Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

NCC-SK
SLOVAKIA CYBERSECURITY COORDINATION CENTRE

POŽIADAVKY KYBERNETICKEJ BEZPEČNOSTI V SAMOSPRÁVE MIEST A OBCÍ

Stretnutie APÚMS, Podbanské

12.10.2023

KOMPETENČNÉ A CERTIFIKAČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

Skrátene „Kompetenčné centrum", alebo „KCCKB" je štátna príspevková organizácia zriadená Národným bezpečnostným úradom podľa § 21 zákona č. 523/2004 Z. z. o rozpočtových pravidlách verejnej správy

Hlavné úlohy:

- Pôsobnosť **Národného koordinačného centra** v zmysle Nariadenia EÚ č. 2021/887 o Európskej sieti centier odvetvových, technologických a výskumných kompetencií
- **Certifikácia:**
  - audítorov a manažérov kybernetickej bezpečnosti
  - systémov manažérstva
  - produktov v kybernetickej bezpečnosti podľa Nariadenia EÚ č. 2019/881
- **Vzdelávanie dospelých** v kybernetickej bezpečnosti
- Organizácia kampaní na zvyšovanie povedomia v kybernetickej bezpečnosti
- Publikačná činnosť
- **Audit kybernetickej bezpečnosti** podľa zákona č. 69/2018 Z.z.
- Konzultačné služby v oblasti kybernetickej bezpečnosti, utajovaných skutočností a dôveryhodných služieb
- Znalecká a expertízna činnosť podľa zákona č. 382/2004 Z. z.. o znalcoch

