KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Sieťová a komunikačná bezpečnosť

01 Úvod do sieťovej bezpečnosti

KCKB UPJS CSIRT UPJS

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

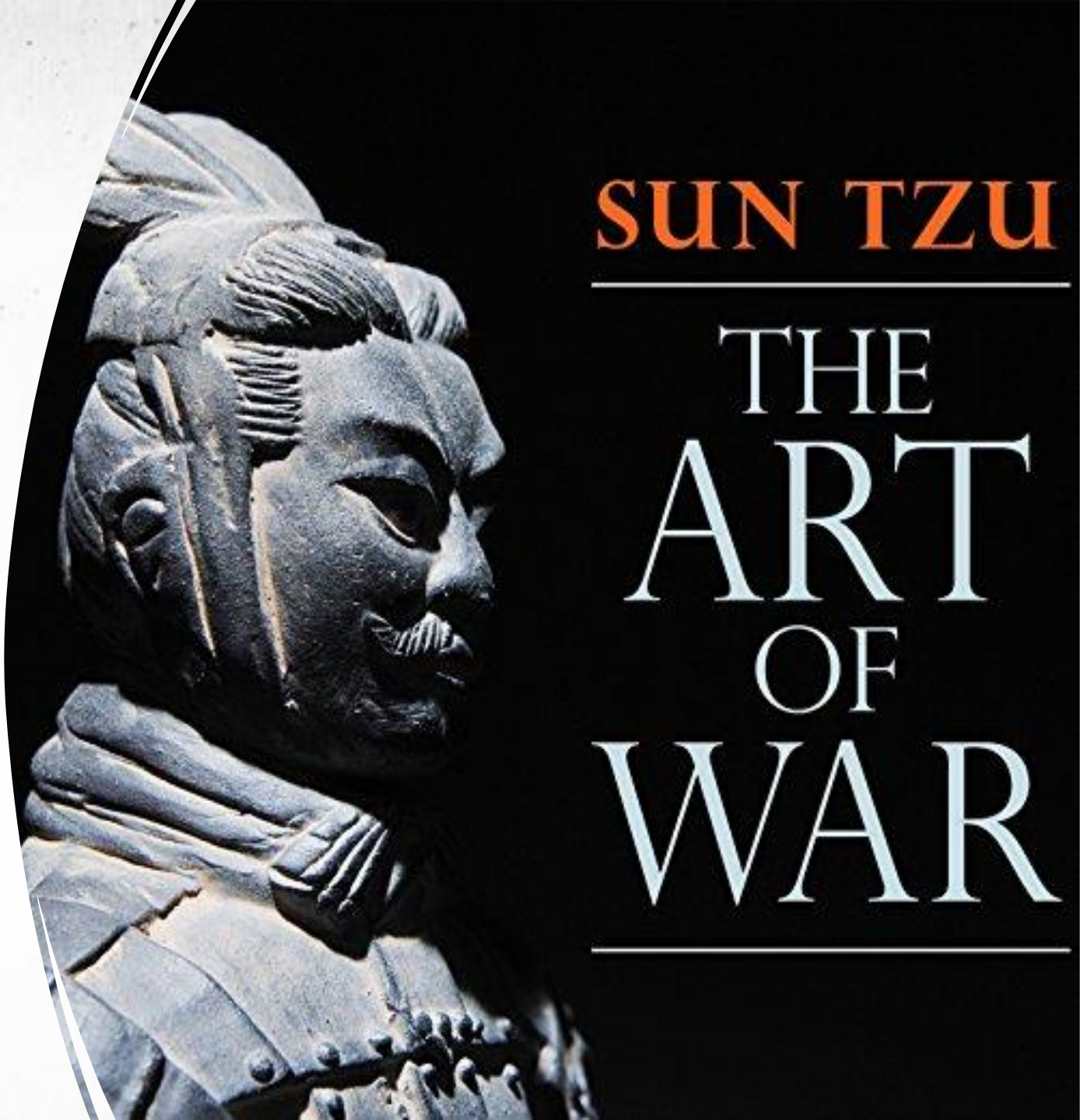
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Úvod do sieťovej bezpečnosti

- sieťová bezpečnosť
- klasifikácia útokov
- triáda CIA
- právna úprava

„Ak poznáš nepriateľa
i seba samého, nebudeš porazený.
Ak nepoznáš nepriateľa, ale
poznáš sám seba, máš 50% šancu
na víťazstvo. Ak nepoznáš sám
seba, ani nepriateľa, prehráš.“

