Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

ZÁKON O KYBERNETICKEJ BEZPEČNOSTI

PRAKTICKÉ RADY PRE AUDIT A IMPLEMENTÁCIU POŽIADAVIEK

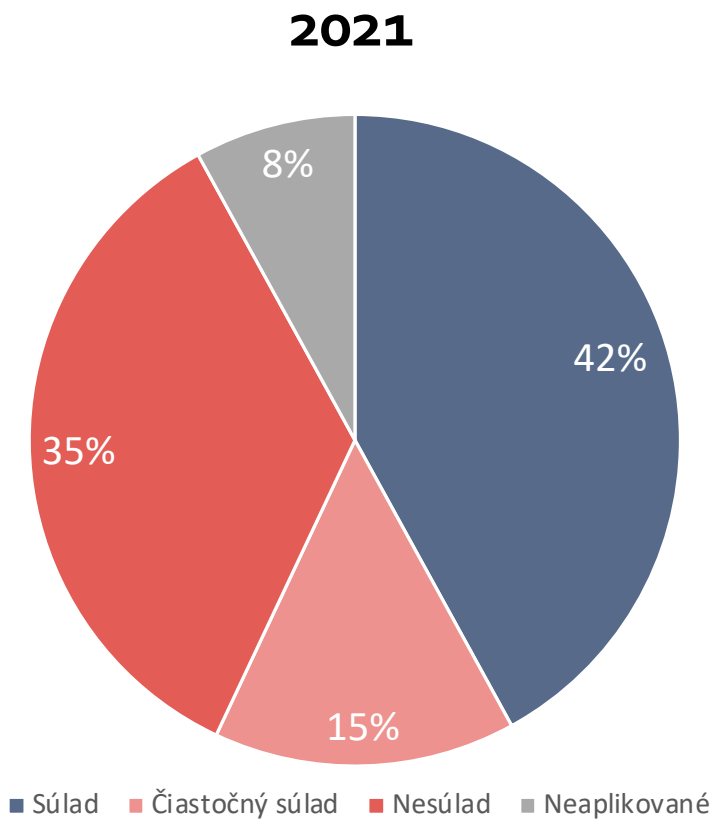
NIS2 Roadshow, Bratislava 12.11.2024

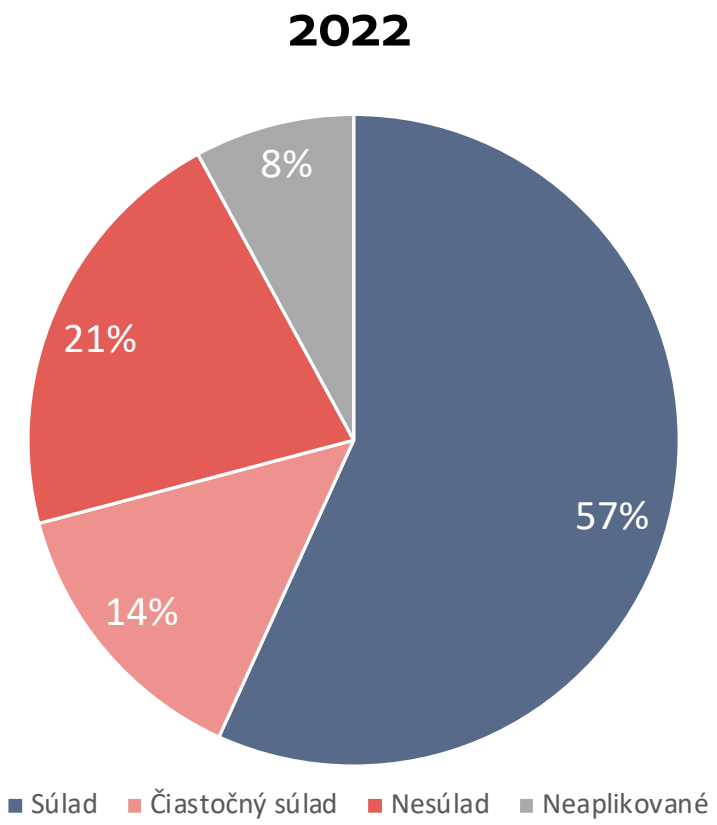
Tomáš Hettych

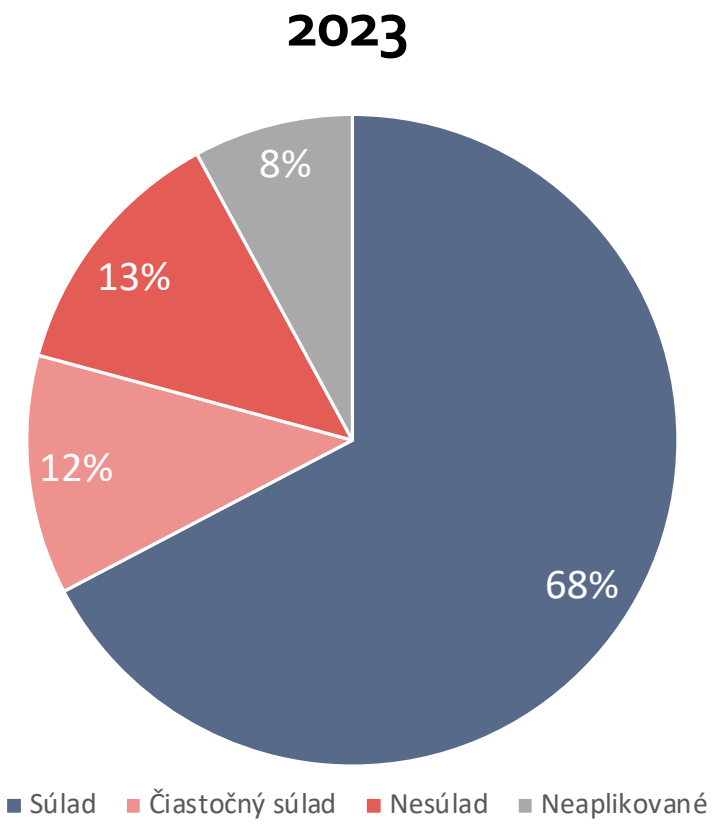
AKTUÁLNY STAV KYBERNETICKEJ BEZPEČNOSTI NA SLOVENSKU

PRAKTICKÉ RADY PRE AUDIT A IMPLEMENTÁCIU POŽIADAVIEK ZÁKONA O KYBERNETICKEJ BEZPEČNOSTI

CELKOVÝ STAV SÚLADU 2021-2023

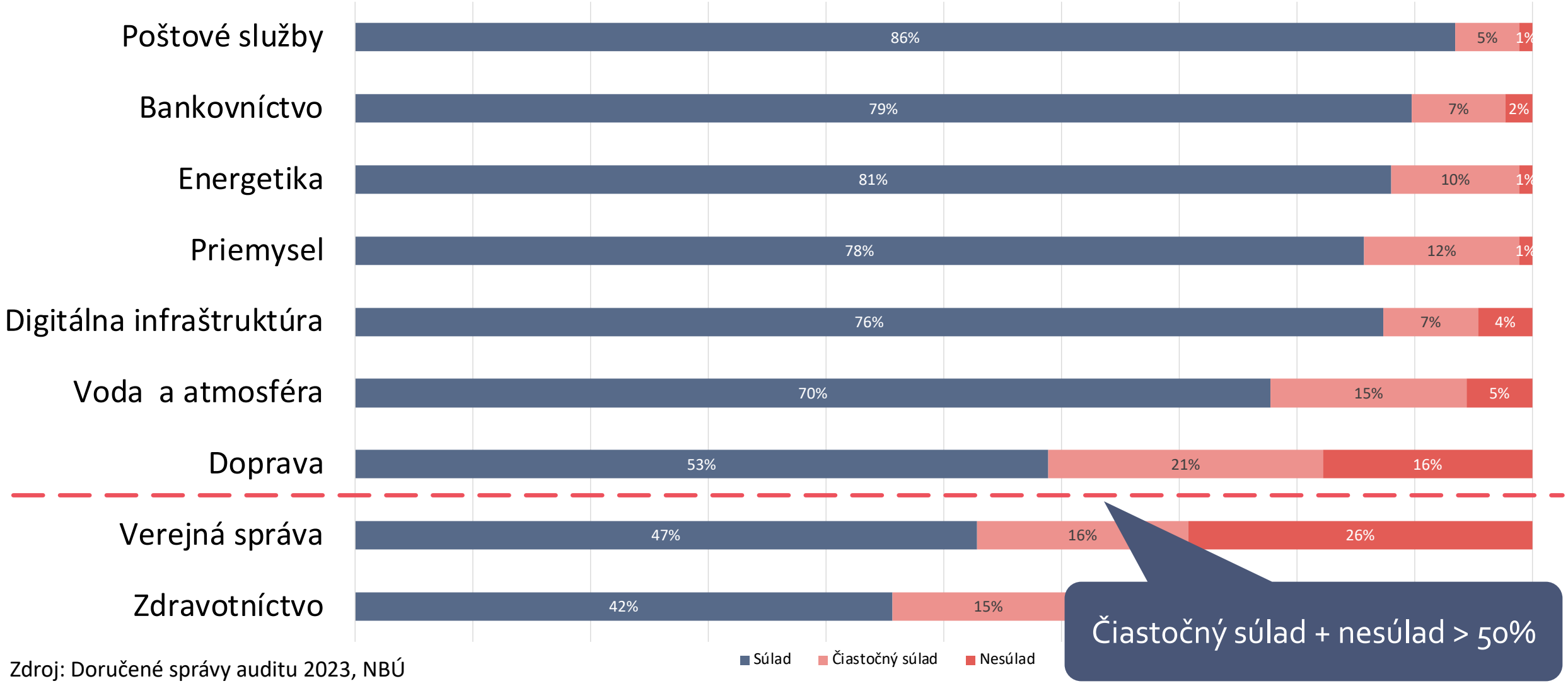






Zdroj: Doručené správy auditu 2021-2023, NBÚ

SÚLAD PODĽA ODVETVÍ 2023



Zdroj: Doručené správy auditu 2023, NBÚ

KOHO SA BUDÚCI ZÁKON TÝKA?

