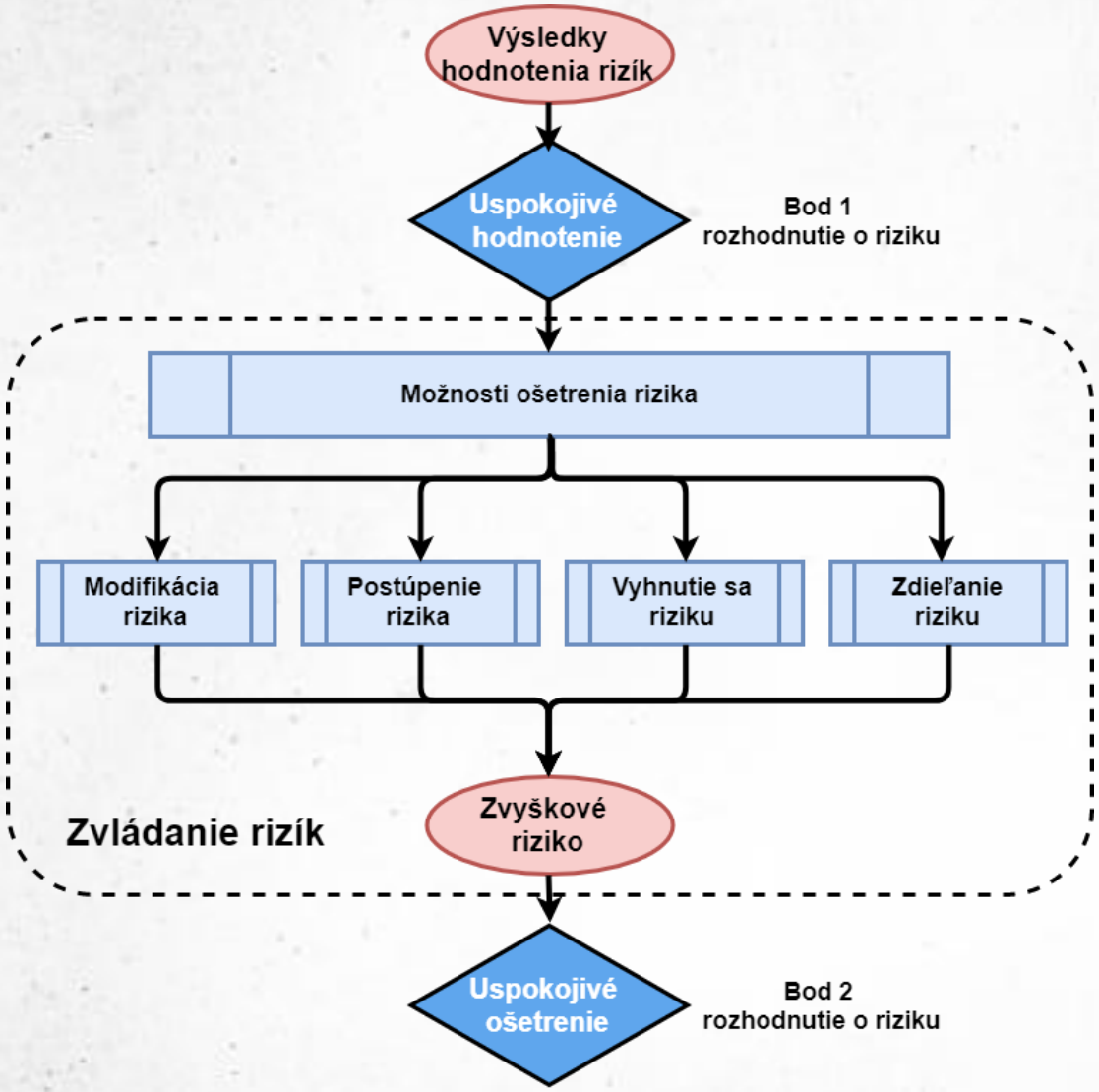
Riadenie kybernetickej bezpečnosti (II.)