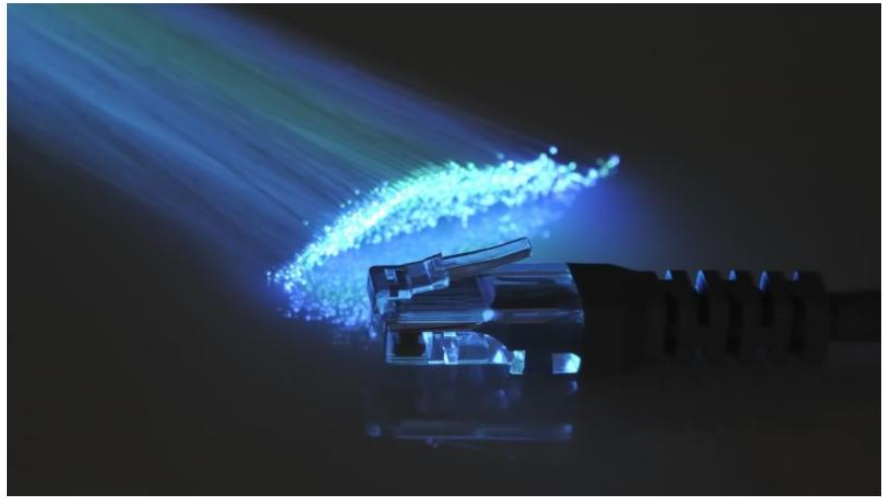
- Sun Tzu



Zdroj: Zdroj: https://www.amazon.com/The-Art-of-War-Sun-Tzu-audiobook/dp/B01MQSRAMM/

Sieťová bezpečnosť (I.)

Hackeri útočili na slovenského poskytovateľa internetu. Najväčším DDoS útokom v histórii



Zdroj: iStockphoto

Security News This Week: The Biggest DDoS Attack in History Hit Russian Tech Giant Yandex

Plus: A TrickBot hacker arrest, a Fortinet VPN password leak, and more of the week's top security news.

Recently Discovered 'EwDoor' Botnet Targets US AT&T Devices

Researchers Who Accessed Control Center Say at Least 5,700 Edge Devices Linked

Dan Gunderman (dangun127) · December 1, 2021

Twitter Facebook LinkedIn Credit Eligible Get Permission

(Photo: Mike Mozart via Flickr)

Zdroj: https://www.wired.com/story/yandex-ddos-fortinet-passwords-security-news/, https://www.govinfosecurity.com/recently-discovered-ewdoor-botnet-targets-us-att-devices-a-18032, https://zive.aktuality.sk/clanok/152131/hackeri-utocia-na-slovenskeho-poskytovatela-internetu-najvacsim-ddos-utokom-v-historii/

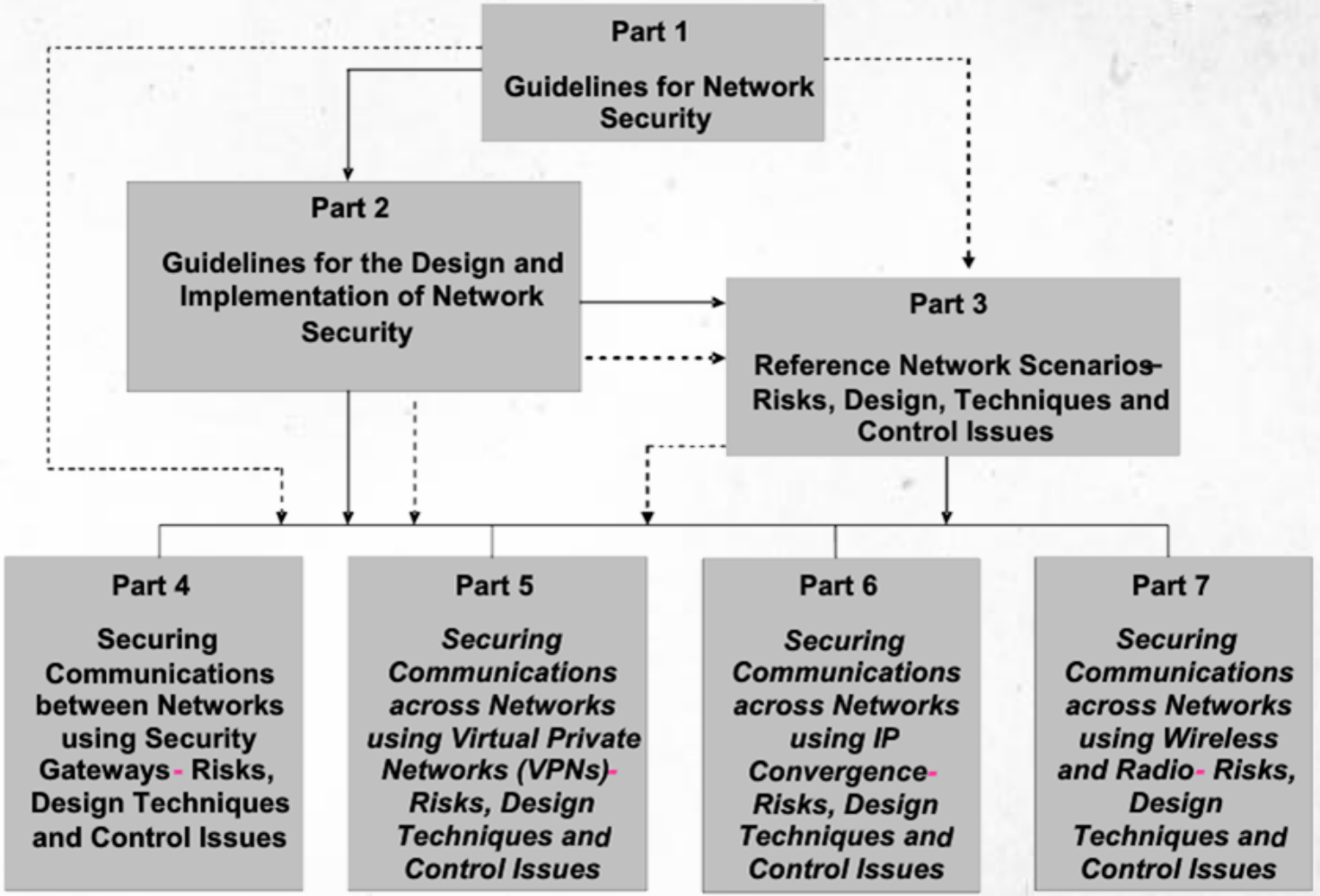
Sieťová bezpečnosť (II.)