PRAKTICKÉ RADY PRE AUDIT A IMPLEMENTÁCIU POŽIADAVIEK ZÁKONA O KYBERNETICKEJ BEZPEČNOSTI

NOVÉ ROZDELENIE SEKTOROV

Smernica NIS (1)	Zákon č. 69/2018 Z.z.	Smernica NIS2	
		Kľúčové subjekty	Dôležité subjekty
Bankovníctvo	Bankovníctvo	Bankovníctvo	
Dodávka a distribúcia pitnej vody	Dodávka a distribúcia pitnej vody	Dodávka a distribúcia pitnej vody	
Doprava	Doprava	Doprava	
Energetika	Energetika	Energetika	
Infraštruktúra finančných trhov	Infraštruktúra finančných trhov	Infraštruktúra finančných trhov	
Digitálna infraštruktúra	Digitálna infraštruktúra		Poskytovatelia digitálnych služieb
	Elektronické komunikácie		Elektronické komunikácie
	Pošta		Poštové a kuriérske služby
	Priemysel		Priemysel
	Verejná správa	Verejná správa	
	Voda a atmosféra		Voda a atmosféra
	Zdravotníctvo	Zdravotníctvo	
		Odpadová voda	
		Riadenie služieb IKT	
		Vesmír	
			Odpadové hospodárstvo
			Výroba a distribúcia chemických látok
			Výroba iných dopravných prostriedkov
			Výroba elektrických strojov a zariadení
			Výroba motorových vozidiel
			Výroba počítačových elektronických a optických výrobkov
			Výroba, distribúcia a spracovanie potravín
			Výroba zdravotníckych pomôcok
			Výskum

ODHADOVANÝ POČET POVINNÝCH OSÔB PODĽA PRÁVNEJ FORMY

Stredné podniky	2719
Veľké podniky	654
	3373

Zdroj: Malé a stredné podnikanie v číslach v roku 2022, SBA

Štátna správa*	110
Samospráva**	1115
OČTK***	89
Stredné podniky	2719
Veľké podniky	654
	4 687

* **Štátna správa** – ministerstvá, ostatné ústredné orgány, miestna štátna správa
** **Samospráva** – obce nad 1000 obyvateľov, úrady VÚC
*** **OČTK** – prezídium PZSR, okresné riaditeľstvá PZSR, generálna prokuratúra, krajské prokuratúry

AUDIT KYBERNETICKEJ BEZPEČNOSTI

PRAKTICKÉ RADY PRE AUDIT A IMPLEMENTÁCIU POŽIADAVIEK ZÁKONA O KYBERNETICKEJ BEZPEČNOSTI

POŽIADAVKA NA VÝKON AUDITU KYBERNETICKEJ BEZPEČNOSTI

§ 29 Zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti

2) Prevádzkovateľ základnej služby je povinný preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených zákonom vykonaním auditu kybernetickej bezpečnosti

   - po každej zmene majúcej významný vplyv na realizované bezpečnostné opatrenia a
   - v určenom časovom intervale

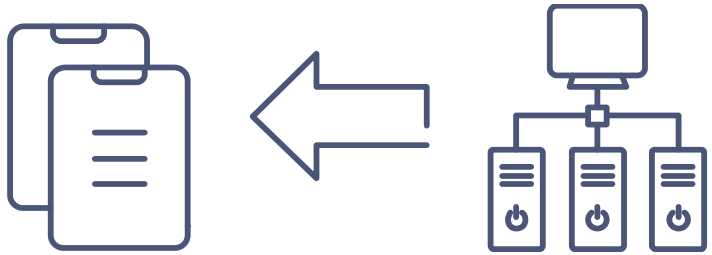
3) Audit kybernetickej bezpečnosti **vykonáva certifikovaný audítor kybernetickej bezpečnosti,** ktorým je fyzická osoba, spoločník, štatutárny orgán alebo zamestnanec právnickej osoby

   - Certifikáciu audítora kybernetickej bezpečnosti vykonáva osoba akreditovaná podľa osobitného predpisu ako orgán certifikujúci osoby v oblasti kybernetickej bezpečnosti

6) Úrad **môže kedykoľvek vykonať audit kybernetickej bezpečnosti** u PZS alebo požiadať certifikovaného audítora kybernetickej bezpečnosti, aby vykonal takýto audit u PZS s cieľom potvrdiť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených zákonom

AUDIT BEZPEČNOSTI

Systematický, nezávislý a zdokumentovaný proces získavania záznamov, konštatovaní faktov alebo iných dôležitých informácií a ich objektívneho posudzovania s cieľom určiť rozsah, v akom sa splnili určené požiadavky



Typické metódy:

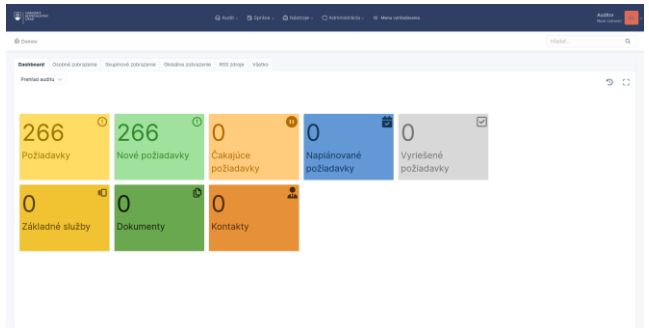
- Auditné rozhovory a dotazníky
- Porovnávanie deklarovaného a skutkového stavu
- Preskúmanie zdokumentovaných informácií
- Vzorkovanie (vykonáva sa, ak nie je praktické alebo efektívne preverenie všetkých dostupných informácií v priebehu auditu)

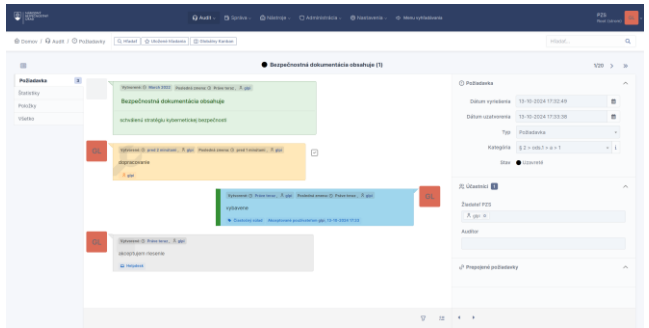
Primárny účel:

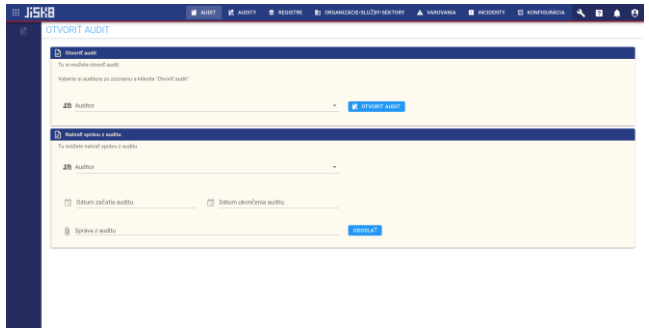
- Získanie informácie o nezhodách a rizikách formou konsolidovanej správy
- Iniciácia návrhov na zmenu jestvujúcich resp. Implementáciu ďalších bezpečnostných opatrení

Pre audit je typická požiadavka na nestrannosť

AUDIT VS. SAMOHODNOTENIE







- Samohodnotenie bolo do 31.12.2023 možné len na základe zákonnej výnimky
- Podľa novelizovaného znenia Zákona:
  - Prevádzkovateľ základnej služby, **ktorý nie je prevádzkovateľom kritickej základnej služby**, môže zabezpečiť plnenie povinnosti vykonať audit kybernetickej bezpečnosti vykonaním samohodnotenia prostredníctvom jednotného informačného systému kybernetickej bezpečnosti – **JISKB**
  - Samohodnotenie vykonáva **manažér kybernetickej bezpečnosti**
  - Takýto prevádzkovateľ základnej služby je povinný podrobiť sa auditu kybernetickej bezpečnosti **do piatich rokov** odo dňa zaradenia do registra prevádzkovateľov základnej služby