STAV SÚLADU

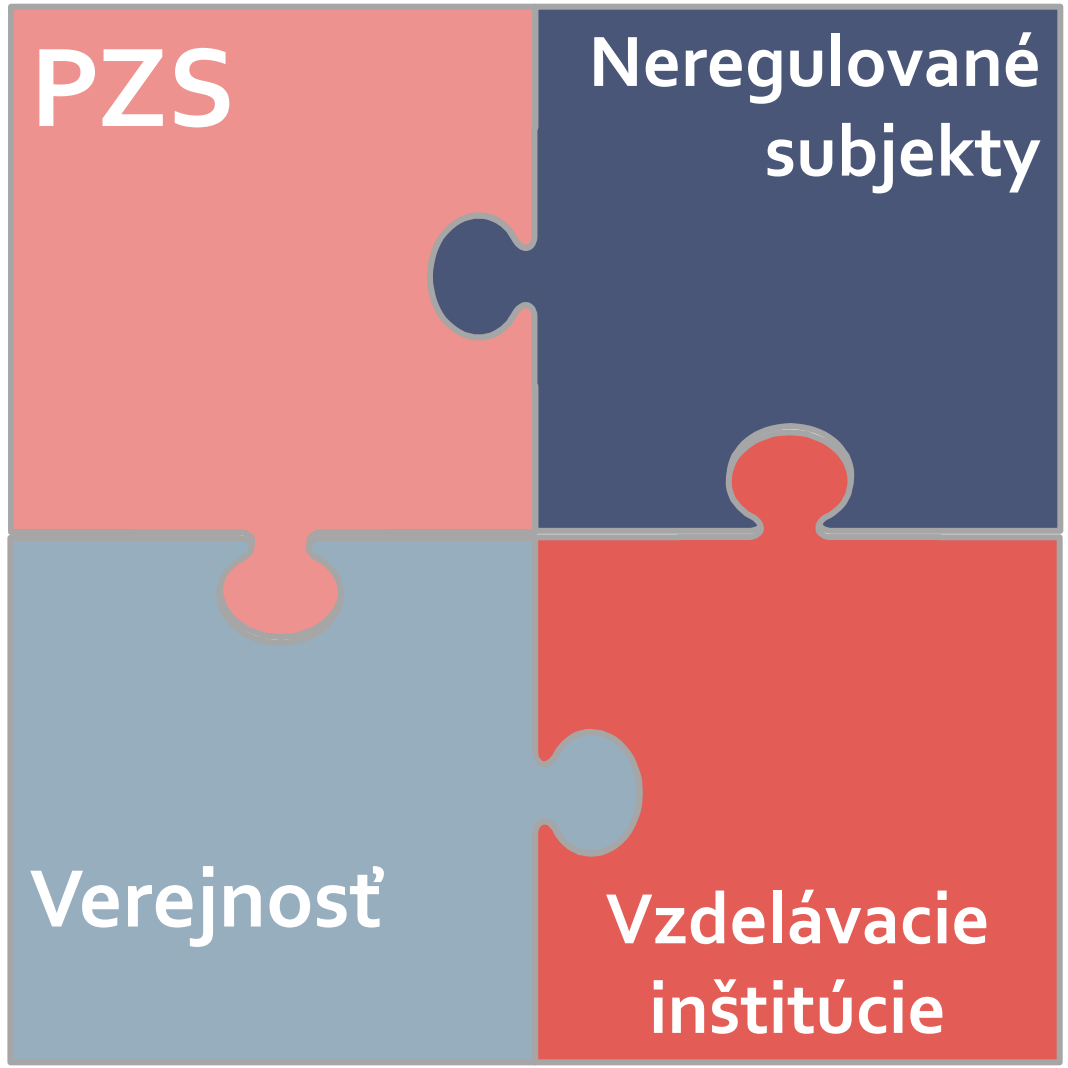
POŽIADAVKY KYBERNETICKEJ BEZPEČNOSTI V SAMOSPRÁVE MIEST A OBCÍ

AKÉ ÚDAJE? Z AKÝCH ZDROJOV?

Anonymizované dáta o počte auditných zistení zo záverečných správ auditu podľa § 29 zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti

Anonymizované dáta z formulárov samohodnotenia doručených Úradu podľa § 34a zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti

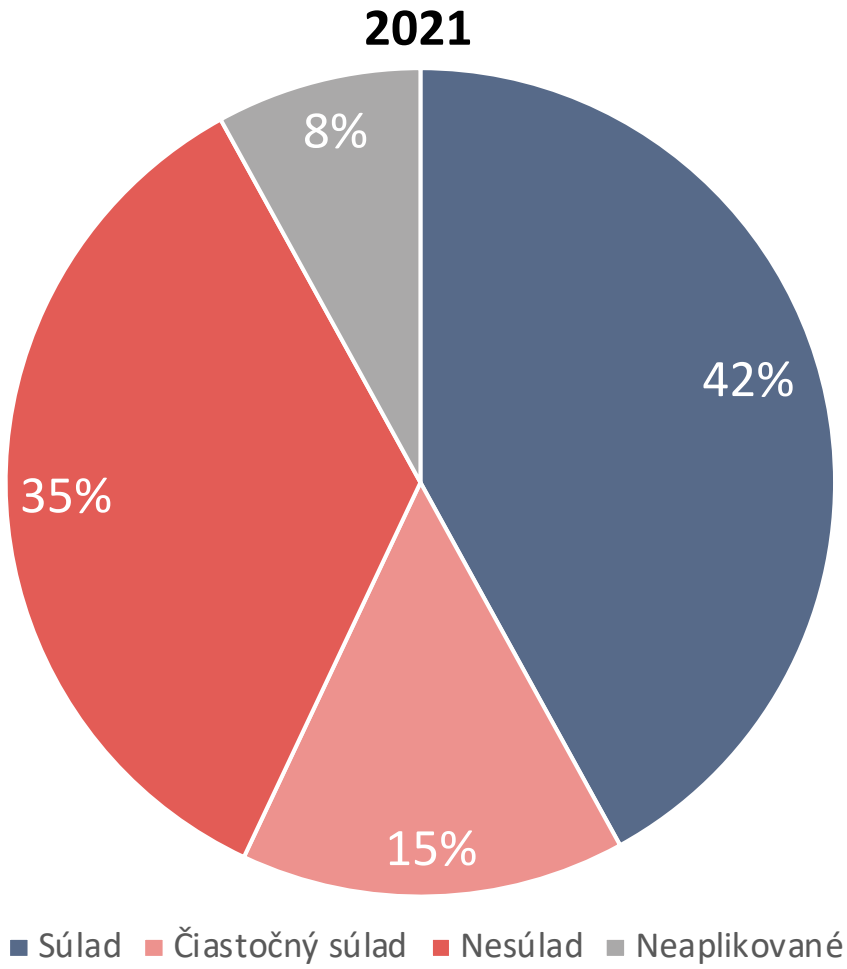
Výsledky prieskumov vypracovaných podľa štandardov Slovenskej Asociácie Výskumných Agentúr, prostredníctvom agentúry AKO