- **Sieťová bezpečnosť**
  - súbor noriem s odporúčaniami pre implementáciu opatrení, ktoré sa vzťahujú k bezpečnosti sietí (vnútornej ochrany a ochrany perimetra).

- **Bezpečnosť sieťovej infraštruktúry**
  - stupeň zabezpečenia digitálneho prenosového prostredia zabezpečujúceho dôvernosť a neporušenosť komunikácie.

Sieťová bezpečnosť (III.)

- **ISO/IEC 27033**
  - normy obsahujúce podrobný návod na **implementáciu bezpečnostných mechanizmov** uvedených v norme ISO/IEC 27002.
  - týkajú sa bezpečnosti zariadení pripojených do siete, sieťových služieb, užívateľov pristupujúcich do siete, informácií prenášaných po sieti a tiež správy týchto bezpečnostných opatrení.

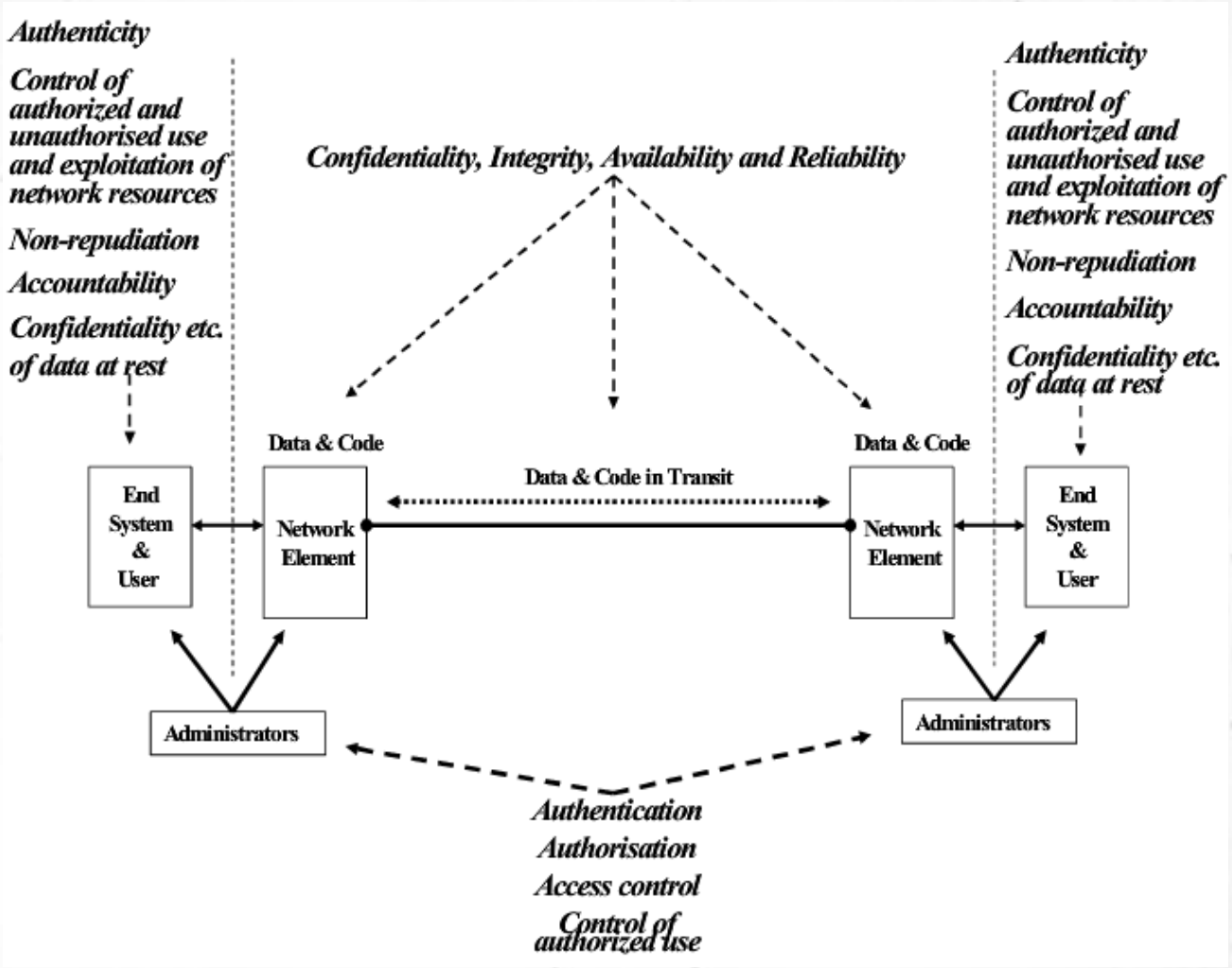


Zdroj: ISO/IEC 27033-1:2011

Sieťová bezpečnosť (IV.)