NAJČASTEJŠIE RIZIKÁ A NÁLEZY AUDITU

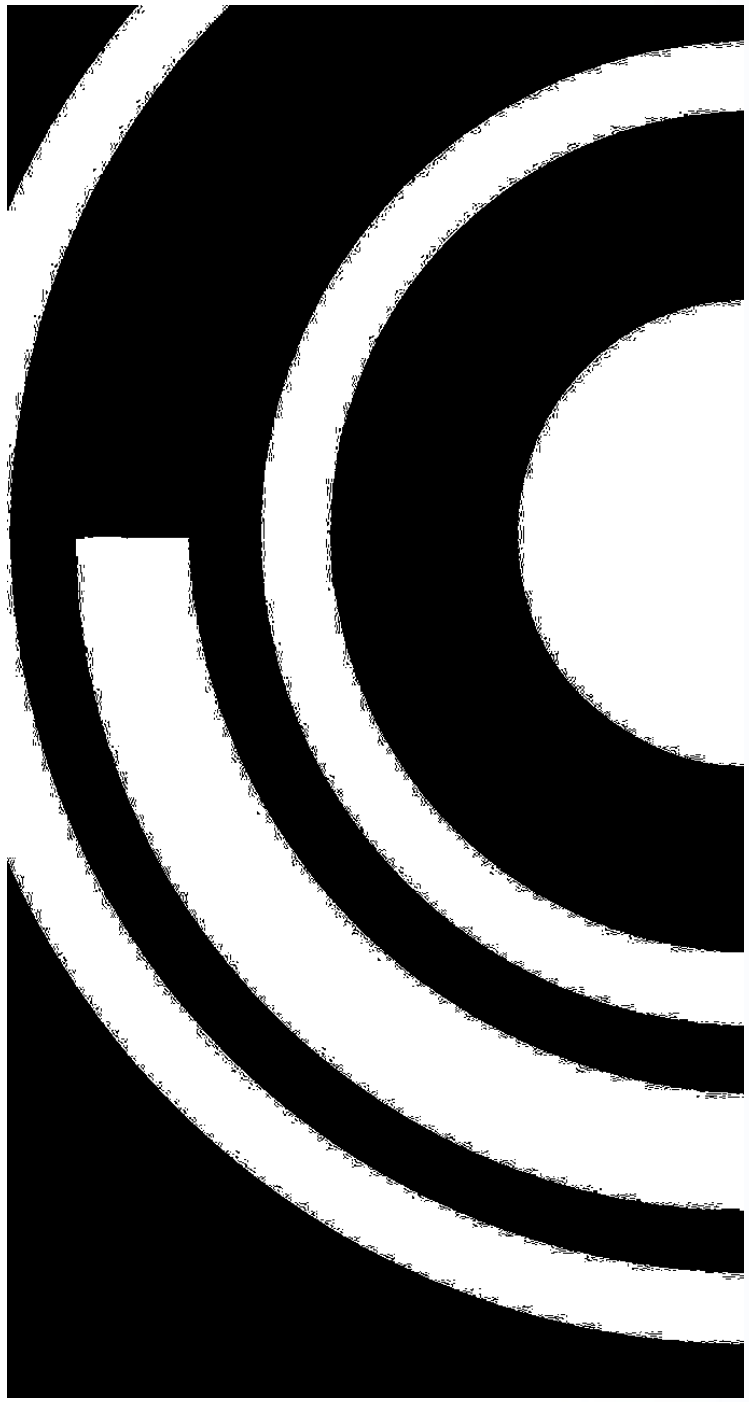
Riadenie bezpečnosti (Security governance):

- Nedostatočná podpora vedenia ústavu
- Nie je definovaná štruktúra riadenia, výkonu a kontroly v oblasti kybernetickej bezpečnosti
- Zodpovednosť za identifikáciu a evidenciu aktív, hrozieb a rizík
- Neexistencia analýzy rizík a analýzy dopadov
- Nedostatočná, alebo stále chýbajúca bezpečnostná dokumentácia
- Nezávislosť riadenia bezpečnosti od riadenia IT
- Vzdelávanie v oblasti informačnej bezpečnosti
- Neformálne riadenie prevádzky

Výkon bezpečnosti (Security operations):

- Chýbajúci bezpečnostný monitoring
- Nesystematické riešenie incidentov
- Vzdialený prístup do interných sietí a IS nie je zabezpečený
- Chýbajúca topológia, segmentácia, zoznamy portov
- Neexistencia procesov riadenia kontinuity činností
- Nejasné a neformálne postupy zálohovania a obnovy
- PZS nedostatočne rieši šifrovú ochranu informácií

Spolufinancovaný Európskou úniou

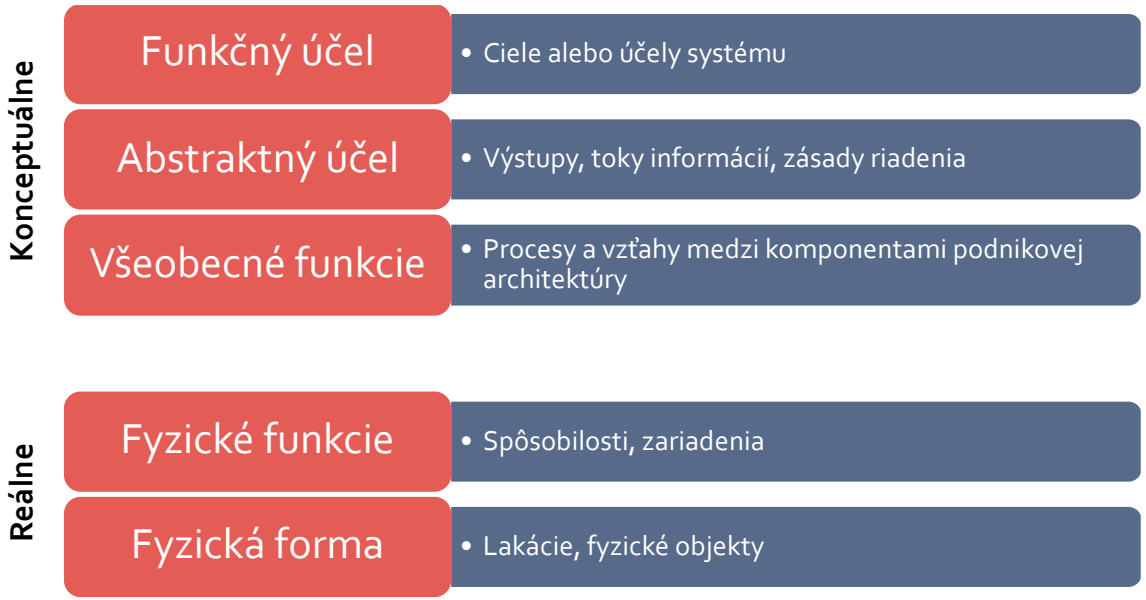


IMPLEMENTÁCIA POŽIADAVIEK

PRAKTICKÉ RADY PRE AUDIT A IMPLEMENTÁCIU POŽIADAVIEK ZÁKONA O KYBERNETICKEJ BEZPEČNOSTI

KDE ZAČAŤ S IMPLEMENTÁCIOU? (1/2)

1. Identifikujte svoje informačné aktíva:



2. Vykonajte Analýzu rizík:

KDE ZAČAŤ S IMPLEMENTÁCIOU? (2/2)

3. Vykonajte Analýzu dopadov (BIA – Business Impact Analysis)
4. Z analýzy rizík identifikujte najväčšie riziká, ktoré budú zároveň scenármi pre riadenie kontinuity
   - Zároveň máte identifikované kritické informačné aktíva
   - Viete, čo je pre vás viac a čo menej dôležité
   - Máte prioritizované opatrenia
5. Pripravte si:
   - Postupy pre riešenie a nahlasovanie incidentov
   - Plány kontinuity (BCP - Business Continuity Plan)
   - Plány obnovy (DRP - Disaster Recovery Plan)
6. Zapojte do procesov najvyššie vedenie organizácie
7. Všetko zdokumentujte v interných smerniciach, aby teória a reálna aplikačná prax boli v súlade
8. Buďte otvorení a transparentní pri príprave podkladov (audítor to aj tak zistí… ☺)

AKO SA PRIPRAVIŤ NA AUDIT KYBERNETICKEJ BEZPEČNOSTI?

- Snažte sa zaviesť v organizácii konsolidovaný proces riadenia rizík
- Ak nie je možné zaviesť štandardný proces riadenia rizík, požiadajte o vykonanie analýzy rizík kvalifikovaného manažéra kybernetickej bezpečnosti
- Výstupy analýzy rizík majú slúžiť vedeniu organizácie na určenie priorít implementácie opatrení
- Interný audit (ak je táto funkcia zriadená) môže vykonať vlastné posúdenie podľa metodiky auditu kybernetickej bezpečnosti
- Zistenia interného auditu by mali poslúžiť ako nezávislý návod na prioritizáciu opatrení
- Pokiaľ funkcia interného auditu nie je zriadená, požiadajte o vykonanie posúdenia stavu kybernetickej bezpečnosti kvalifikovaného manažéra kybernetickej bezpečnosti
- Implementujte primerané opatrenia podľa navrhnutých priorít
- Vykonajte samohodnotenie podľa Zákona, alebo objednajte certifikovaného audítora kybernetickej bezpečnosti na vykonanie auditu Do 30 dní odošlite záverečnú správu auditu na NBÚ
- Vzdelávajte sa, vzdelávajte zamestnancov, dbajte o zvyšovanie bezpečnostného povedomia!