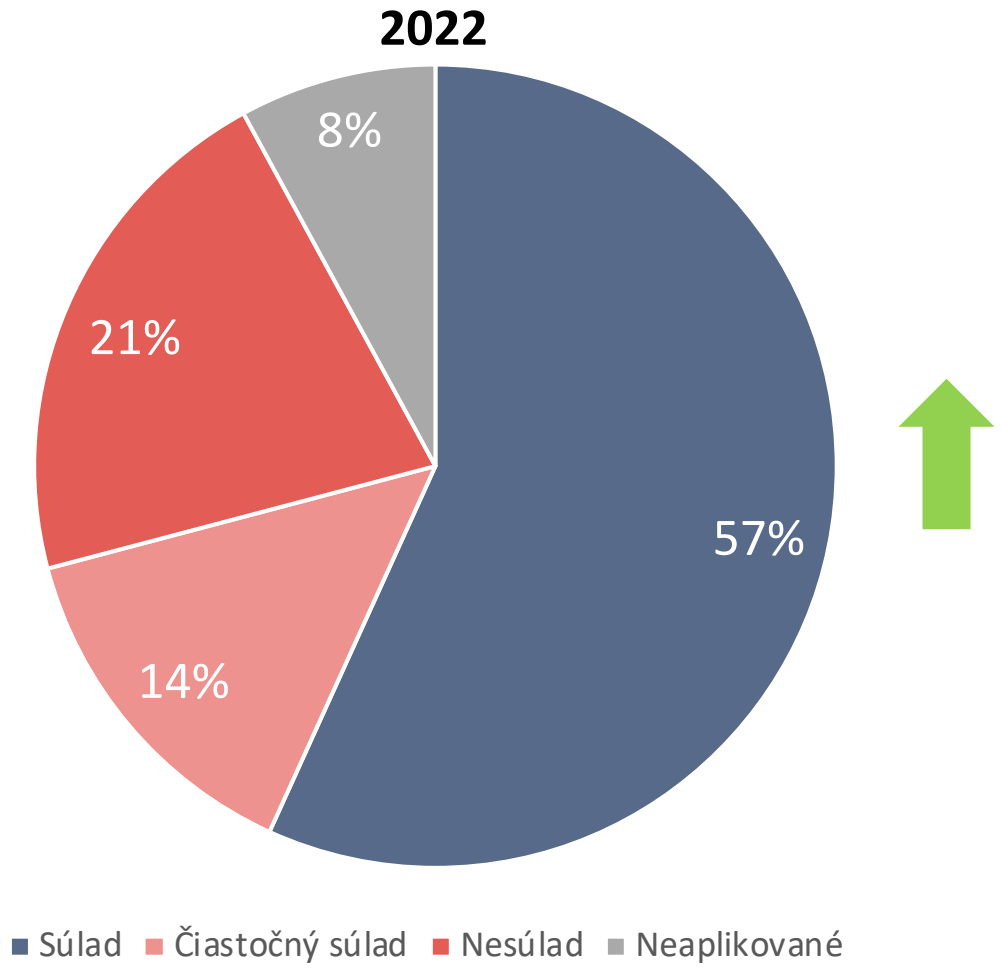
Výsledky prieskumov vypracovaných podľa štandardov Slovenskej Asociácie Výskumných Agentúr, prostredníctvom agentúry AKO