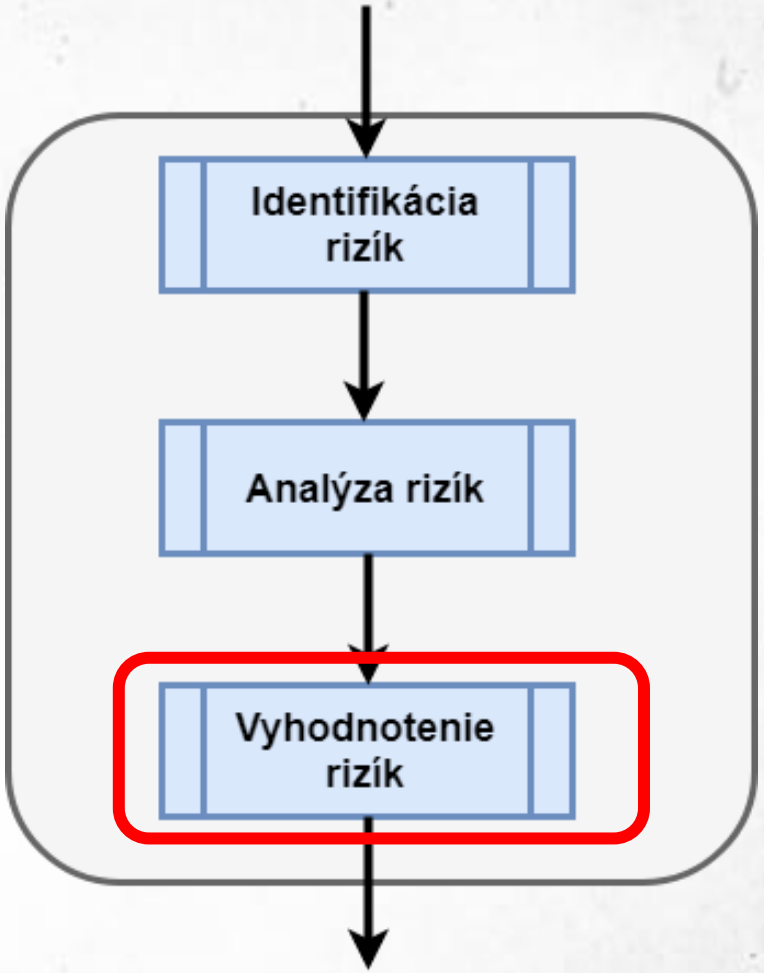


Vyjadrenie rizika (kvalitatívny prístup)

Dopad → Pravdepodobnosť ↓	nízky	stredný	Vysoký
Nulová	Nulové	Nulové	Nulové
Nízka	Nízke	Nízke	Stredné
Stredná	Nízke	Stredné	Vysoké
Vysoká	Stredné	Vysoké	Vysoké

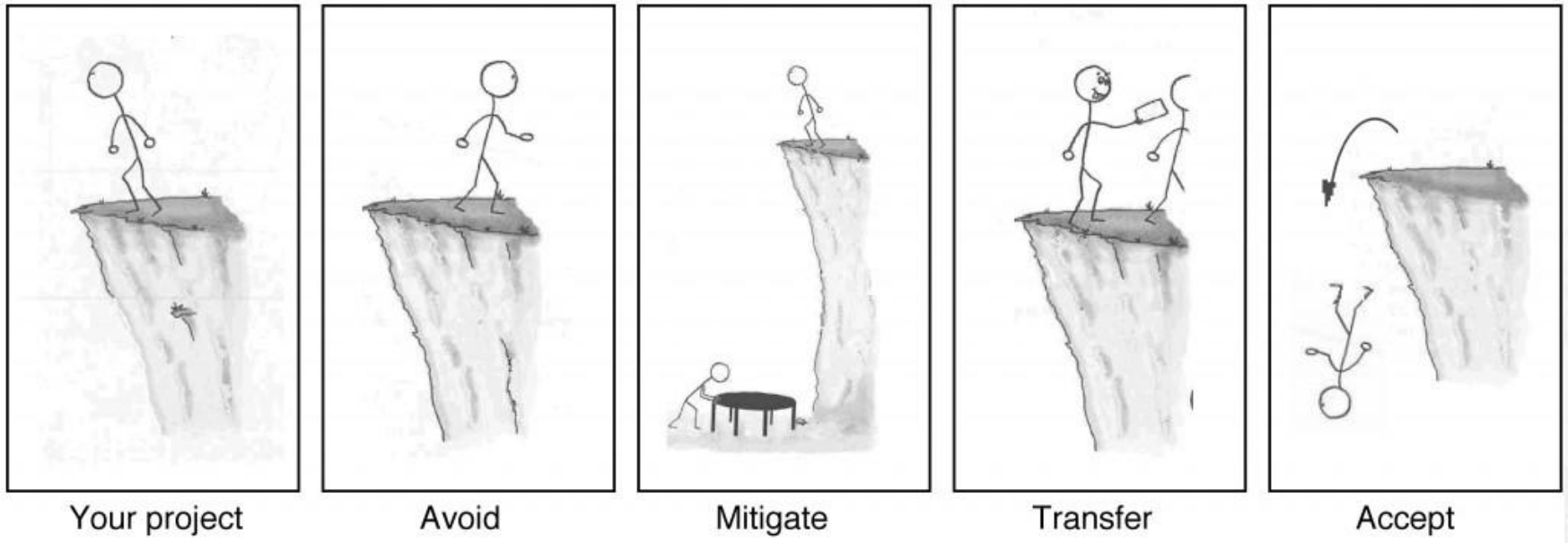
Riadenie kybernetickej bezpečnosti (III.)