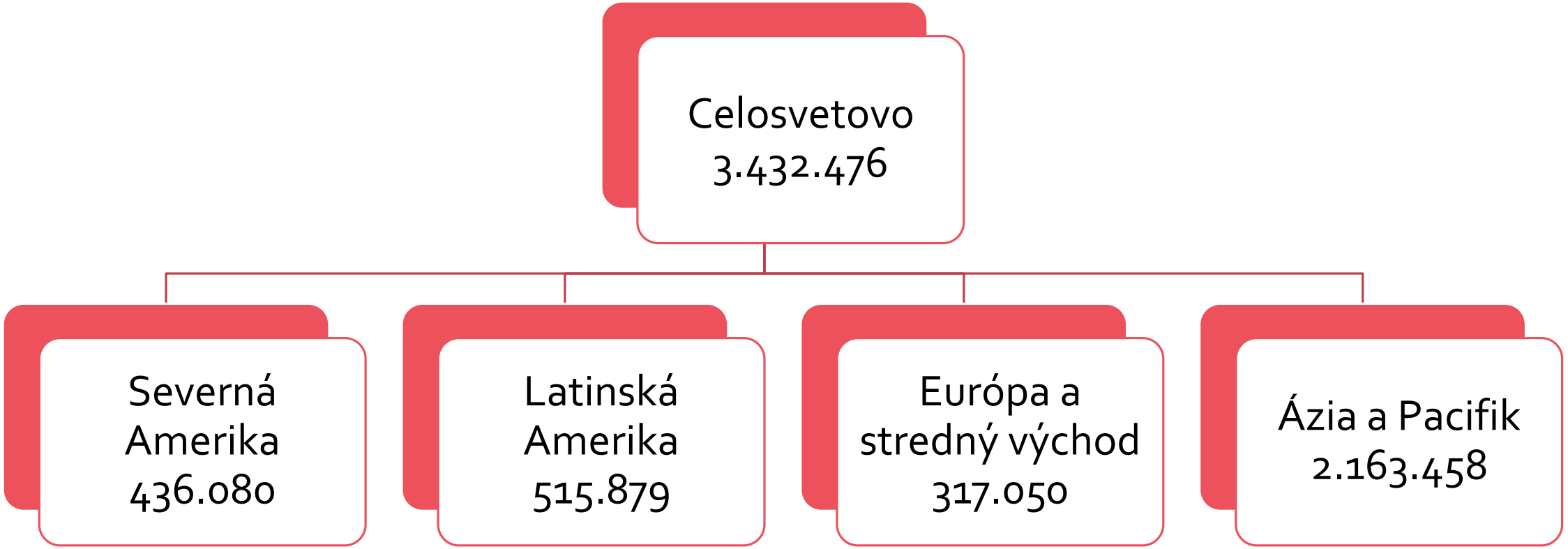
AUDIT NIE JE SANKČNÝ MECHANIZMUS!

ĽUDSKÉ ZDROJE PRE KYBERNETICKÚ BEZPEČNOSŤ

PRAKTICKÉ RADY PRE AUDIT A IMPLEMENTÁCIU POŽIADAVIEK ZÁKONA O KYBERNETICKEJ BEZPEČNOSTI

CELKOVÝ ODHAD POŽIADAVIEK PRACOVNÉHO TRHU

Ročný nárast: **26,2%**



Zdroj: *(ISC)2 Cybersecurity workforce study*

POŽIADAVKY SLOVENSKÉHO PRACOVNÉHO TRHU

Rola / Kategória subjektu	PZS	Stredné podniky	Verejná správa	OVM	OČTK	Vysoké školy
1.Manažér kybernetickej bezpečnosti	1	1	1	1	1	
2.Špecialista pre vyšetrovanie KBI	1		1	10	200	
3.Špecialista pre riadenie súladu	1		1	1	1	
4.Špecialista pre riešenie KBI	1			10	10	
5.Architekt kybernetickej bezpečnosti	1		1	2		
6.Audítor kybernetickej bezpečnosti				100		
7.Lektor kybernetickej bezpečnosti				50		
8.Špecialista kybernetickej bezpečnosti	2			10		
9.Výskumník kybernetickej bezpečnosti				10		20
10.Špecialista pre riadenie rizík	1		1	1	1	
11.Špecialista pre analýzu digitálnych stôp			2	10	200	
12.Tester kybernetickej bezpečnosti			1	5		
TYPOVÝ POČET RÔL V KB	8	1	8	210	413	20
POČET SUBJEKTOV	1 600	2 688	300	2	2	5
Odhadovaná potreba FTE podľa subjektov	**12 800**	**2 688**	**2 400**	**420**	**826**	**100**

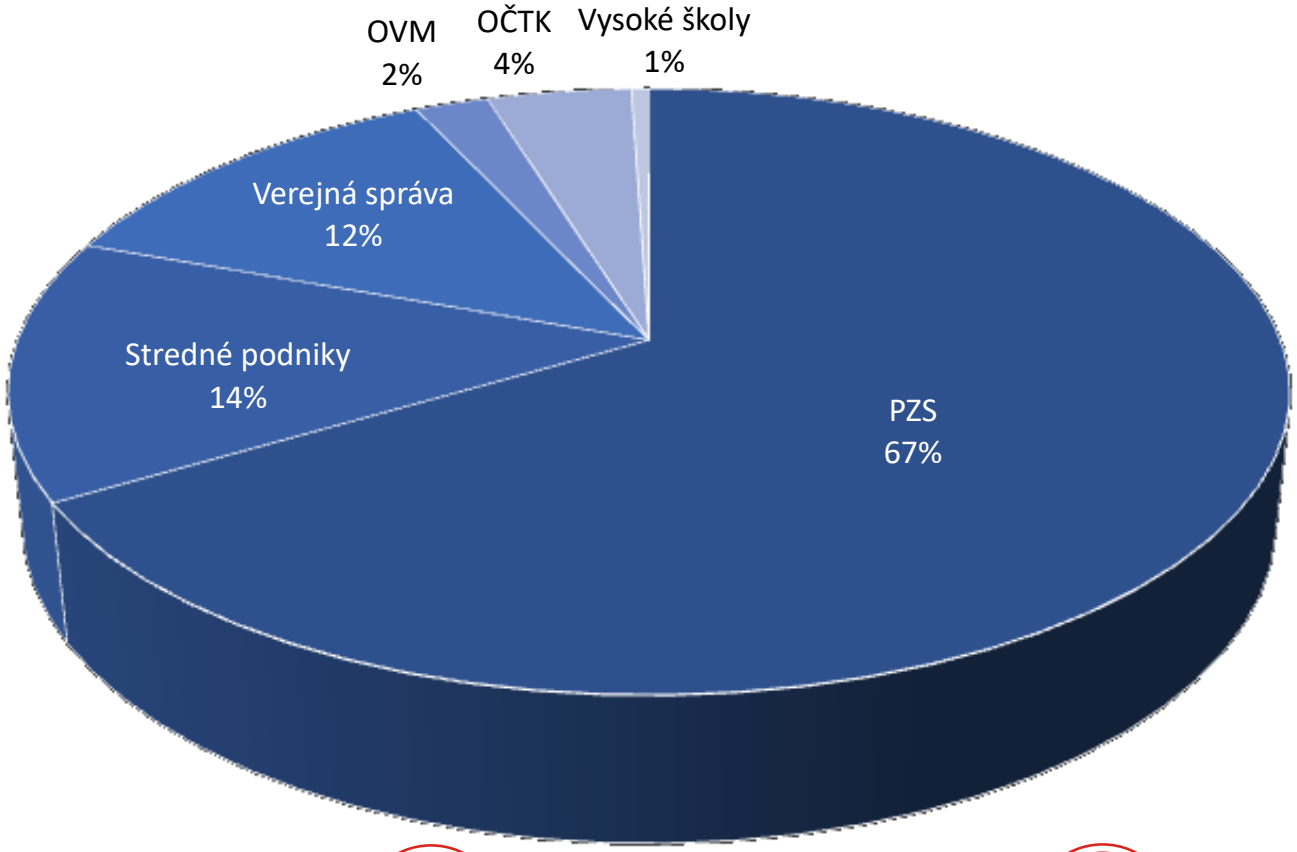
Analyzované subjekty:

- Prevádzkovatelia základných služieb (vrátane veľkých podnikov)
- Stredné podniky
- Verejná správa (ústredné orgány a samospráva)
- Orgány verejnej moci (regulátori: NBÚ / MIRRI)
- Orgány činné v trestnom konaní
- Relevantné vysoké školy

ODHAD POŽIADAVIEK PRACOVNÉHO TRHU

Rola / Kategória subjektu	PZS	Stredné podniky	Verejná správa	OVM	OČTK	Vysoké školy
1.Manažér kybernetickej bezpečnosti	1	1	1	1	1	
2.Špecialista pre vyšetrovanie KBI	1		1	10	200	
3.Špecialista pre riadenie súladu	1		1	1	1	
4.Špecialista pre riešenie KBI	1			10	10	
5.Architekt kybernetickej bezpečnosti	1		1	2		
6.Audítor kybernetickej bezpečnosti				100		
7.Lektor kybernetickej bezpečnosti				50		
8.Špecialista kybernetickej bezpečnosti	2			10		
9.Výskumník kybernetickej bezpečnosti				10		20
10.Špecialista pre riadenie rizík	1		1	1	1	
11.Špecialista pre analýzu digitálnych stôp			2	10	200	
12.Tester kybernetickej bezpečnosti			1	5		
TYPOVÝ POČET RÔL V KB	8	1	8	210	413	20
POČET SUBJEKTOV	1 600	2 688	300	2	2	5
Odhadovaná potreba FTE podľa subjektov	**12 800**	**2 688**	**2 400**	**420**	**826**	**100**

19 234 FTE!