Priame prieskumy na základe memoránd o spolupráci s VŠ

CELKOVÁ PRIEMERNÁ MIERA SÚLADU V SR



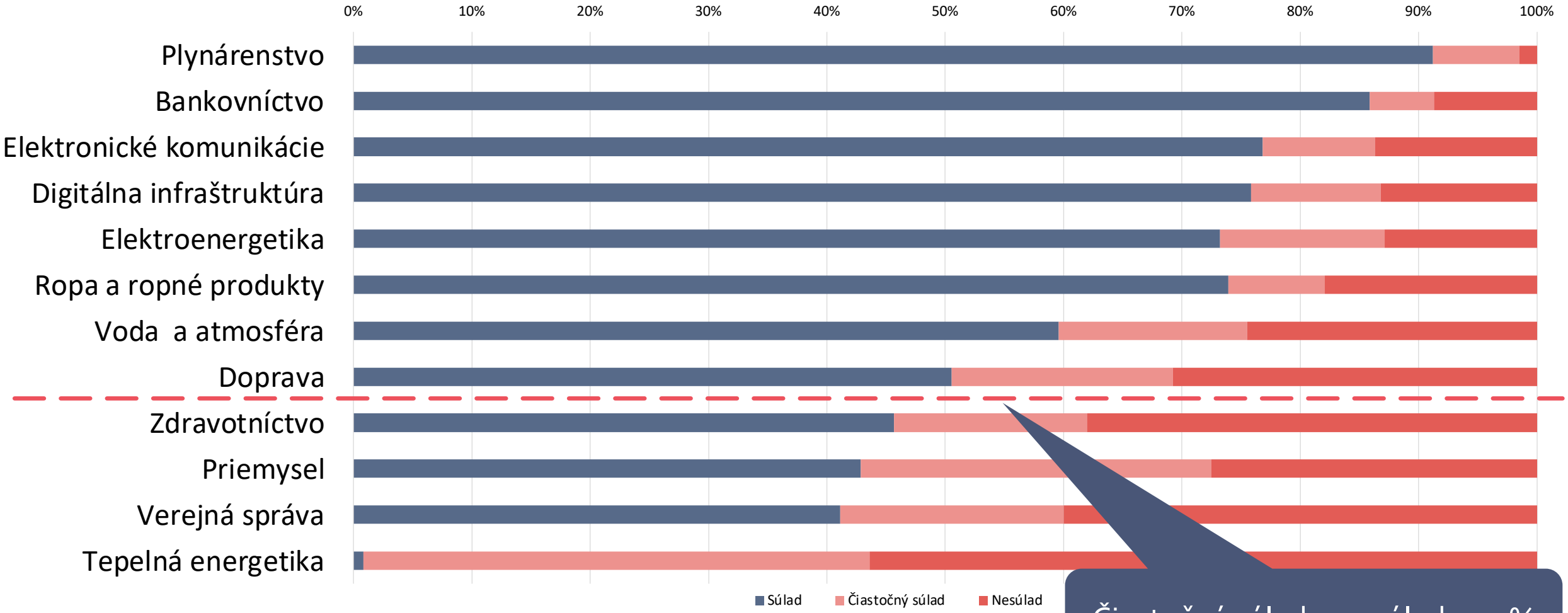
Zdroj: Doručené správy auditu 2022, NBÚ



Zdroj: Doručené správy auditu 2023, NBÚ

Spolufinancovaný Európskou úniou

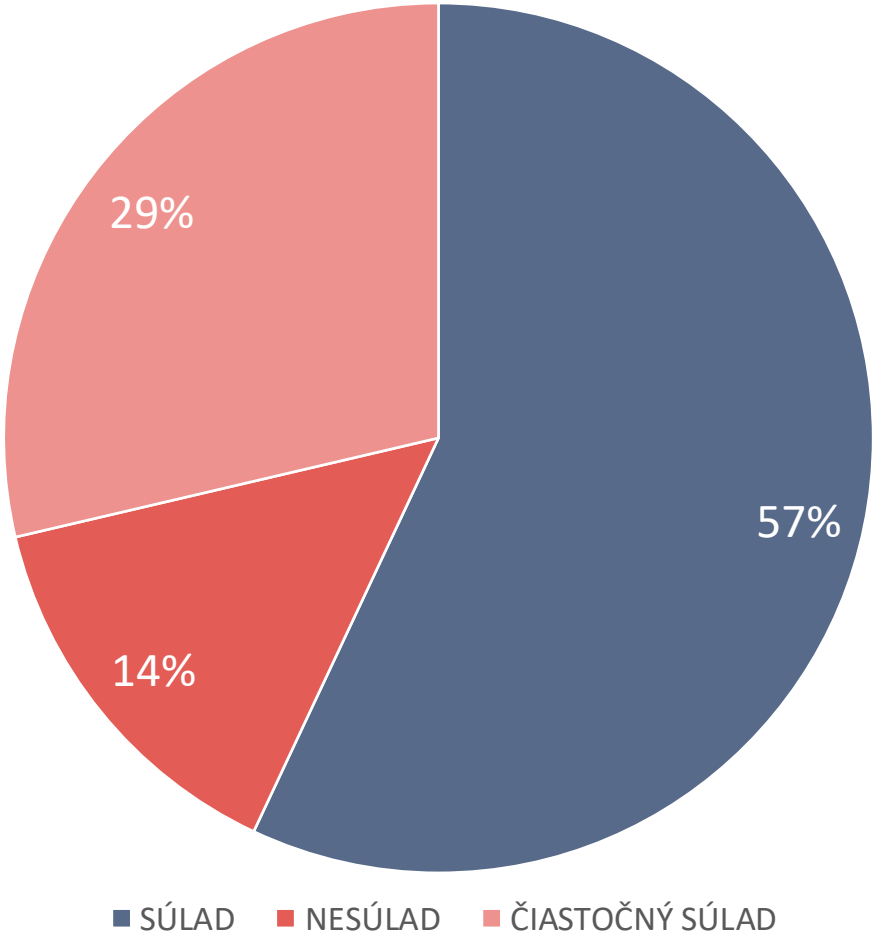
STAV SÚLADU PODĽA ODVETVÍ (2022)



