Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

KYBERNETICKÁ BEZPEČNOSŤ V KONTEXTE KOMPETENCIÍ

Sektorová rada pre Informačné technológie a telekomunikácie
18. 10. 2021

Ivan Makatura

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti (KCCKB)

- Štátna príspevková organizácia, zriadená 16. decembra 2019 rozhodnutím riaditeľa NBÚ ako súčasť európskej siete národných koordinačných centier odvetvových, technologických a výskumných kompetencií v kybernetickej bezpečnosti
- Hlavné úlohy Kompetenčného centra:
  - pôsobnosť National Coordination Centre v zmysle Nariadenia EÚ č. 2021/887
  - **audit kybernetickej bezpečnosti** podľa zákona č. 69/2018 Z.z.
  - **vzdelávanie dospelých** v kybernetickej bezpečnosti
  - organizácia kampaní na zvyšovanie povedomia v kybernetickej bezpečnosti
  - **certifikácia:**
    - audítorov a manažérov kybernetickej bezpečnosti,
    - systémov manažérstva
    - produktov v kybernetickej bezpečnosti podľa Nariadenia EÚ č. 2019/881
  - poskytovanie konzultácií v oblasti kybernetickej bezpečnosti, ochrany utajovaných skutočností, šifrovej ochrany a dôveryhodných služieb
- KCCKB je zároveň znaleckou organizáciou, ktorá vykonáva znaleckú a expertíznu činnosť podľa zákona č. 382/2004 Z. z..

Overovanie úrovne kybernetickej bezpečnosti

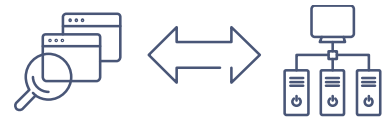
KYBERNETICKÁ BEZPEČNOSŤ V KONTEXTE KOMPETENCIÍ

METÓDY OVEROVANIA ÚROVNE BEZPEČNOSTI

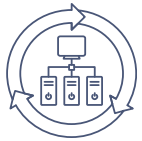
Overované entity a prvky sú v procese overovania úrovne bezpečnosti všeobecne nazývané ako „**objekty posúdenia**“ (z angl. „assessment objects“)

- Štyri základné prístupy ako sa môže subjekt uistiť o požadovanej úrovni KB:

1. **Posúdenie** - Dokazovanie, že sa splnili určené požiadavky týkajúce sa objektu posudzovania

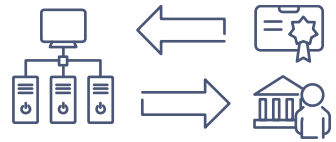


2. **Testovanie** - Proces, v ktorom je jeden alebo viac objektov posudzovania vystavených podľa opakovateľného postupu určitým podmienkam, s cieľom porovnať ich aktuálne a očakávané charakteristiky



3. **Audit** - 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

4. **Certifikácia** (Posudzovanie zhody) - Atestácia nezávislým akreditovaným orgánom posudzovania zhody, týkajúca sa charakteristík objektu posudzovania



POROVNANIE METÓD OVEROVANIA ÚROVNE BEZPEČNOSTI

Metóda	Určený nástroj	Opakovateľný postup	Formálna špecifikácia	Nestrannosť	Dôkazy	Certifikovaná osoba	Akreditácia	Dohľad
Posudzovanie	✗	✗	✗	✗	✗	✗	✗	✗
Testovanie	✓	✓	✓	✗	✗	✗	✗	✗
Audit	✓	✓	✓	✓	✓	✓	✗	✗
Certifikácia	✓	✓	✓	✓	✓	✓	✓	✓