Manažér KB (ako zákonná povinnosť) – 1600

Manažér KB (nepovinne) – 2992

Počet zamestnancov KB u PZS – 12 800

ZÁKONNÉ ROLY V KYBERNETICKEJ BEZPEČNOSTI

Manažér kybernetickej bezpečnosti

Podľa §20 ods. 4 písm. a) Zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti:

- bezpečnostné opatrenia musia zahŕňať najmenej **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

Audítor kybernetickej bezpečnosti

Podľa §29 ods. 3 Zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti:

- Audit kybernetickej bezpečnosti vykonáva **certifikovaný audítor kybernetickej bezpečnosti,** ktorým je fyzická osoba, spoločník, štatutárny orgán alebo zamestnanec právnickej osoby
- Certifikáciu audítora kybernetickej bezpečnosti vykonáva **osoba akreditovaná podľa osobitného predpisu** ako orgán certifikujúci osoby (v oblasti kybernetickej bezpečnosti)

EURÓPSKY VS. SLOVENSKÝ RÁMEC ROLÍ V KB

1. Manažér kybernetickej bezpečnosti
2. Špecialista pre vyšetrovanie kybernetických bezpečnostných incidentov
3. Špecialista pre riadenie súladu
4. Špecialista pre riešenie kybernetických bezpečnostných incidentov
5. Architekt kybernetickej bezpečnosti
6. Audítor kybernetickej bezpečnosti
7. Lektor kybernetickej bezpečnosti
8. Špecialista kybernetickej bezpečnosti
9. Výskumník kybernetickej bezpečnosti
10. Špecialista pre riadenie rizík
11. Špecialista pre analýzu digitálnych stôp
12. Tester kybernetickej bezpečnosti

Zdroj: Vyhláška NBÚ č. 492/2022 o znalostných štandardoch v KB

KTO JE MANAŽÉR KYBERNETICKEJ BEZPEČNOSTI?

- MKB/CISO je pracovná rola, nie len pozícia
  - nemusí byť jedinou rolou zamestnanca
  - rolu môže plniť viacero osôb (zastupiteľnosť)
  - a naopak – rola môže byť zdieľaná medzi viacerými zákazníkmi (outsourcing)
- SR je prvým ČŠ EÚ, ktorý má požiadavky na znalosti a zručnosti v KB stanovené právnym predpisom:
  - Vyhláška Národného bezpečnostného úradu č. 492/2022 Z. z. ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti

Zdroj: Vyhláška NBÚ č. 492/2022 o znalostných štandardoch v KB

KTO JE CERTIFIKOVANÝ AUDÍTOR?

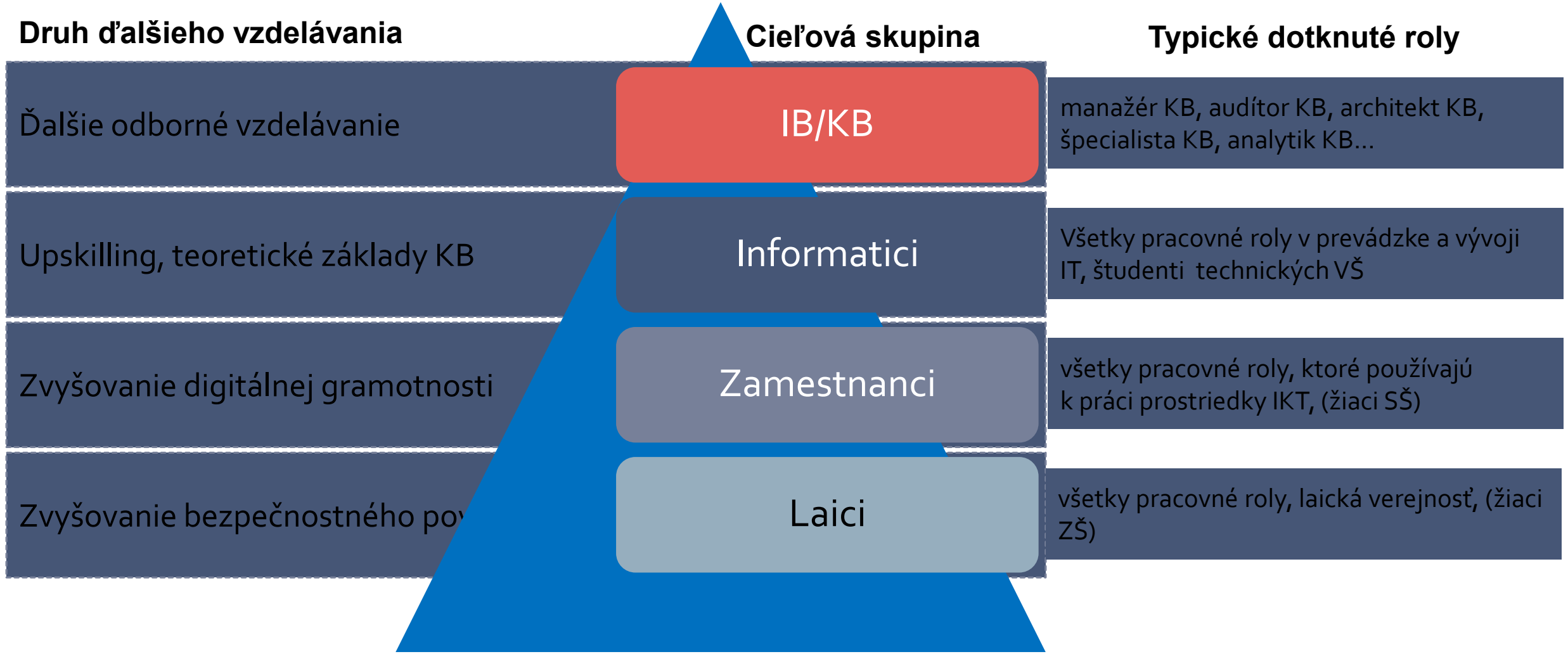
- Podľa §29 ods. 3 Zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti:
  - Audit kybernetickej bezpečnosti vykonáva **certifikovaný audítor kybernetickej bezpečnosti,** ktorým je fyzická osoba, spoločník, štatutárny orgán alebo zamestnanec právnickej osoby
  - Certifikáciu audítora kybernetickej bezpečnosti vykonáva **subjekt akreditovaný podľa osobitného predpisu** ako orgán certifikujúci osoby (v oblasti kybernetickej bezpečnosti)
- Aké predpoklady musí certifikovaný audítor splniť?
  - Spĺňa minimálne požiadavky na úroveň vzdelania a prax (10-7-5 rokov praxe v IT, 7-5-3 rokov praxe v audite)
  - Disponuje medzinárodným IT alebo security auditným certifikátom (CISA, ISO27001 Lead Audítor, ISO20000 Audítor)
  - Má dokladovateľné auditné skúsenosti (aj z iných auditných rámcov)
  - Úspešne absolvoval certifikačnú skúšku
- Podrobnosti nájdete v Certifikačnej schéme overovania odbornej spôsobilosti audítora (na webe NBÚ)

Aktuálny počet certifikovaných audítorov KB: 85

MOŽNÉ RIEŠENIA NEDOSTATKU ODBORNÍKOV NA KB

PRAKTICKÉ RADY PRE AUDIT A IMPLEMENTÁCIU POŽIADAVIEK ZÁKONA O KYBERNETICKEJ BEZPEČNOSTI

CIEĽOVÉ SKUPINY VZDELÁVANIA V KB



Zdroj: NIST Special Publication 800-16: Information Technology Security Training Requirements