- **ISO/IEC 27033**

Zdroj: ISO/IEC 27033-1:2011



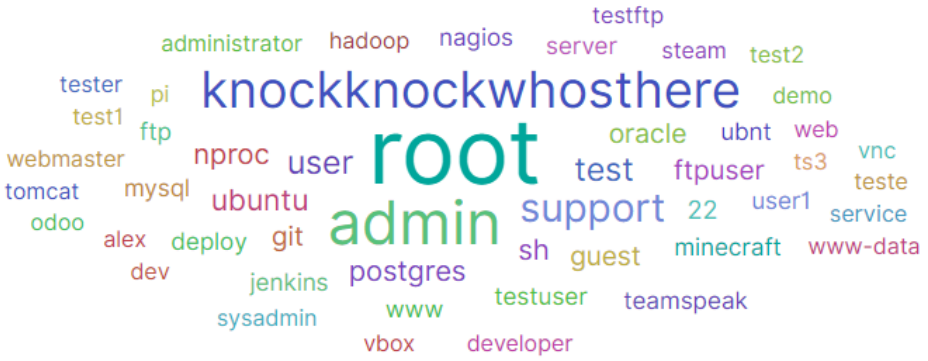
Sieťová bezpečnosť (V.)

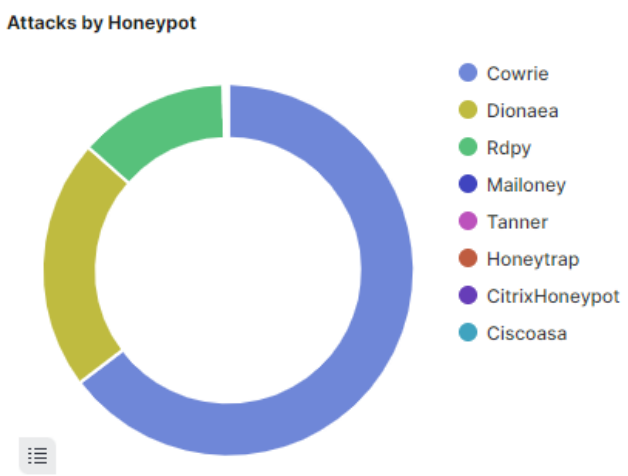
Pasívna obrana	Aktívna obrana: Šedá zóna		Ofenzívna činnosť
▪ Základné bezpečnostné kontroly ▪ Firewally ▪ Monitoring ▪ AV systémy ▪ IDS ▪ ...	▪ Zdieľanie informácií ▪ Podvodný systémy ▪ Hunting ▪ Zbieranie informácií na darknete ▪ ...	▪ Zastavenie botnetov ▪ White-hat ransomvér ▪ ...	▪ Späť hacknutie ▪ Akcie zamerané na zničenie/poškodenie ▪ ...

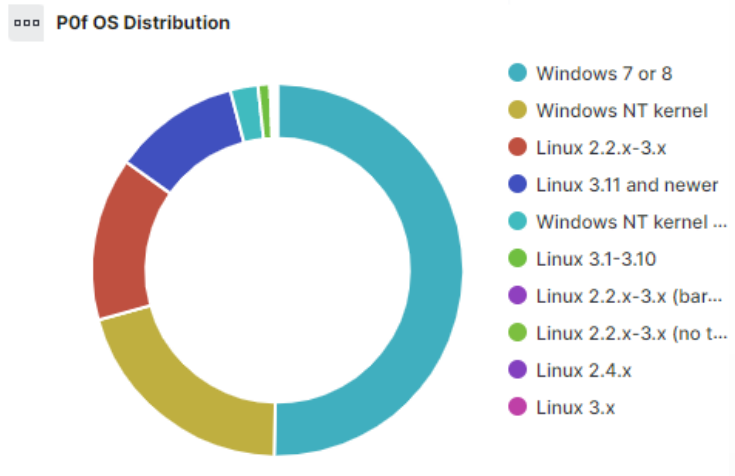
← Menšie riziko — Vyššie riziko →

Zdroj: https://cchs.gwu.edu/gray-zone-active-defense-private-sector-against-cyber-threats&usg=AOvVaw1_T0DfdpAvAMvozdDlfDsn

Poznaj svojho nepriateľa (II.)