OBJEKTY POSUDZOVANIA ZHODY V OBLASTI BEZPEČNOSTI

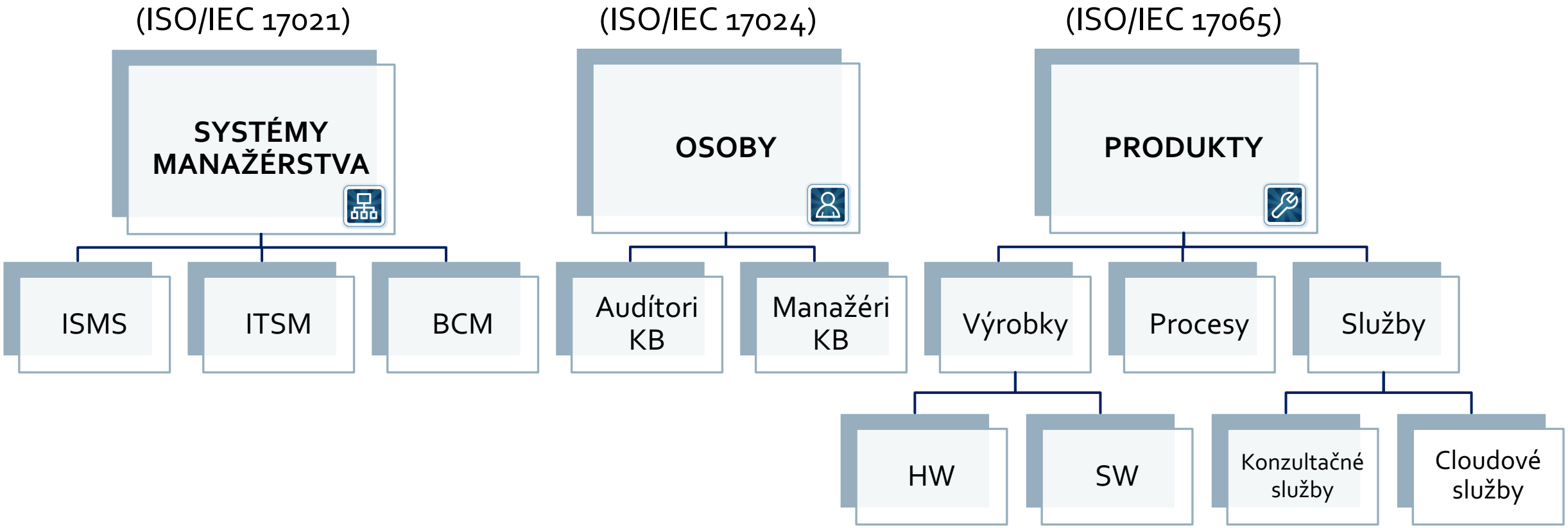


Schéma podľa Nariadenia 2008/765

POŽIADAVKA NA VÝKON AUDITU KYBERNETICKEJ BEZPEČNOSTI

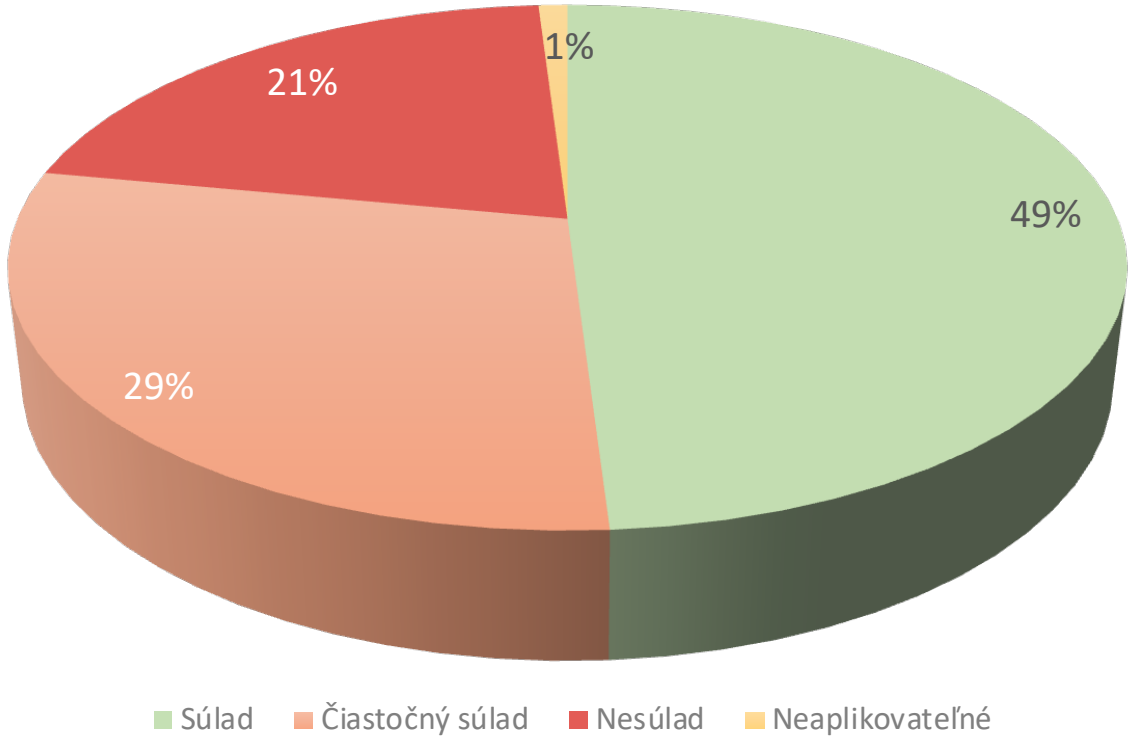
§ 29 Zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti:

1) Prevádzkovateľ základnej služby je povinný preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených zákonom **vykonaním auditu kybernetickej bezpečnosti** v rozsahu stanovenom **podľa všeobecne záväzného právneho predpisu**, ktorý vydá úrad, a to v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov **po každej zmene majúcej významný vplyv** na realizované bezpečnostné opatrenia **a v určenom časovom intervale**

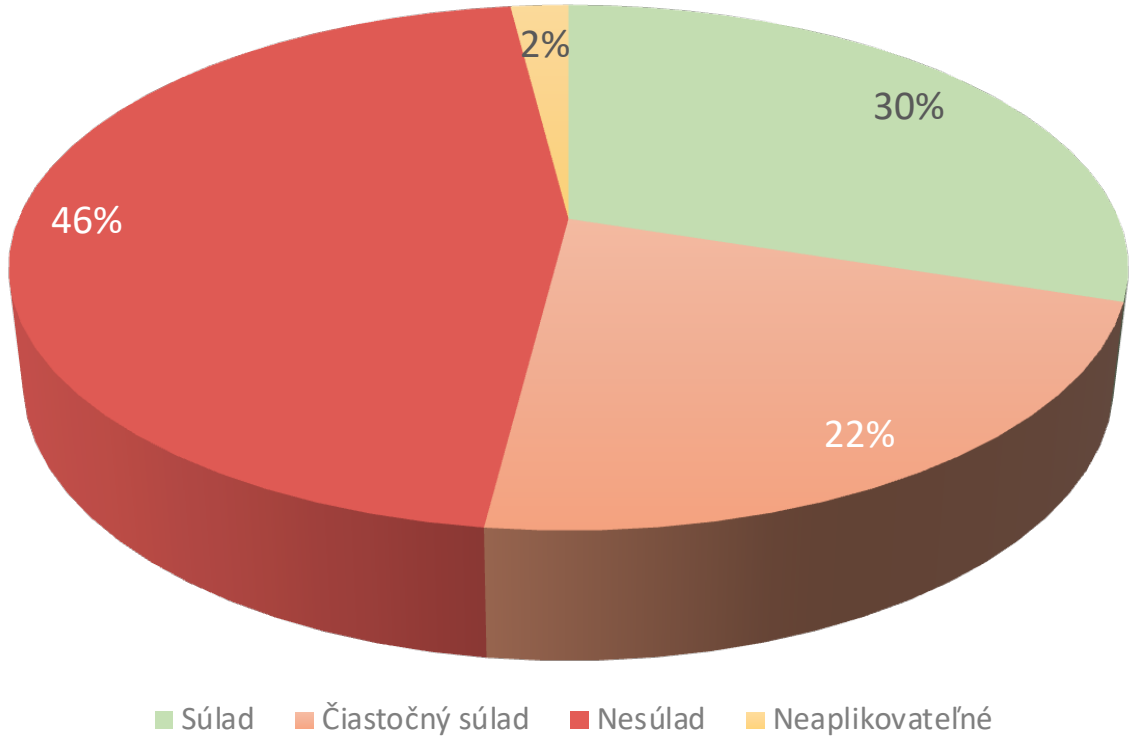
2) Audit kybernetickej bezpečnosti **vykonáva certifikovaný audítor kybernetickej bezpečnosti**, ktorým je fyzická osoba, spoločník, štatutárny orgán alebo zamestnanec právnickej osoby.
Certifikáciu audítora kybernetickej bezpečnosti vykonáva osoba akreditovaná podľa osobitného predpisu ako orgán certifikujúci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