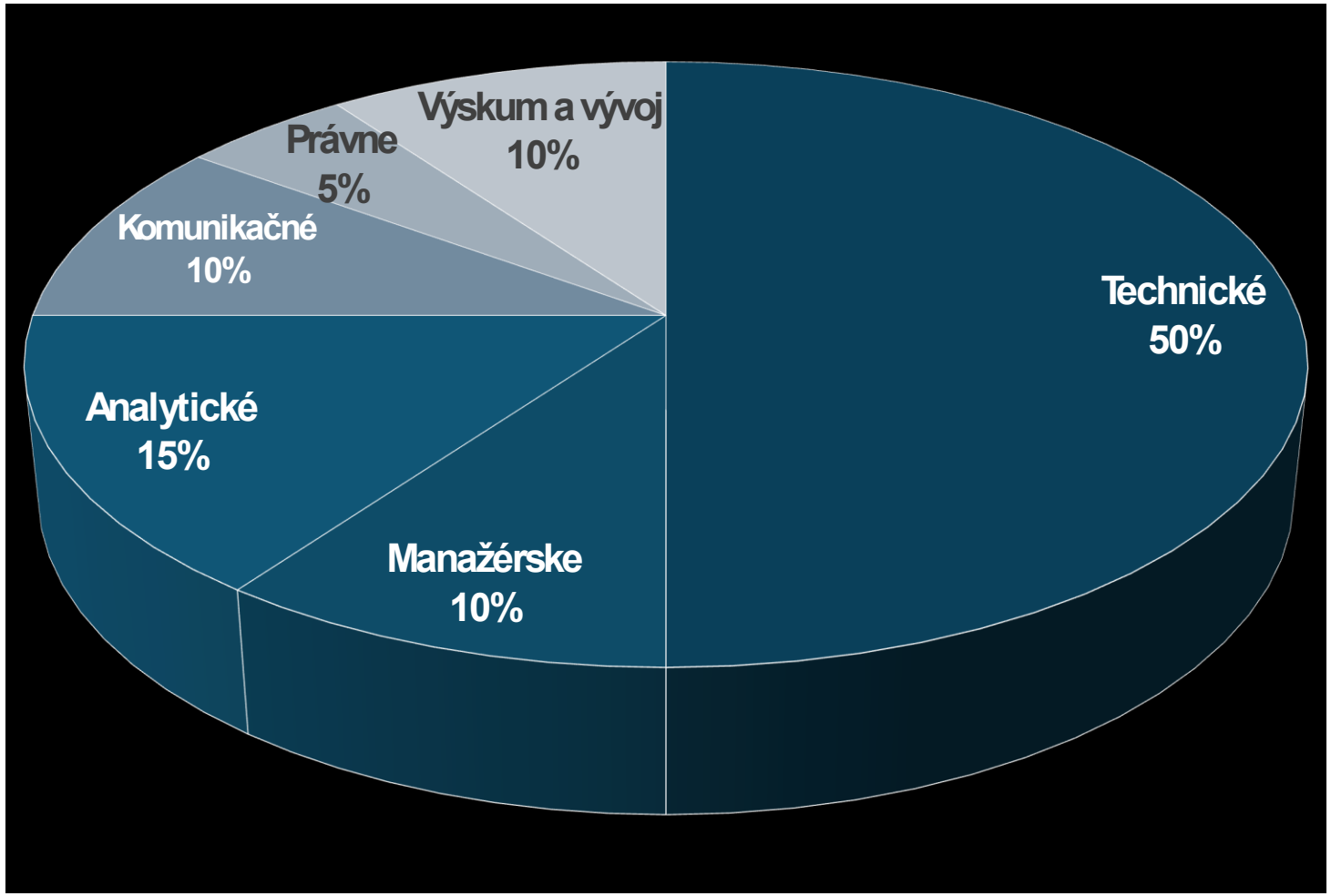
Spolufinancovaný Európskou úniou

DISTRIBÚCIA POŽIADAVIEK NA KVALIFIKÁCIE

Inšpirácia pre kvalifikačný rámec rolí:
National Initiative for Cybersecurity Education (NICE)

Komponenty rámca:

- **Kategórie** – Vysokoúrovňové skupiny kvalifikačných komponentov
- **Skupiny kompetencií** – Odlišné oblasti pracovnej špecializácie
- **Pracovné roly** – množiny špecifických znalostí, zručností a schopností potrebných na vykonávanie činností v konkrétnej pracovnej úlohe



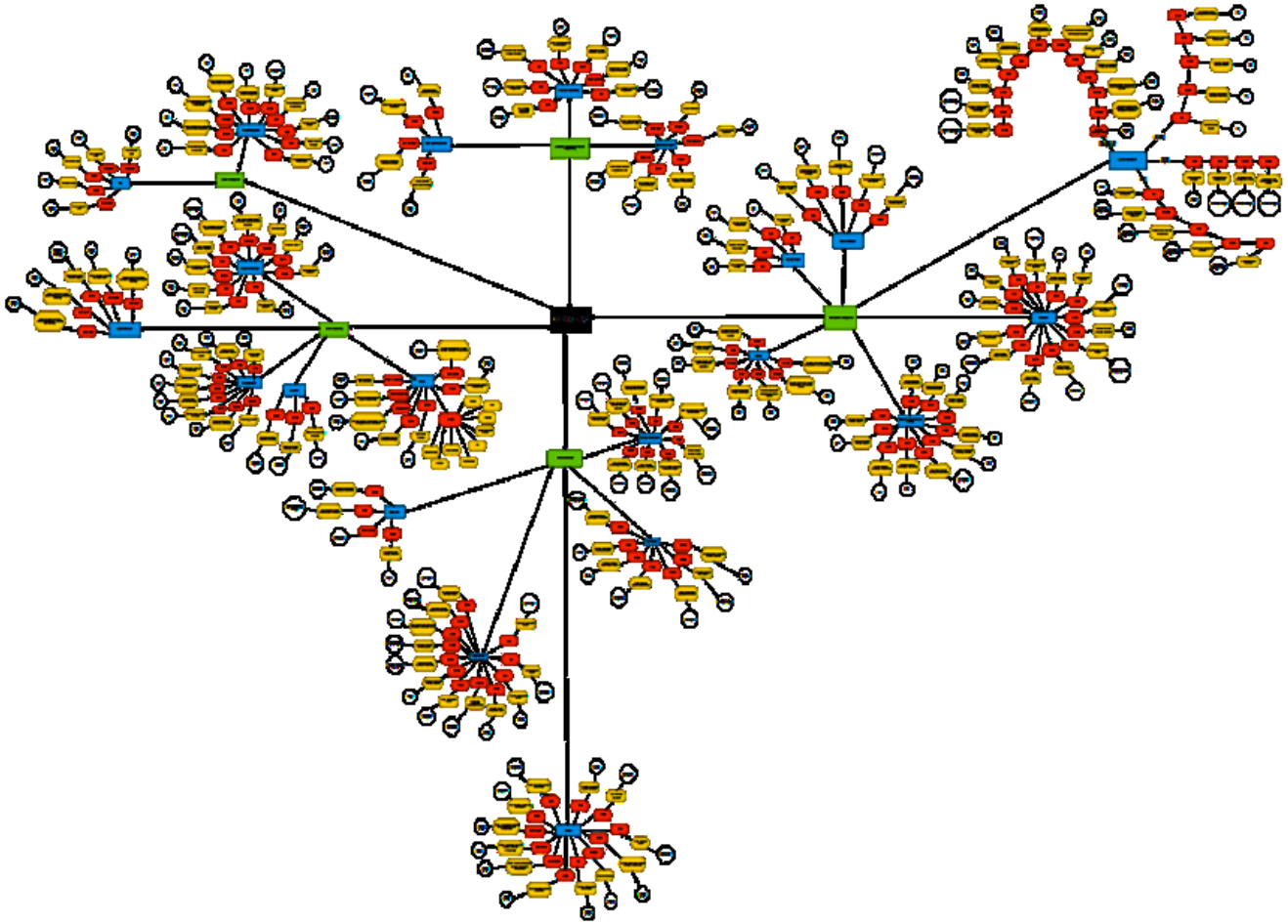
UPSKILLING

Zvyšovanie zručností (upskilling):

- Trend, ktorý uľahčuje ďalšie vzdelávanie poskytovaním školiacich programov a príležitostí na rozvoj, ktoré rozširujú schopnosti zamestnancov a minimalizujú nedostatky v zručnostiach
- Zvyšovanie zručností sa zameriava na **zlepšovanie zručností súčasných profesionálov**
- **Zvyčajné metódy**: školenia a tréningy vo forme ďalšieho vzdelávania
- **Cieľ**:
  - napredovanie v práci
  - nájdenie nových príležitostí v rámci organizácie
  - zvýšenie disponibilnej kapacity ľudských zdrojov v konkrétnych profesiách a roliach
- Upskilling je možné formálne **ukončiť certifikačnou skúškou a potvrdiť certifikátom**

POUŽITEĽNOSŤ CERTIFIKÁTOV OSÔB

- Na základe vyžiadania relevantných certifikátov môžu štatutári rozhodnúť o existencii primeraných záruk spôsobilosti uchádzača
- Kybernetická bezpečnosť sa už špecializuje a postupne sa delí na mnohé subdomény
- Vznikajú rôzne odbornosti a tým aj rôzne certifikácie
- Ako sa v tom vyznať?
  - Pochopiť princíp certifikácií
  - Rozhodnúť, aký predmet certifikácie hľadá
  - Vyberať cielene vlastníctvo certifikátov poc požadovanej špecializácie
  - Opierať sa najmä o akreditované certifikač