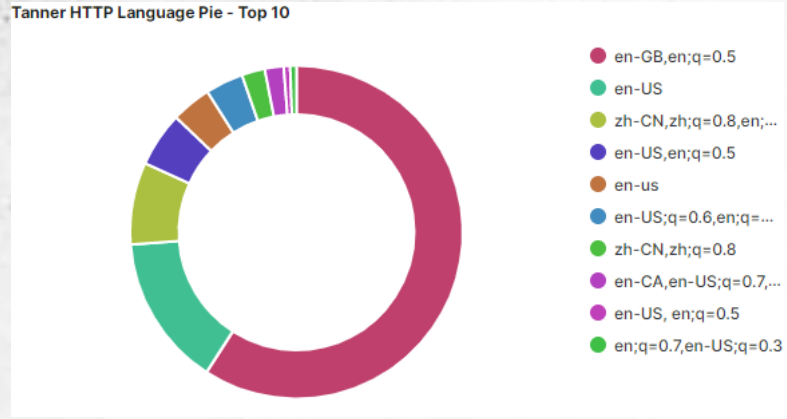


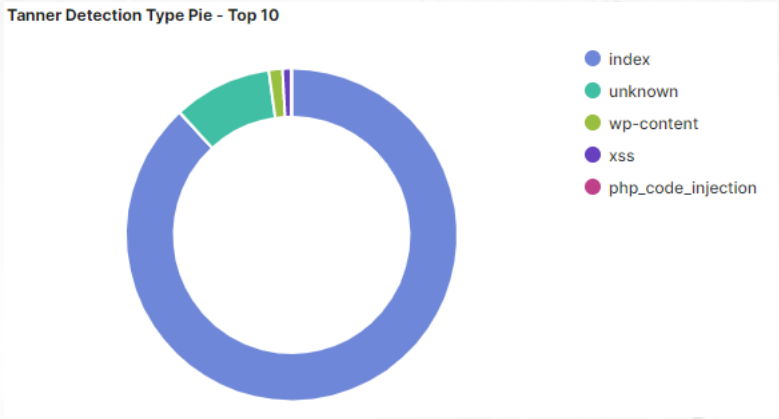


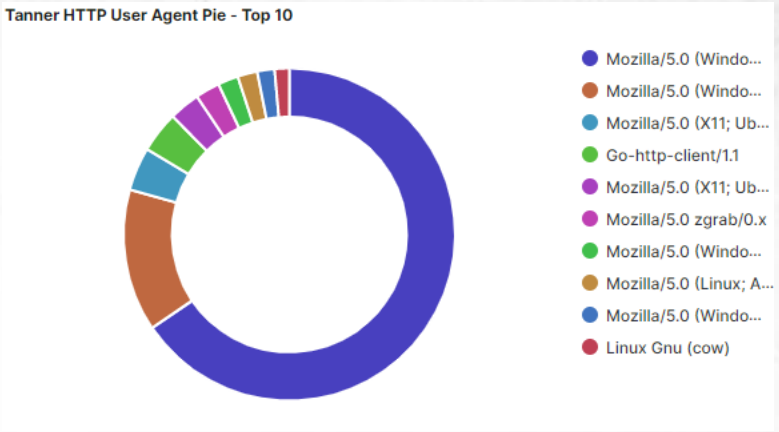


uname -a	6,822
which ls	6,804
cat /proc/cpuinfo | grep model | grep name | wc -l	6,802
cat /proc/cpuinfo | grep name | head -n 1 | awk '{print $4,$5,$6,$7,$...	6,802
ls -lh $(which ls)	6,802
crontab -l	6,801
free -m | grep Mem | awk '{print $2 ,$3, $4, $5, $6, $7}'	6,801
top	6,801
uname	6,801
uname -m	6,801

Poznaj svojho nepriateľa (III.)