STAV SÚLADU PODĽA VÝSLEDKOV AUDITU

KOMERČNÉ ORGANIZÁCIE



VEREJNÁ SPRÁVA

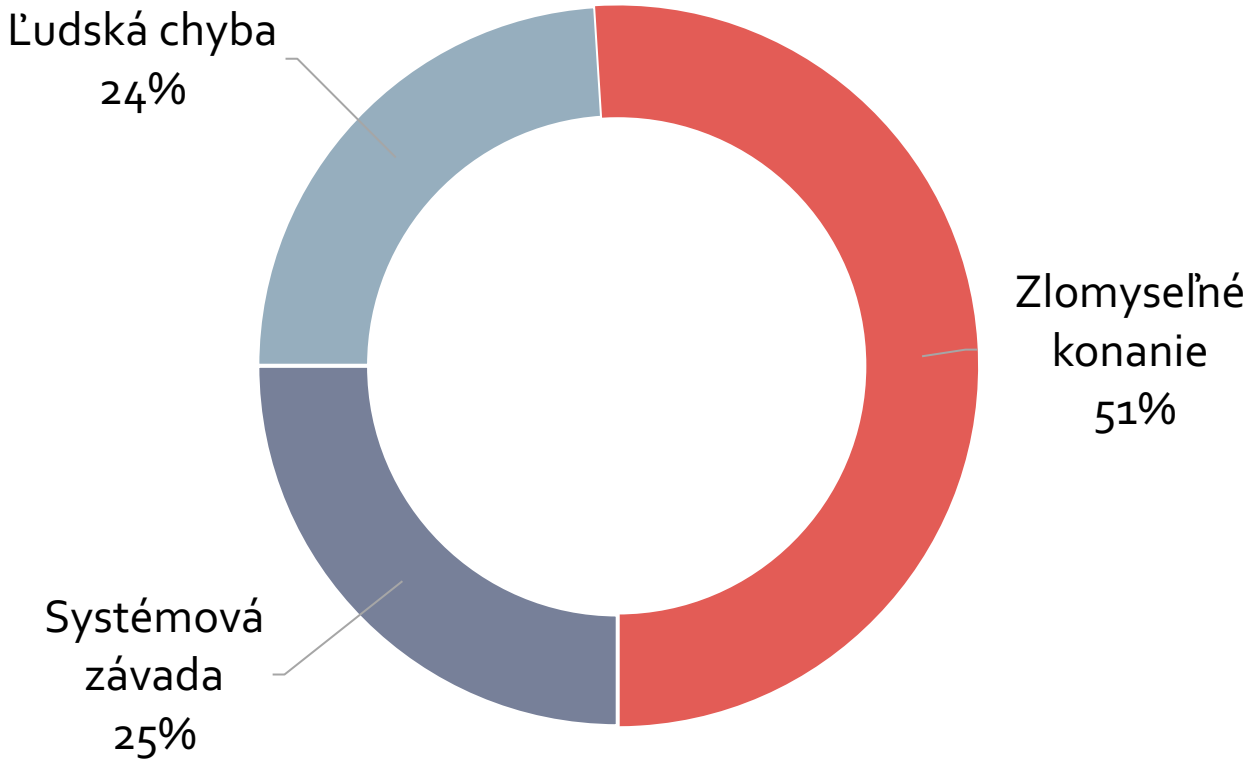


NAJČASTEJŠIE NÁLEZY AUDITU

- **Neexistujúca stratégia KB a nedostatočná podpora najvyššieho vedenia**
- **Neurčený Manažér KB**
- **Neformálne zaradený Manažér KB**
- **Neexistencia vzdelávania v oblasti informačnej bezpečnosti**
- Nedostatočná, alebo chýbajúca bezpečnostná dokumentácia (aj pri PZS s certifikátmi ISO27001)
- **Bezpečnostná dokumentácia často tvorená len dodávateľmi konkrétneho projektu**
- Bezpečnosť podriadená IT
- Závislosť na dodávateľoch (vendor lock)
- Neexistujúce riadenie aktív, hrozieb a rizík
- Nízka vyspelosť procesu riadenia rizík
- **Chýbajúci vlastníci rizík a ich zodpovednosti**
- Neformálne riadenie prevádzky IT
- Chýbajúci monitoring a logovanie
- Nesystematické riešenie incidentov
- Nedostatky v riadení bezpečnosti sietí (typicky - plný outsourcing bez prehľadu o procese)
- Chýbajúca topológia, segmentácia, zoznamy portov
- Nezabezpečenie a nevybavenosť „serverovní", často plných kvalitného HW
- Neexistencia procesov riadenia kontinuity činností
- Nejasné a neformálne postupy zálohovania, obnova netestovaná
- (Ne)šifrovanie komunikácie, prenosov údajov a záloh
- **Nepripravenosť na krízové situácie**