Riadenie kybernetickej bezpečnosti (IV.)

- Akceptovanie/Zachovanie rizika (Accept)
- Vyhnutie sa riziku (Avoid)
- Limitácia/Zníženie rizika (Mitigate / Limit)
- Presun rizika (Transfer)



Zdroj: http://cnx.org/content/col11120/1.4/

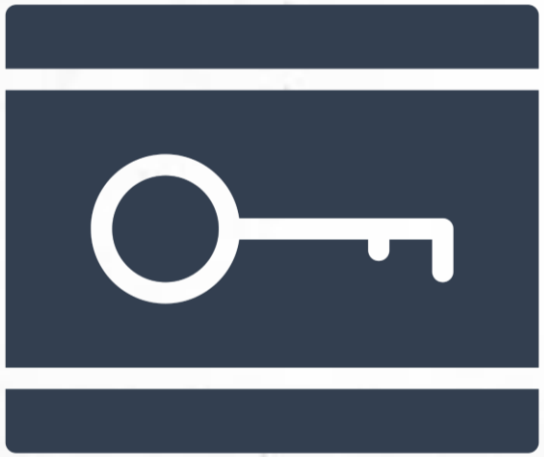
Bezpečnostné opatrenia (I.)

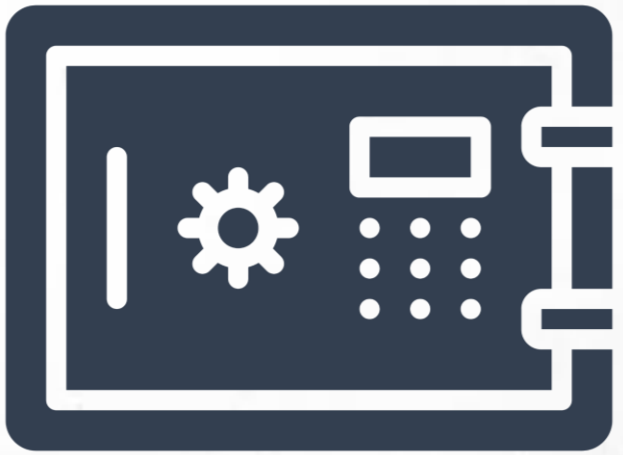
- **Bezpečnostné opatrenia**
  - sú úlohy, procesy, role a technológie v organizačnej, personálnej, fyzickej a technologickej oblasti, ktorých cieľom je dosiahnutie, zaručenie a udržanie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov a operačných technológií. Bezpečnostné 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.)