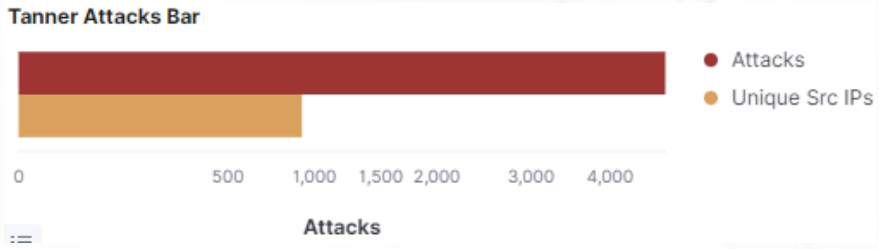






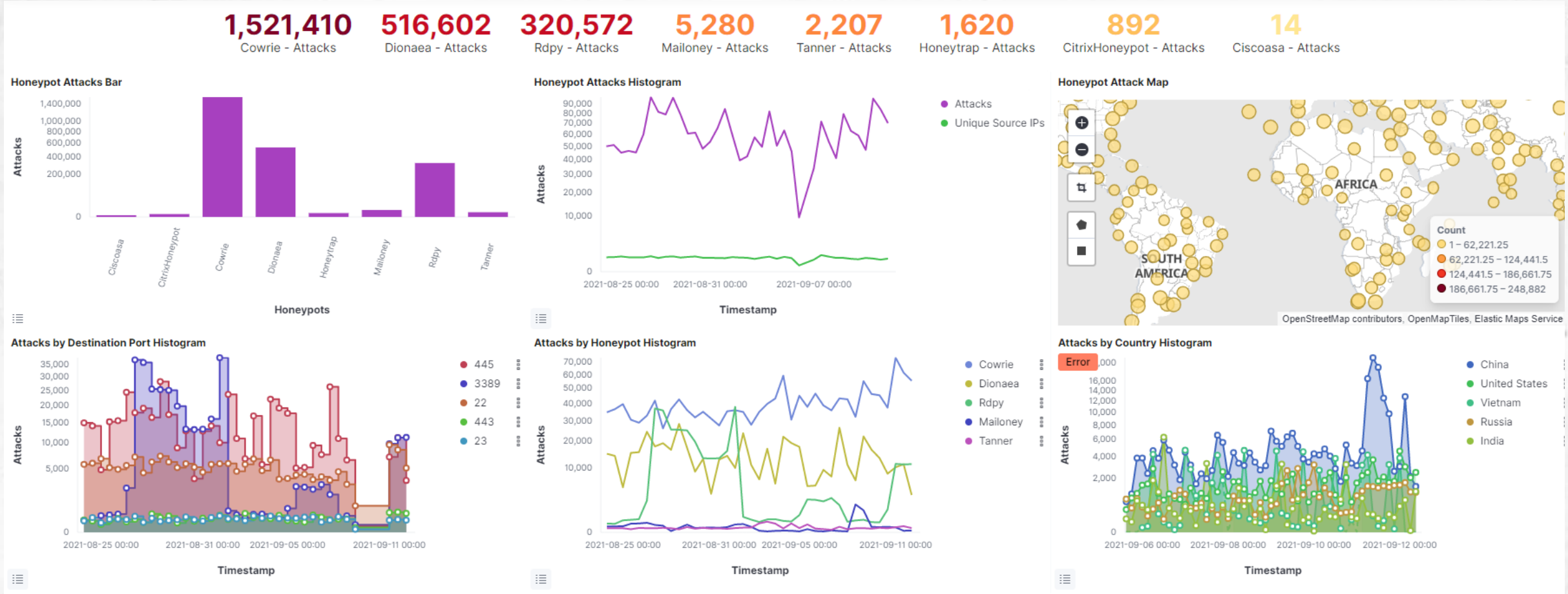
Tanner URI - Top 10

URI	Count
/	964
/boaform/admin/formLogin	139
http://azenv.net/	97
/config/getuser?index=0	80
/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php	73
/_ignition/execute-solution	41
/.env	36
/robots.txt	36
/data/tanner/log/tanner_report.json	34
/?XDEBUG_SESSION_START=phpstorm	31



Poznaj svojho nepriateľa (IV.)

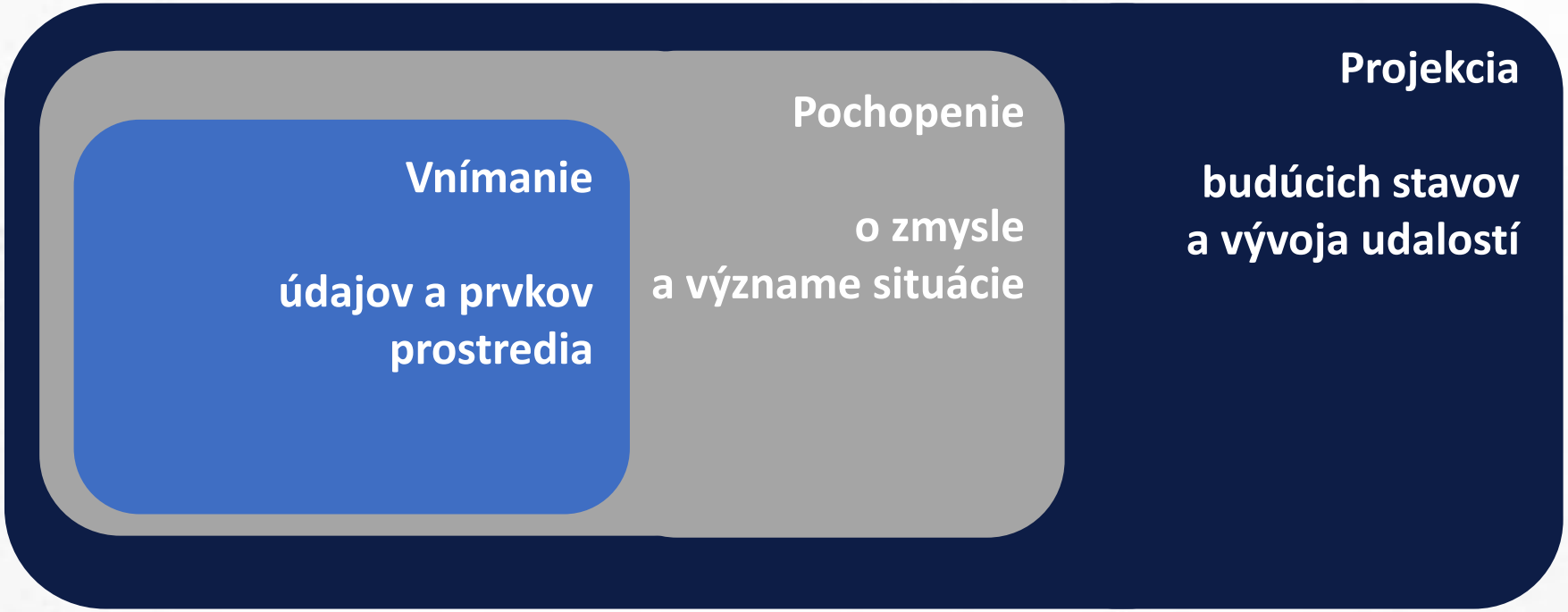
Sieťové situačné povedomie (I.)



Sieťové situačné povedomie (II.)