PRÍČINY INCIDENTOV PODĽA ZDROJA

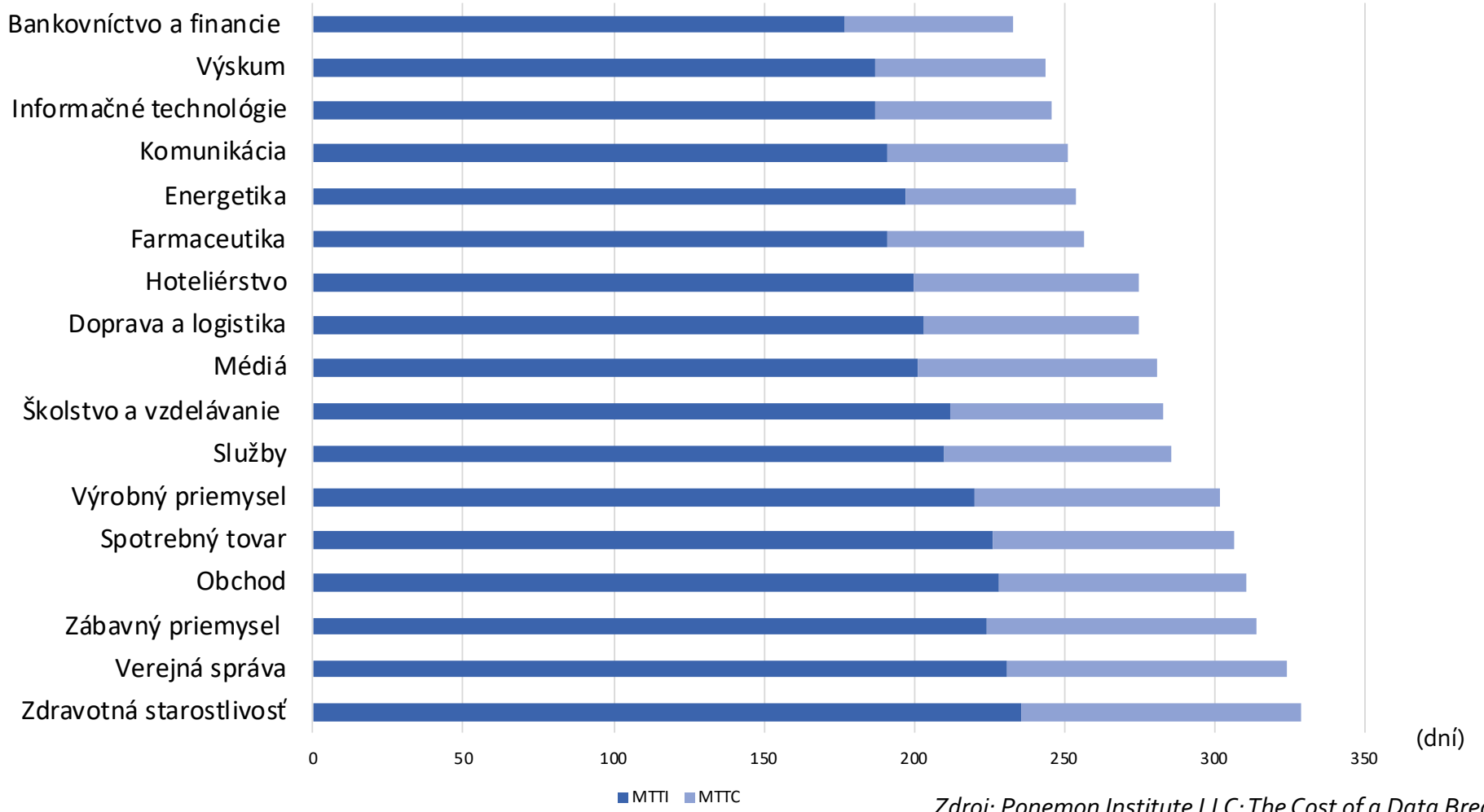
- Spôsob riešenia incidentu spôsobeného vonkajším útočníkom alebo zlomyseľným zamestnancom sa podstatne líši od riešenia incidentu spôsobeného ľudskou chybou alebo zlyhaním systému.
- V reportoch zvyknú byť skúmané najmä nasledujúce tri základné príčiny incidentov a náklady s nimi spojené.



Zdroj: Ponemon Institute LLC: The Cost of a Data Breach Report

STREDNÁ DOBA IDENTIFIKÁCIE A RIEŠENIA INCIDENTU PODĽA ODVETVÍ

MTTI - Mean Time to Identify, **MTTC** - Mean Time to Correct



Zdroj: Ponemon Institute LLC: The Cost of a Data Breach Report

Vzdelávanie v kybernetickej bezpečnosti

KYBERNETICKÁ BEZPEČNOSŤ V KONTEXTE KOMPETENCIÍ

CHARAKTERISTIKA VZDELÁVACÍCH POTRIEB V KB

Druh ďalšieho vzdelávania	Cieľová skupina	Typické dotknuté roly
Ďalšie odborné vzdelávanie	Špecialisti IB/KB	manažér KB, audítor KB, architekt KB, špecialista KB, analytik KB…
Upskilling a špecializačné tréningy	Informatici	správca systému, vývojár SW, IT architekt, operátor, databázový špecialista…
Zvyšovanie digitálnej gramotnosti	Odborní zamestnanci	všetky pracovné roly, ktoré používajú k práci prostriedky IKT, s dôrazom na riadiacich zamestnancov
Zvyšovanie bezpečnostného povedomia	Všetci zamestnanci	všetky pracovné roly