Spolufinancovaný Európskou úniou

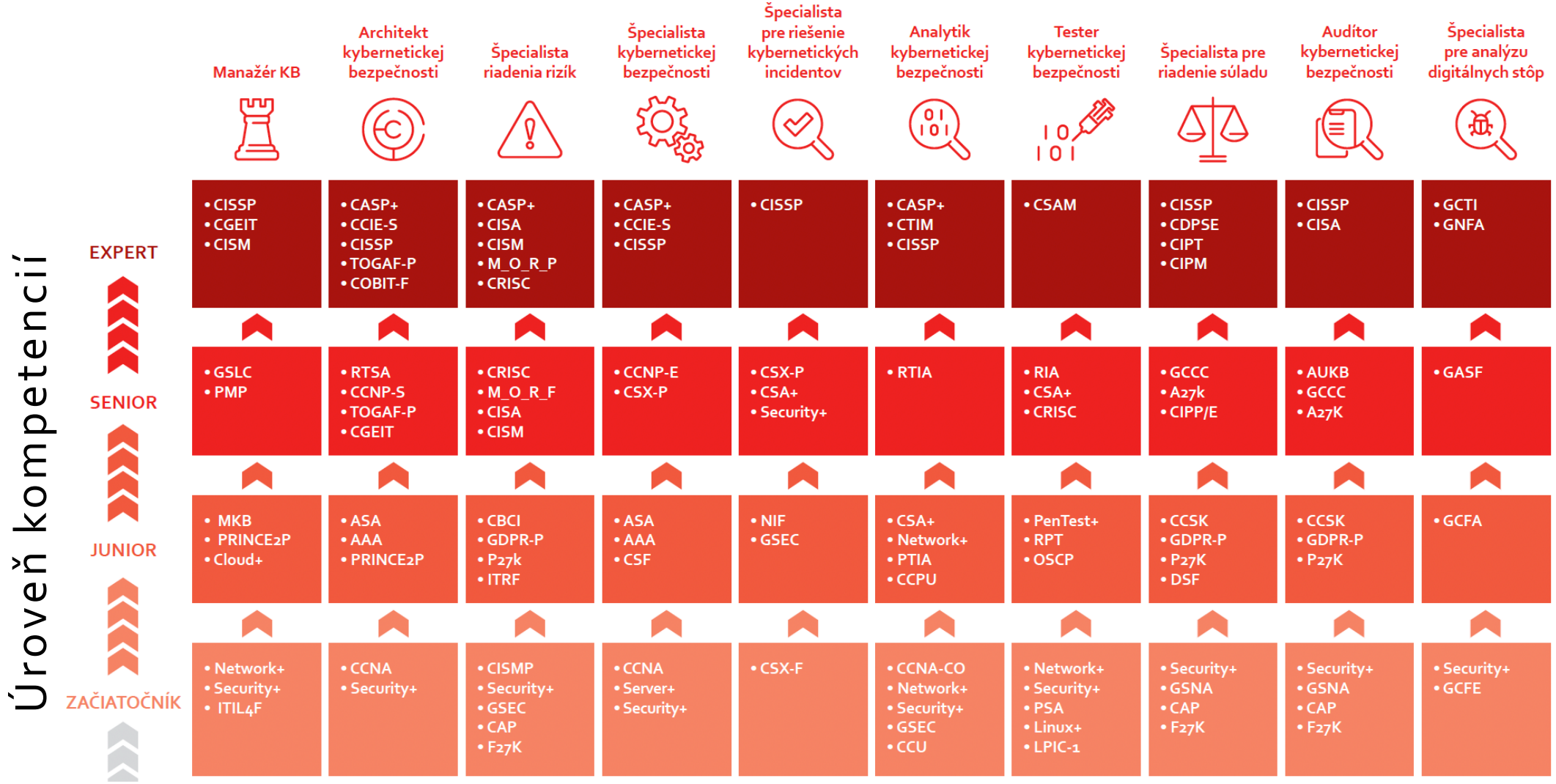
CERTIFIKÁCIA OSÔB

- Ako potvrdiť získané vedomosti a zručnosti?
  - Vysokoškolské vzdelávanie je po absolvovaní štúdia formálne **ukončené štátnou skúškou a potvrdené vysokoškolským diplomom**
  - Ďalšie vzdelávanie (upskilling) je možné formálne **ukončiť certifikačnou skúškou a potvrdiť certifikátom**
- Certifikácia je zásadne dobrovoľná
- Existujú dve kategórie certifikátov:
  - **Komerčné certifikáty vydávané v neakreditovanom režime** poskytované medzinárodnými organizáciami, patria medzi uznávané v oblasti kybernetickej bezpečnosti (Typicky napríklad certifikáty od ISACA, ISC2, CompTIA, GIAC, SANS, a ďalšie)
  - **Certifikáty od akreditovaných vzdelávacích inštitúcií** môžu ich poskytovať výhradne tie vzdelávacie inštitúcie, ktoré prešli atestáciou spôsobilosti vykonávať posudzovanie kompetencií osôb

Certifikovaný audítor
Ev. č. 001/O-024
cybercompetence.sk

Spolufinancovaný Európskou úniou

UZNANÉ KOMERČNÉ (NEAKREDITOVANÉ) CERTIFIKÁTY



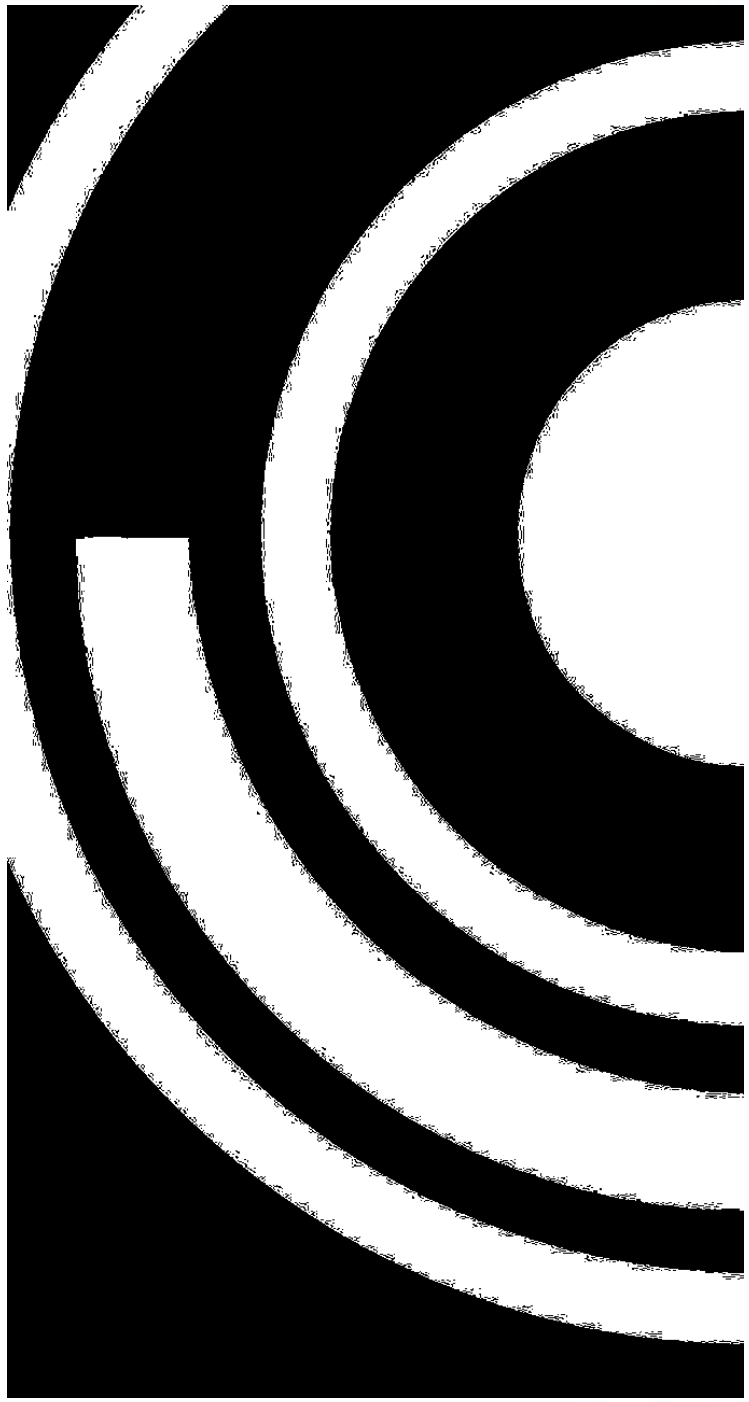
Spolufinancovaný Európskou úniou

ZOZNAM KOMERČNÝCH CERTIFIKÁTOV

Skratka	Názov	Vydavateľ
AUKB	Audítor kybernetickej bezpečnosti	KCCKB
MKB	Manažér kybernetickej bezpečnosti	
CISA	Certified Information Systems Auditor	ISACA
CISM	Certified Information Systems Manager	
CRISC	Certified in Risk and Information Systems Control	
CDPSE	Certified Data Privacy Security Engineer	
CSX-F	CyberSecurity Fundamentals	
CSX-P	Cybersecurity Practitioner	
COBIT-F	COBIT 5 Foundation	
CGEIT	Certified in the Governance of Enterprise IT	
NIF	Network & Infrastructure Fundamentals	ISAC – ITCA
DSF	Data Science Fundamentals	
CCU	Core Certified User	SPLUNK
CCPU	Core Certified Power User	
CISSP	Certified Information Systems Security Professional	(ISC)2
CAP	Certified Authorization Professional	
CASP+	Advanced Security Practitioner	CompTIA
CSA+	Cyber Security Analyst	
Security+	Security+	
Pentest+	Pentest+	
Cloud+	Cloud+	
Network+	Network+	
Server+	Server+	
Linux+	Linux+	
OSCP	Certified Professional	OFFENSIVE SECURITY
GCFE	Certified Forensic Examiner	GIAC
GASF	Advanced Smartphone Forensics	
GSLC	Security Leadership	
GCCC	Critical Controls Certification	
GSEC	Security Essentials Certification	
GSNA	Systems and Network Auditor	
GCFA	Certified Forensic Analyst	
GCTI	Cyber Threat Intelligence	
GNFA	Network Forensic Analyst	