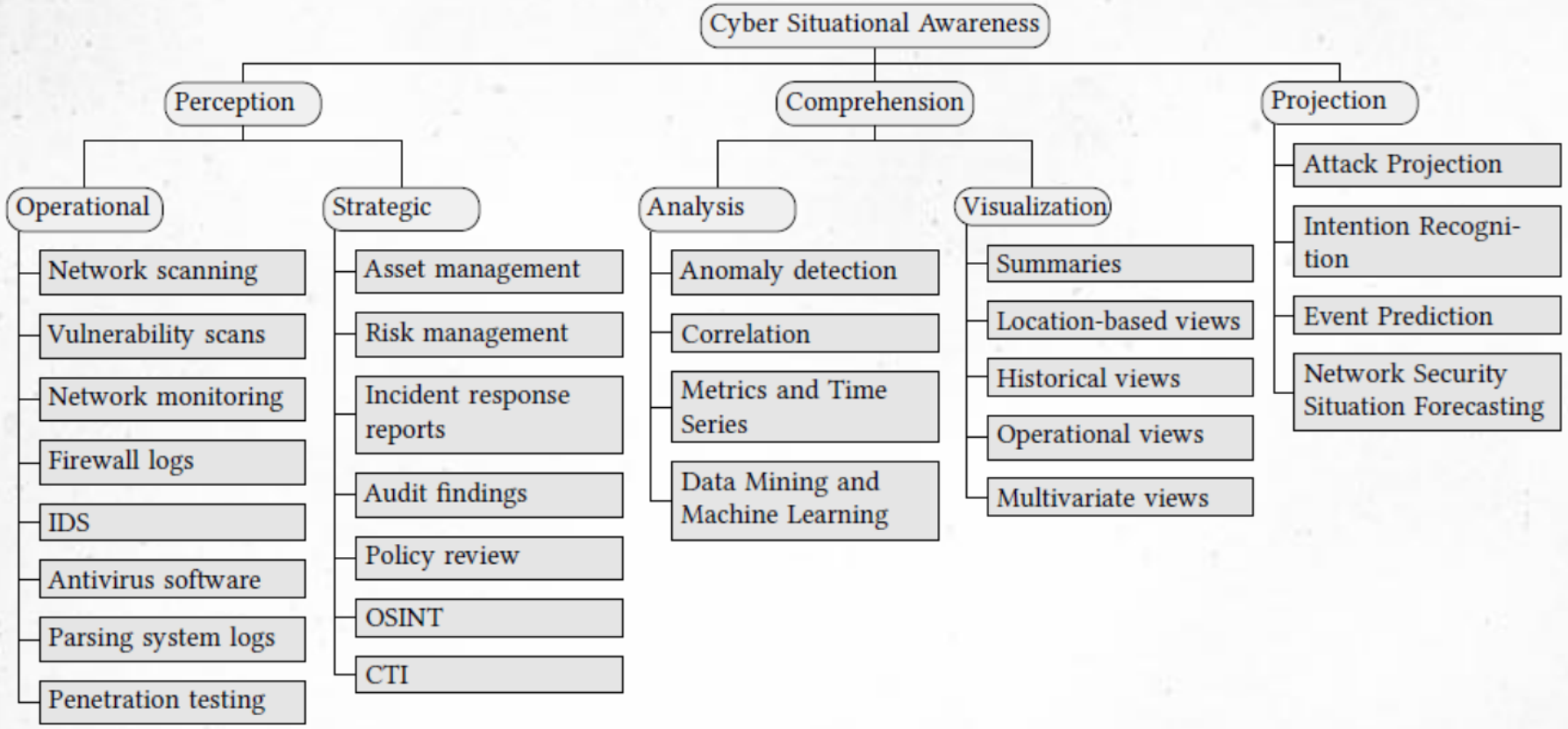
Sieťové situačné povedomie (III.)

- monitorovanie kybernetických systémov, pochopenie kybernetickej bezpečnostnej situácie reprezentovanej modelovaním kybernetických hrozieb alebo súvisiacimi bezpečnostnými výstrahami a predpovedanie zmien v kybernetickej bezpečnostnej situácii (Husák, 2020).



Zdroj: Husák, M., Jirsík, T., & Yang, S. J. (2020, August). SoK: contemporary issues and challenges to enable cyber situational awareness for network security. In *Proceedings of the 15th International Conference on Availability, Reliability and Security* (pp. 1-10).

Sieťové situačné povedomie (IV.)



Zdroj: Husák, M., Jirsík, T., & Yang, S. J. (2020, August). SoK: contemporary issues and challenges to enable cyber situational awareness for network security. In *Proceedings of the 15th International Conference on Availability, Reliability and Security* (pp. 1-10).

Bezpečnostné opatrenia (I.)