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

ZODPOVEDNOSŤ ZA VZDELÁVANIE V KB

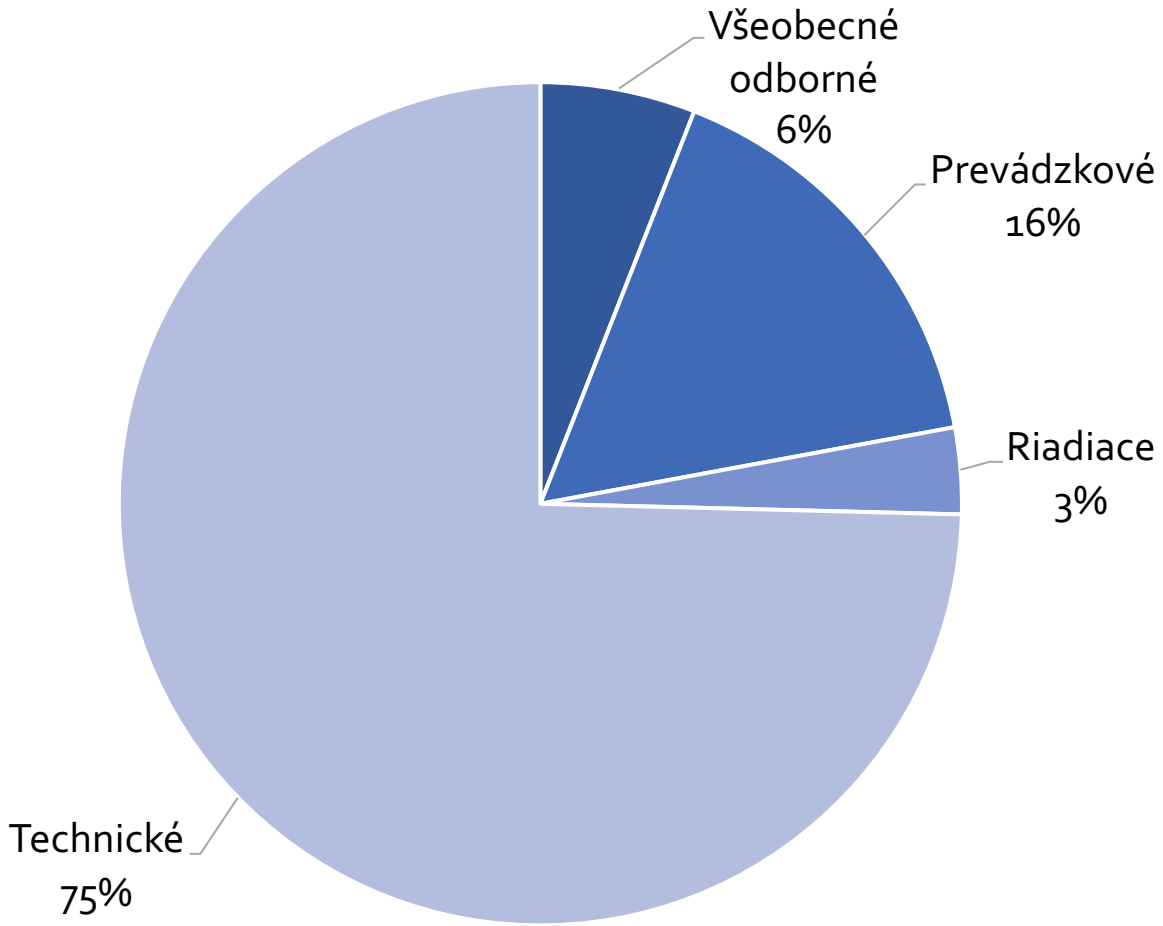
Základné školstvo	Stredné školstvo	Vysoké školy Univerzity	VZDELÁVANIE DOSPELÝCH
▪ Štát / NGO ▪ Školské kluby ▪ Základný prehľad	▪ Štát / NGO ▪ Komerčné organizácie ▪ Základy IT a KB	▪ Štát / Komerčné organizácie ▪ VŠ diplomy ▪ Teória KB / IB	▪ Štát / Komerčné organizácie ▪ Certifikácia osôb ▪ Teória & dobrá prax

METODIKA PRE STANOVENIE KVALIFIKAČNÉHO RÁMCA ROLÍ

Použiteľná inšpirácia pre kvalifikačný rámec jednotlivých rolí je: National Initiative for Cybersecurity Education (NICE).

Rámec pozostáva z nasledujúcich komponentov:

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



Zdroj: NICE

TYPICKÉ ROLY V KYBERNETICKEJ BEZPEČNOSTI V SR

- Manažér kybernetickej bezpečnosti
- Audítor kybernetickej bezpečnosti
- Bezpečnostný architekt
- Špecialista kybernetickej bezpečnosti
- Špecialista riadenia rizík
- Operátor bezpečnostnstných systémov
- Analytik kybernetickej bezpečnosti
- Tester kybernetickej bezpečnosti (etický hacker)
- Špecialista fyzickej a objektovej bezpečnosti
- Špecialista ochrany osobných údajov / riadenie súladu
- Špecialista pre analýzu digitálnych stôp

TYPY VZDELÁVACÍCH PRODUKTOV

VIAC TEORETICKÉ – ZNALOSTI → **VIAC PRAKTICKÉ – ZRUČNOSTI**

PREDNÁŠKA

- Výklad z prezentácie, na konci niekoľko otázok
- Vhodné pre veľké audítorium, prezenčné/online
- Príklad: konferencie
- Rozsah: 0,2-2 hod

WEBINÁR

- Ako prednáška, ale pre uzavretú skupinu ľudí
- Prednáška a diskusia na konci, pomer cca.: 85/15
- Príklad: klient potrebuje pochopiť legislatívu KB
- Rozsah: 0,5-1 deň

KURZ

- Interaktívne vzdelávanie skupiny max 12-15 úč.
- Teoretický výklad s diskusiami a cvičeniami, pomer cca. 70:30
- Verejné/inhouse, online/prezenčné
- Rozsah: 1-3 dni

WORKSHOP

- Spoločná práca na špecifickú tému (skupiny, simulácie)
- Teoretická/praktická časť pomer 20/80
- Najmä inhouse
- Príklad: Ako spraviť analýzu rizík

TRÉNING

- Simulácia konkrétneho prípadu
- Praktické, min. teórie
- Najmä inhouse
- Príklad: Riadenie KBI na konkrétnej technológii