Skratka	Názov	Vydavateľ
F27K	ISO/IEC 27001 Foundation	ISO
A27K	ISO/IEC 27001 Auditor	
P27K	ISO/IEC 27001 Practitioner	
CISMP	Certificate in Information Security Management Principles	BCS
GDPR-P	GDPR Practitioner	QA
CBCI	Certificate of the Business Continuity Institute	BCI
AAA	Azure Administrator Associate	MS
ASA	Associate Solutions Architect	AWS
ITIL4F	ITIL4® Foundation	AXELOS
PRINCE2F	PRINCE2® Foundation	
PRINCE2P	PRINCE2® Practitioner	
M_O_R_F	MoR® Foundation	
CTIM	Certified Threat Intelligence Manager	CREST
RTIA	Registered Threat Intelligence Analyst	
PTIA	Practitioner Threat Intelligence Analyst	
CSAM	Certified Simulated Attack Manager	
RIA	Registered Intrusion Analyst	
RPT	Registered Penetration Tester	
CCIE-S	Certified Internetwork Expert Security	CISCO
CCNP-S	Certified Network Professional Security	
CCNP-E	Certified Network Professional Enterprise	
CCNA	Certified Network Associate	
CCNA-CO	Certified Cyber Operations	
TOGAF-P	TOGAF Practitioner	THE OPEN GROUP
TOGAF-F	TOGAF Foundation	
LPIC-1	Linux Professional Infrastructure Certification	LPI
CCSK	Cloud Security Knowledge	CLOUDSEC ALLIANCE
PMI PMP	Project Management Professional	PMI
CIPT	Certified Information Privacy Technologists	IAPP
CIPM	Certified Information Privacy Manager	
CIPP/E	Certified Information Privacy Professional/Europe	

Spolufinancovaný Európskou úniou



ZÁVER

PRAKTICKÉ RADY PRE AUDIT A IMPLEMENTÁCIU POŽIADAVIEK ZÁKONA O KYBERNETICKEJ BEZPEČNOSTI

ZHRNUTIE

- Stav kyberbezpečnosti v SR u regulovaných subjektov od roku 2021 vykazuje postupné medziročné zlepšenie z **42% -> 57% -> 68%**
- Vyšší počet povinných osôb – PZS (**1 500 -> cca 5 000**)
- Nebojte sa auditu – je to jediný dostupný spôsob, ako sa od nezávislej a odborne spôsobilej osoby dozviete o vašich reálnych potrebách vy kybernetickej bezpečnosti
- Ak ste oprávnení vykonať posúdenie samohodnotením, neodkladajte ho
- Pripravte sa na audit resp. samohodnotenie
- Pre efektívne zvýšenie počtu spôsobilých profesionálov v kyberbezpečnosti je možné použiť metódu upskillingu
- Zvýši sa tlak na školy a vzdelávacie inštitúcie s cieľom naplniť požiadavky pracovného trhu
- Nedajte sa oklamať samozvanými odborníkmi! (Existuje Metodika posúdenia kvalifikácie MKB)

Spolufinancovaný Európskou úniou

Limity informácií

Informácie obsiahnuté v tomto dokumente sú poskytované iba na informačné účely a bez akejkoľvek záruky, výslovnej či implicitnej. Názov KCCKB, logo KCCKB a ďalšie produkty a služby KCCKB sú ochrannými známkami KCCKB. Ostatné názvy spoločností, produktov alebo služieb môžu byť ochrannými známkami, alebo značkami služieb iných organizácií.

Vyjadrené názory a postoje sú názormi a vyhláseniami autorov a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za nich nepreberajú žiadnu zodpovednosť.

Ochrana vlastníckych práv

Vlastnícke práva tretích strán

Všetky ochranné známky a iné obdobné právne chránené označenia spomenuté v tomto dokumente sú výhradným vlastníctvom ich vlastníkov, ktorí sú, pokiaľ sa nejedná o KCCKB, v dokumente označení vo forme príslušnej citácie.

Akékoľvek kopírovanie či iné neoprávnené použitie celého dokumentu alebo jeho časti, v elektronickej alebo listinnej podobe, bez predchádzajúceho písomného súhlasu jeho autorov, napr. KCCKB, je zakázané. Porušenie vlastníckych a iných súvisiacich práv bude riešené v zmysle právnych predpisov Slovenskej republiky.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

10 MANAŽÉRSKYCH CHÝB, KTORÉ VEDÚ K INCIDENTU

PRAKTICKÉ RADY PRE AUDIT A IMPLEMENTÁCIU POŽIADAVIEK ZÁKONA O KYBERNETICKEJ BEZPEČNOSTI

10 MANAŽÉRSKYCH CHÝB, KTORÉ VEDÚ K INCIDENTU

1 CHÝBAJÚCE, ALEBO FORMÁLNE RIADENIE RIZÍK

Neochota zaviesť štandardizované, konsolidované a udržateľné riadenie kybernetických rizík môže viesť k podceňovaniu reálnych hrozieb, čím sa organizácia stáva zraniteľnejšou voči kybernetickým incidentom.

Je potrebné implementovať a udržiavať riadenie rizík, ako bežnú súčasť všetkých procesov.

2 BEZPEČNOSŤ IZOLOVANÁ OD PREVÁDZKY

Organizačná štruktúra, v ktorej prevádzkové procesy a kybernetická bezpečnosť nie sú vzájomne prepojené, vedie k nesúladom a potenciálnym zlyhaniam v ochrane informačných aktív.

Spolupráca prevádzky a kyberbezpečnosti je nevyhnutná pre efektívnu ochranu organizácie.

3 PRESVEDČENIE, ŽE PENIAZE VYRIEŠIA VŠETKO

Prílišné spoliehanie sa na rozpočet, bez súčasného zlepšovania procesov a budovania silnej organizačnej kultúry, nevedie k reálnej odolnosti voči kybernetickým hrozbám.

Udržateľná kybernetická bezpečnosť si vyžaduje rovnováhu medzi finančnými prostriedkami a efektívnym riadením procesov.

4 VNÍMANIE KYBERNETICKEJ BEZPEČNOSTI AKO PREKÁŽKY

Kybernetická bezpečnosť by nemala byť považovaná za prekážku alebo zbytočný náklad.

Bezpečnosť musí byť neoddeliteľnou súčasťou podpory a ochrany základných činností organizácie, pričom prispieva k udržaniu a posilneniu jej dobrého mena.

Spolufinancovaný Európskou úniou

10 MANAŽÉRSKYCH CHÝB, KTORÉ VEDÚ K INCIDENTU

5 KULTÚRA VINY

Podpora kultúry viny vytvára atmosféru strachu, kde zamestnanci vykonávajú len nevyhnutné minimum. Utajovanie alebo popieranie problémov a rizík však vedie ku skreslenému vnímaniu reality.

Kultúra zodpovednosti, otvorená, trasnsparentná komunikácia a efektívny kontrolný systém sú kľúčové pre udržateľnú úroveň odolnosti voči hrozbám.

6 PREHNANÁ TOLERANCIA RIZIKA

Prílišné riskovanie a vágne vyhlásenia o akceptácii rizika môžu viesť k vážnym dôsledkom, ktoré procesy riadenia kontinuity nemusia zvládnuť a poistenie nemusí pokryť.

Je nevyhnutné mať jasne definované a realistické rámce pre akceptáciu rizika, aby sa minimalizovali potenciálne škody.

7 NEREÁLNE OČAKÁVANIA

Nastavenie nereálnych očakávaní od bezpečnostných opatrení a procesov riadenia bezpečnosti môže viesť k zlyhaniam.

Je dôležité mať jasný, realistický plán, ktorý zohľadňuje aktuálne spôsobilosti a dostupné personálne, finančné a časové zdroje.

8 TECHNOKRATICKÁ BEZPEČNOSTNÁ STRATÉGIA

Zameranie sa na technológiu, bez dostatočného dôrazu na ľudí, ich vzdelávanie a angažovanosť, vedie k zraniteľnostiam, ktoré technológia sama o sebe nedokáže pokryť.

Ľudský prvok v stratégii kybernetickej bezpečnosti nesmie byť prehliadaný.

Spolufinancovaný Európskou úniou

10 MANAŽÉRSKYCH CHÝB, KTORÉ VEDÚ K INCIDENTU

9 IGNOROVANIE VNÚTORNÝCH HROZIEB

Vnútorné hrozby predstavujú významné riziko, ktoré môže pochádzať od zamestnancov alebo dodávateľov organizácie. Tieto osoby môžu úmyselne, neúmyselne alebo z neznalosti spôsobiť incident, ako je únik citlivých informácií, zastavenie prevádzkových činností alebo nenávratnú stratu dát.

Včasná identifikácia a riadenie vnútorných hrozieb je nevyhnutné pre komplexnú ochranu organizácie.

10 CHÝBAJÚCE RIADENIE KONTINUITY

Prírodné katastrofy, kybernetické útoky, nedostupnosť zdrojov, alebo závažné poruchy technológie bez krízového plánu môže viesť k dlhodobým výpadkom produkcie, strate dôvery zákazníkov, reputačným škodám a v konečnom dôsledku aj k finančným stratám.

Prostredníctvom procesu riadenia kontinuity činností (Business Continuity Management - BCM) organizácia dokáže reagovať na nečakané udalosti a obnoviť svoje kľúčové aktivity v čo najkratšom čase.

Spolufinancovaný Európskou úniou