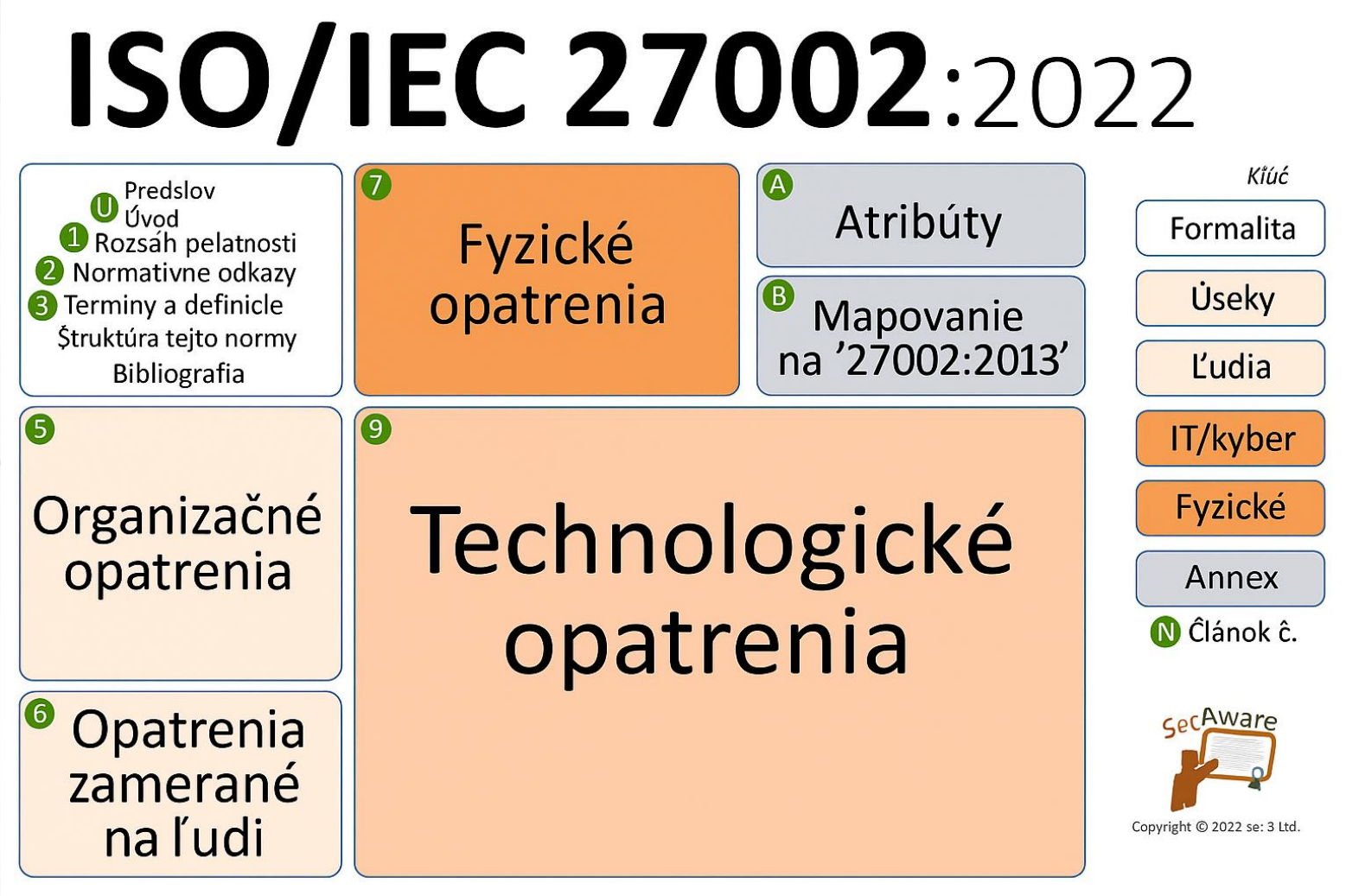
- akákoľvek činnosť, technické zariadenie, proces, mechanizmus, alebo čokoľvek, čo chráni informačný systém a jeho časti (aktíva) pred pôsobením konkrétnych hrozieb alebo hrozby.

- **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. 2 Zákona o KB: Bezpečnostné opatrenia sa prijímajú a realizujú najmä pre oblasť

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.

Bezpečnostné opatrenia (V.)