CENA →

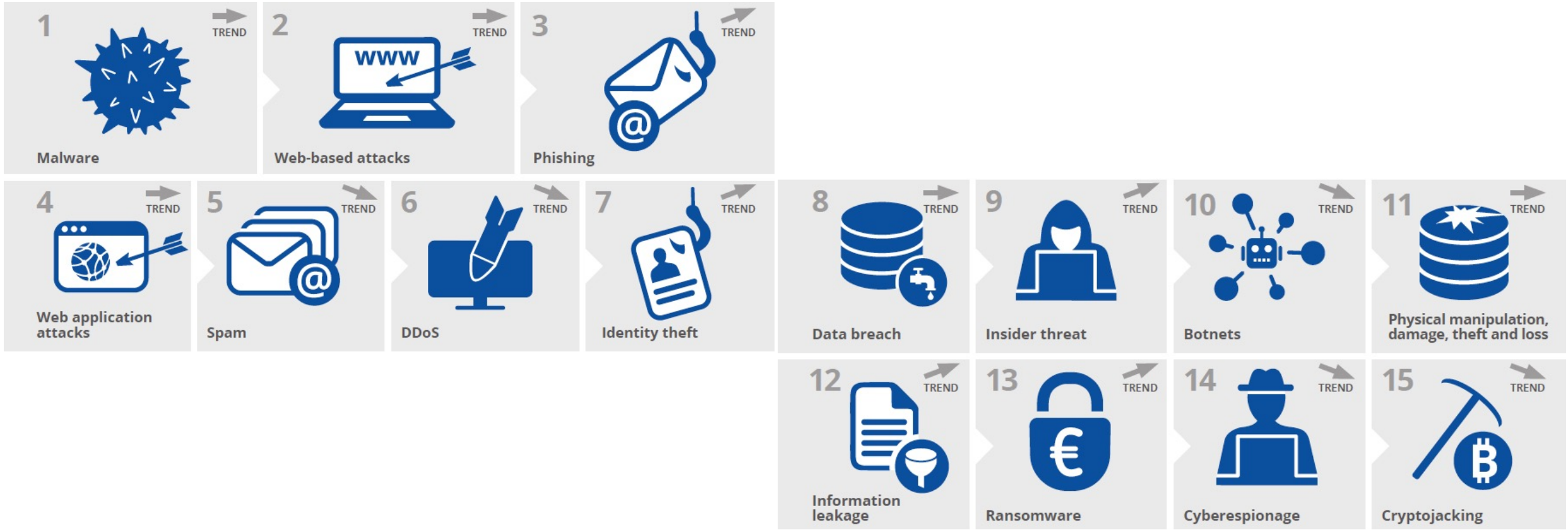
TYPICKÁ DISTRIBÚCIA KVALIFIKÁCIÍ

ÚROVEŇ ZNALOSTÍ	Laici	Odborní zamestnanci	Manažéri	IT manažéri	Informatici	Špecialisti KB	Manažéri KB	Audítori KB
Znalosť vybraných základných pojmov a ich významu	✓	✓	✓	✓	✓	✓	✓	✓
Použitie mechanizmov a procesov v bezpečnostných riešeniach		✓	✓	✓	✓	✓	✓	✓
Legislatíva, súlad a etika ochrany údajov				✓			✓	✓
Implementácia a uplatňovanie bezpečnostných mechanizmov a riešení				✓	✓	✓	✓	✓
Návrh bezpečnostných mechanizmov a riešení					✓	✓	✓	✓
Návrh stratégií a analýza bezpečnostných mechanizmov a riešení						✓	✓	✓
Posudzovanie zhody a efektivity procesov, bezpečnostných mechanizmov a riešení								✓
PRÍSLUŠNÝ KURZ	PREHĽAD KB 〉			ZÁKLADY KB 〉		MANAŽÉR KB 〉		AUDÍTOR KB 〉