- Vyhláška NBÚ č. 227/2025 Z. z. o bezpečnostných opatreniach – príloha č. 2

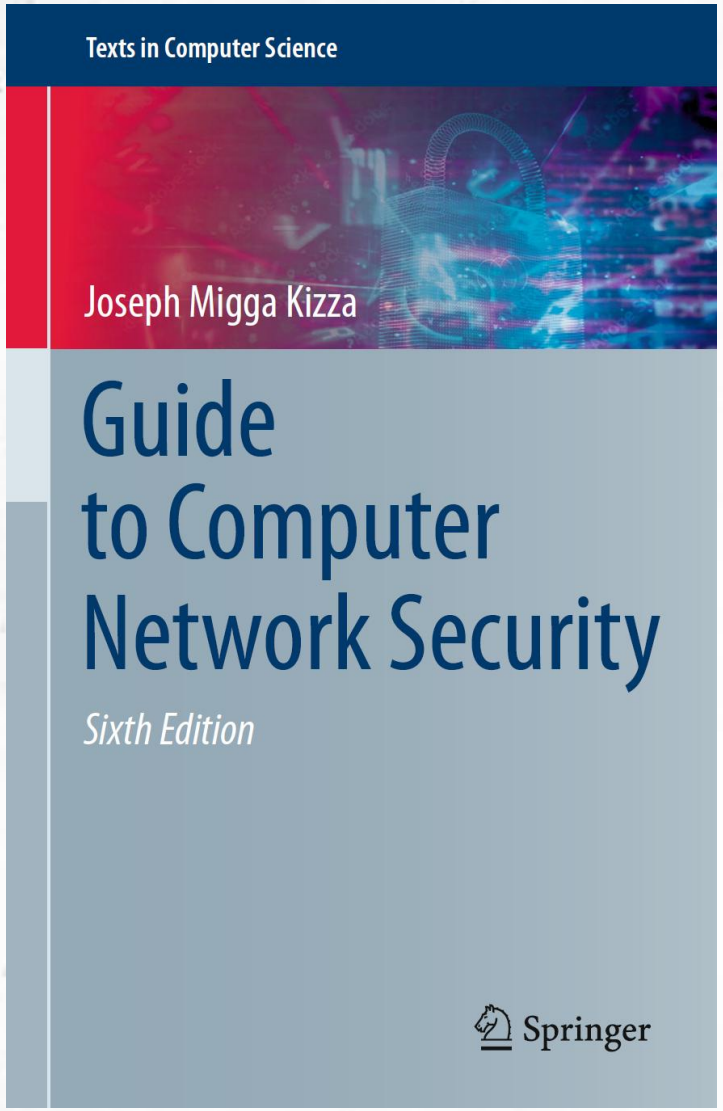
Položka	Bezpečnostné opatrenia pre systémovú bezpečnosť, sieťovú bezpečnosť a komunikačnú bezpečnosť podľa § 20 ods. 2 písm. m) zákona prijíma prevádzkovateľ základnej služby tak, že:	Relevancia pre IKT*		Relevancia pre OT*	
		PZS*	PKZS*	PZS*	PKZS*
101.	sú vypracované a zavedené postupy na prenos informácií 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
104.	na informačné systémy, siete a technické prostriedky, ktoré spracúvajú, uchovávajú alebo prenášajú chránené informácie, podľa klasifikácie informácií, sa aplikujú opatrenia na prevenciu úniku informácií vrátane zohľadnenia proprietárnych protokolov a dátových tokov; identifikácia vybraných informácií prebieha pomocou klasifikácie informácií	ÁNO	ÁNO	ÁNO	ÁNO

Bezpečnostné opatrenia (II.)

- Vyhláška NBÚ č. 227/2025 Z. z. o bezpečnostných opatreniach – príloha č. 2

105.	siete a technické prostriedky sietí sa zabezpečujú, spravujú a kontrolujú s cieľom chrániť informácie v informačných systémoch, programových prostriedkoch a mobilných aplikáciách	ÁNO	ÁNO	ÁNO	ÁNO
106.	sú určené, zavedené a monitorované bezpečnostné funkcie, úrovne služieb a požiadavky týkajúce sa sieťových služieb	ÁNO	ÁNO	ÁNO	ÁNO
107.	sú prijaté a udržiavané systémy detekcie narušenia, ktoré zohľadňujú proprietárne protokoly a dátové toky	-	-	ÁNO	ÁNO
108.	pre komponenty operačných technológií je automaticky ukončovaná vzdialená relácia po stanovenom, konfigurovateľnom čase nečinnosti	-	-	ÁNO	ÁNO
109.	je definovaná a zavedená segmentácia sietí, pričom informačné systémy so službami priamo prístupnými z externých sietí sa nachádzajú v samostatných sieťových segmentoch a v rovnakom segmente sú len informačné systémy s podobným účelom	ÁNO	ÁNO	ÁNO	ÁNO
110.	sú prijaté a udržiavané mechanizmy na smerovanie a filtráciu sieťovej prevádzky do a z externých sietí cez sieťový firewall	-	-	ÁNO	ÁNO
111.	je definovaná a zavedená logická segmentácia medzi operačnými technológiami, sieťami a informačnými systémami	-	-	ÁNO	ÁNO
112.	je definovaná a zavedená fyzická segmentácia medzi operačnými technológiami, sieťami a informačnými systémami	-	-	-	ÁNO
113.	sú segmentované vybrané siete riadiaceho systému od ostatných sietí operačných technológií – toto opatrenie je relevantné pre komponenty zaradené do vrstiev* pre operačné technológie 3 a vyššie	-	-	ÁNO	ÁNO
114.	sieťový firewall pre operačné technológie je nezávislý od ostatných mechanizmov na smerovanie a filtráciu sieťovej prevádzky	-	-	ÁNO	ÁNO
115.	v sieťach určených pre operačné technológie je blokované odosielanie a prijímanie správ medzi používateľmi	-	-	ÁNO	ÁNO

Odporúčaná literatúra (I.)



KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Ďakujeme za pozornosť