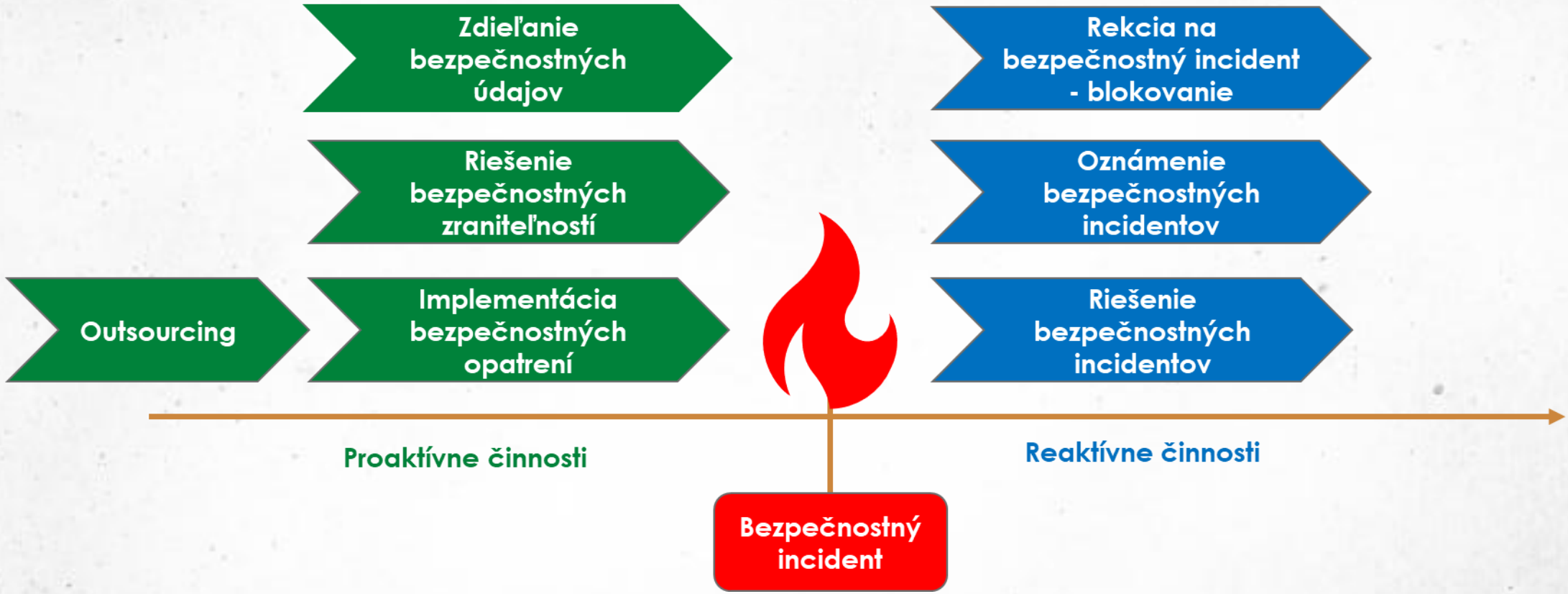
- **Vyhláška NBÚ č. 227/2025 Z. z.,** ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení

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.

Preventívne a reaktívne činnosti (I.)



Preventívne a reaktívne činnosti (II.)

- **§ 15 ods. 2 ZoKB - preventívne služby:**
  - vytváraním bezpečnostného povedomia,
  - výcvikom,
  - spoluprácou s ostatnými jednotkami CSIRT,
  - monitorovaním a evidenciou zraniteľností, kybernetických hrozieb, kybernetických kríz a kybernetických bezpečnostných incidentov,
  - pripojením na jednotný informačný systém kybernetickej bezpečnosti,
  - poskytovaním informácií a údajov do jednotného informačného systému kybernetickej bezpečnosti,
  - prijímaním a zasielaním včasného varovania pred kybernetickými bezpečnostnými incidentmi prostredníctvom jednotného informačného systému kybernetickej bezpečnosti,
  - poskytovaním pomoci s monitorovaním siete a informačného systému alebo vykonávaním takéhoto monitorovania po dohode so správcom siete alebo prevádzkovateľom siete alebo prevádzkovateľom informačného systému,

Preventívne a reaktívne činnosti (III.)

§ 15 ods. 3 ZoKB - reaktívne služby:

- výstraha a varovanie,
- detekcia kybernetických bezpečnostných incidentov,
- analýza kybernetických bezpečnostných incidentov,
- odozva, ohraničenie, riešenie a náprava následkov kybernetických bezpečnostných incidentov,
- asistencia pri riešení kybernetického bezpečnostného incidentu na mieste,
- reakcia na kybernetický bezpečnostný incident,
- podpora reakcií na kybernetické bezpečnostné incidenty,
- koordinácia reakcií na kybernetické bezpečnostné incidenty,
- návrh opatrení na zabránenie ďalšiemu pokračovaniu, šíreniu a opakovanému výskytu kybernetických bezpečnostných incidentov.

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