Záver

KYBERNETICKÁ BEZPEČNOSŤ V KONTEXTE KOMPETENCIÍ

NAJZÁVAŽNEJŠIE HROZBY 2020

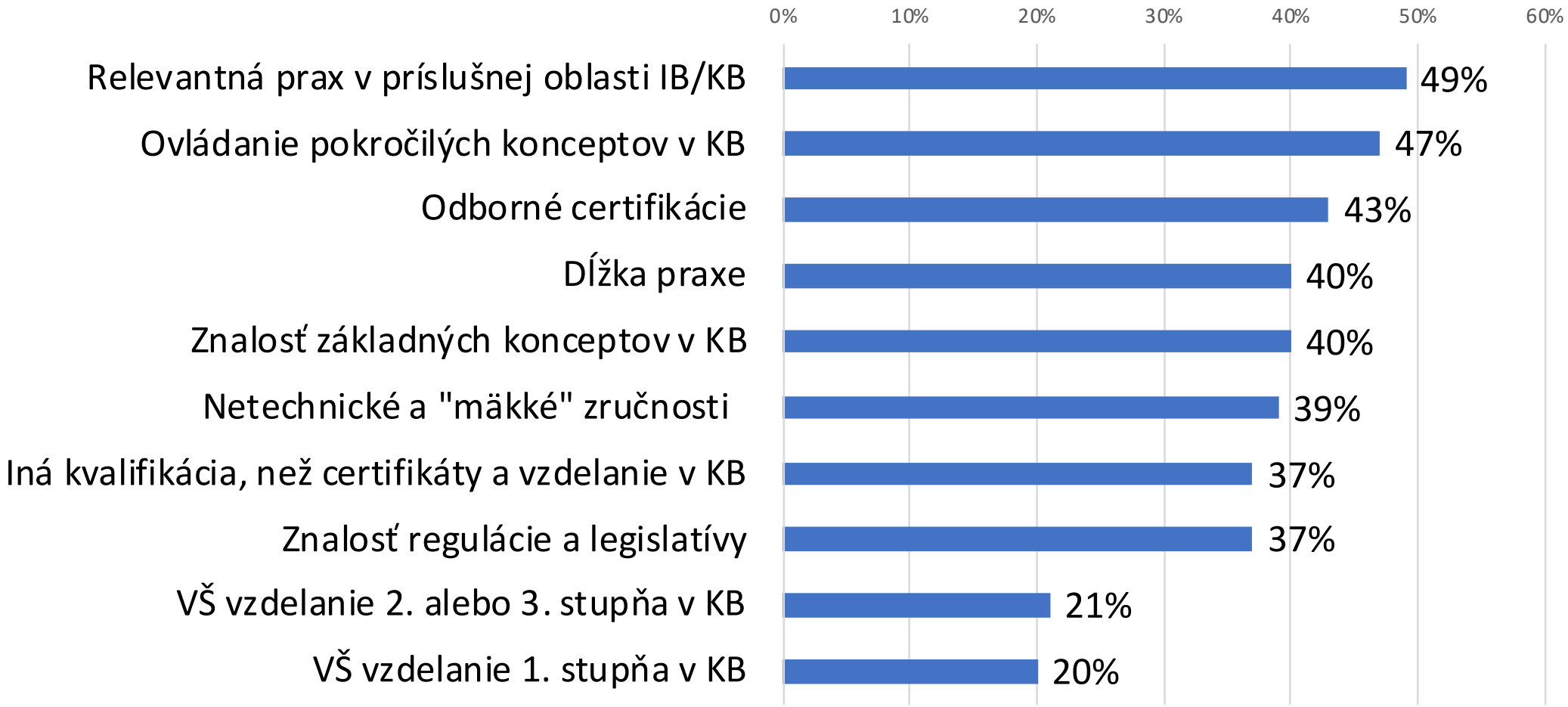


https://www.enisa.europa.eu

VYHĽADÁVANÉ KOMPETENCIE V KB

Zdroj: Enterprise Security Group

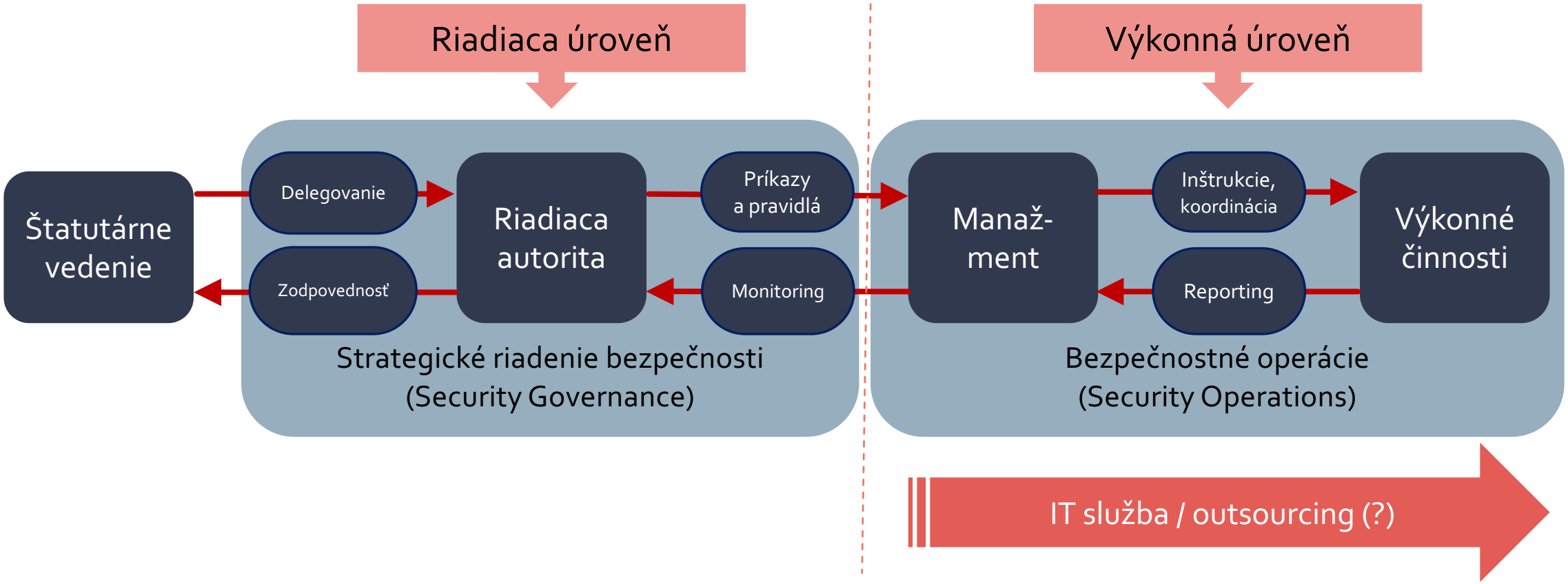
DÔLEŽITOSŤ RÔZNYCH DRUHOV KVALIFIKÁCIÍ V KB



Zdroj: ISC2 Cybersecurity Workforce Study

AKO PREKLENÚŤ NEDOSTATOK KAPACITY?

KĽÚČOVÉ ROLY A VZŤAHY V RIADENÍ A VÝKONE BEZPEČNOSTI:

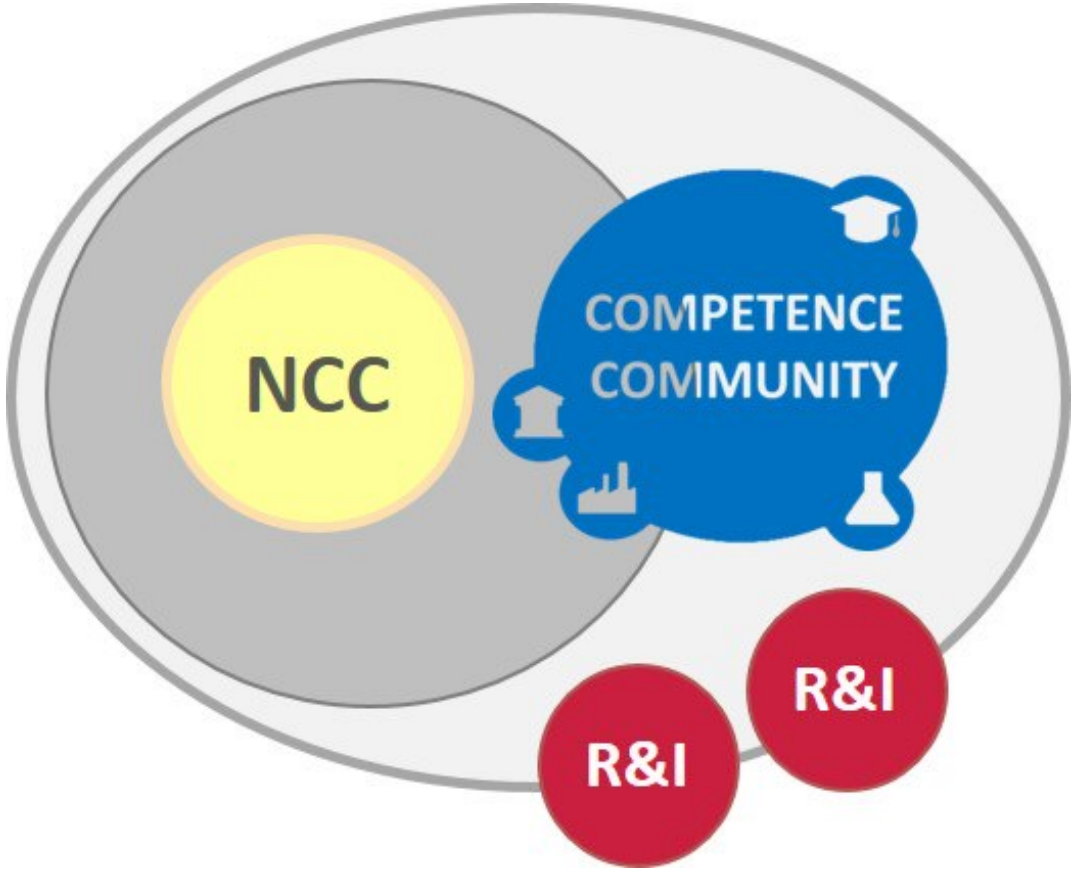


Zdroj: ISACA, isaca.org/cobit5

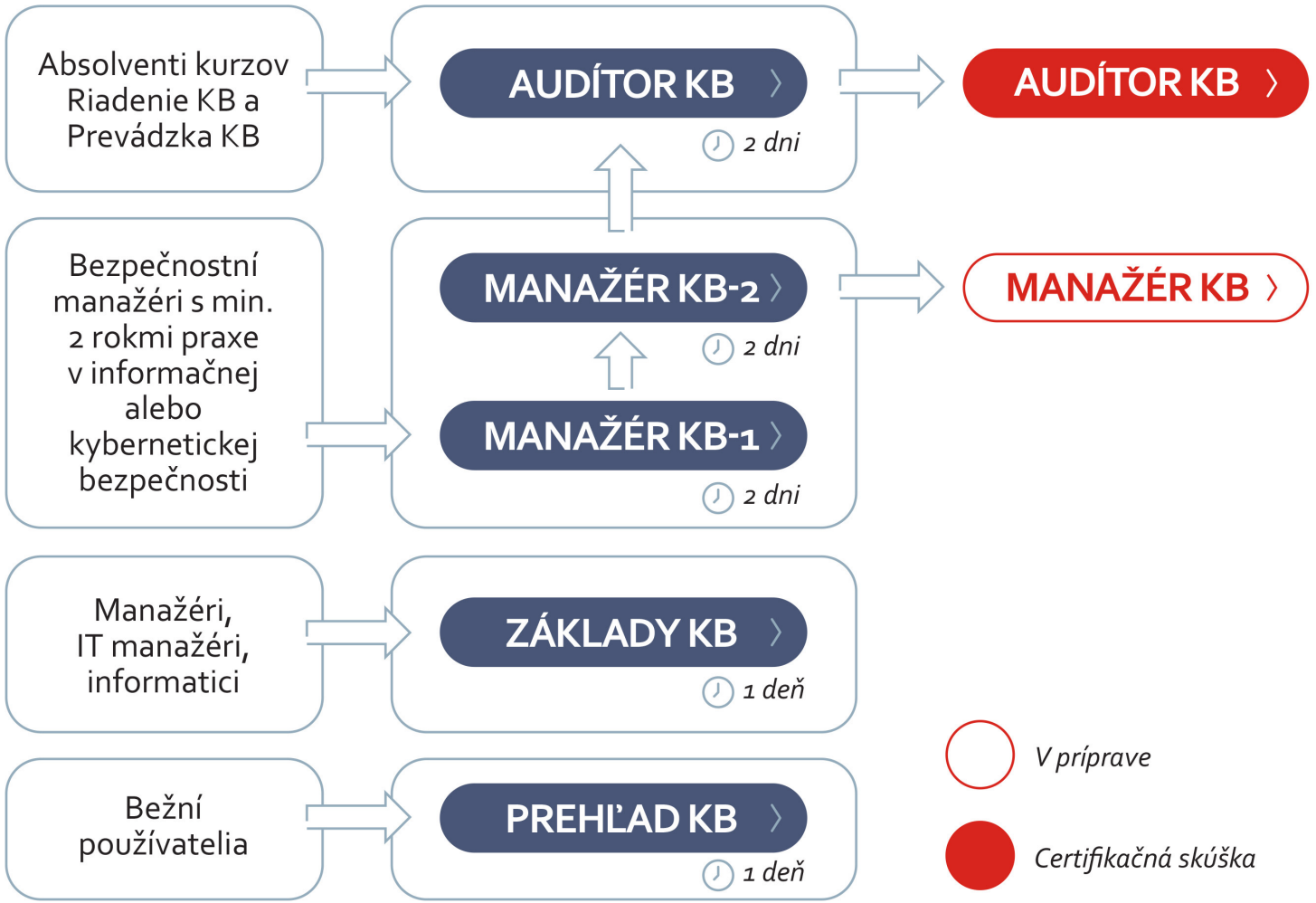
NÁRODNÉ KOORDINAČNÉ CENTRUM (NCC)

Subjekt verejného sektora alebo subjekt vo väčšinovom vlastníctve ČŠ, ktorý vykonáva funkcie verejnej správy, ktorý:

- má spôsobilosť podporovať ECCC a sieť pri plnení ich úloh a poslania
- disponuje výskumnými a technologickými odbornými znalosťami v KB (alebo k nim má prístup)
- má kapacitu na účinnú spoluprácu a koordináciu činností s priemyslom, verejným sektorom, akademickou obcou, výskumnou komunitou a občanmi, ako aj PZS (smernica NIS)



KCCKB: VZDELÁVACÍ PROGRAM & CERTIFIKÁCIA V KB



Podmienky absolvovania kurzov:

- Kurz Audítor KB je nadstavbou nad kurzy Manažér KB-1 a KB-2 a nie je možné ho absolvovať samostatne
- Certifikačnú skúšku je možné absolvovať aj bez účasti na kurzoch, ale nie je to odporúčané
- Pre účasť na certifikačnej skúške nestačí absolvovanie kurzov, je potrebné splniť aj podmienky praxe a vzdelania uvedené na stránkach www.cybercompetence.sk

Ochrana vlastníckych práv

Vlastnícke práva tretích strán

Limity informácií