Zdroj: Doručené správy auditu 2022, NBÚ

Spolufinancovaný Európskou úniou

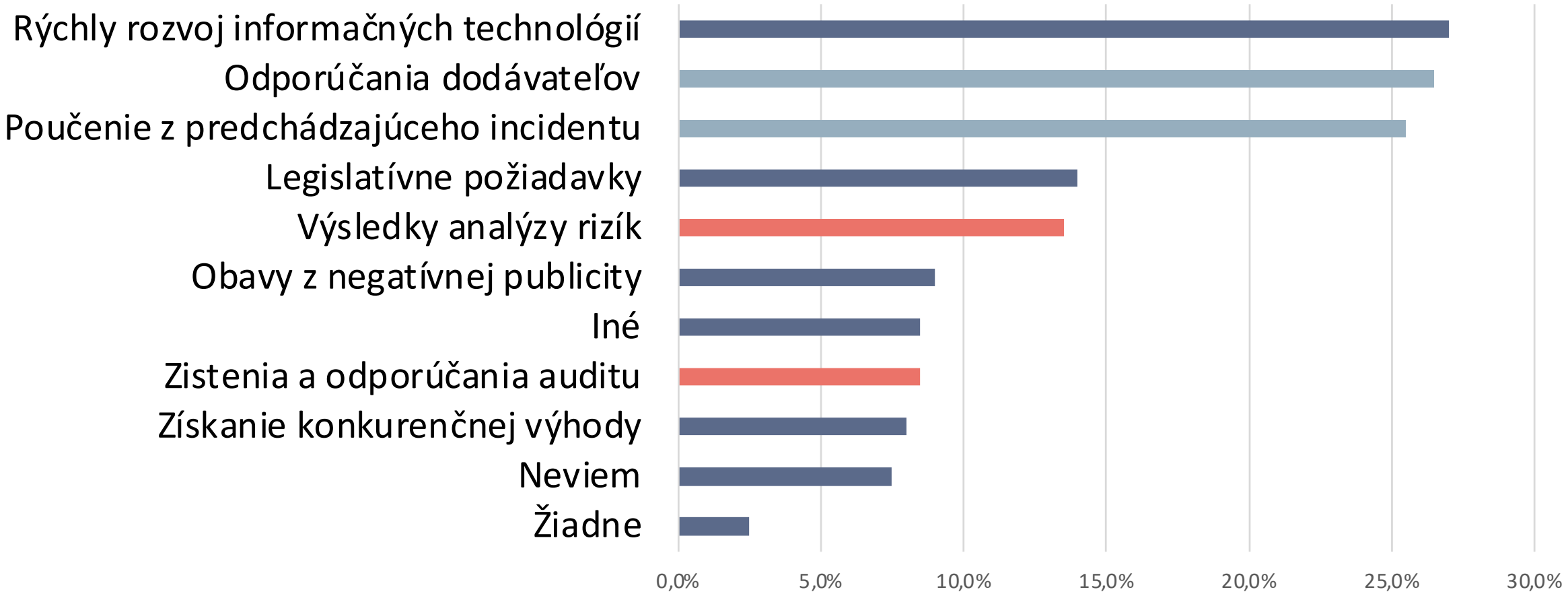
VÝSLEDKY SAMOHODNOTENIA (2022)



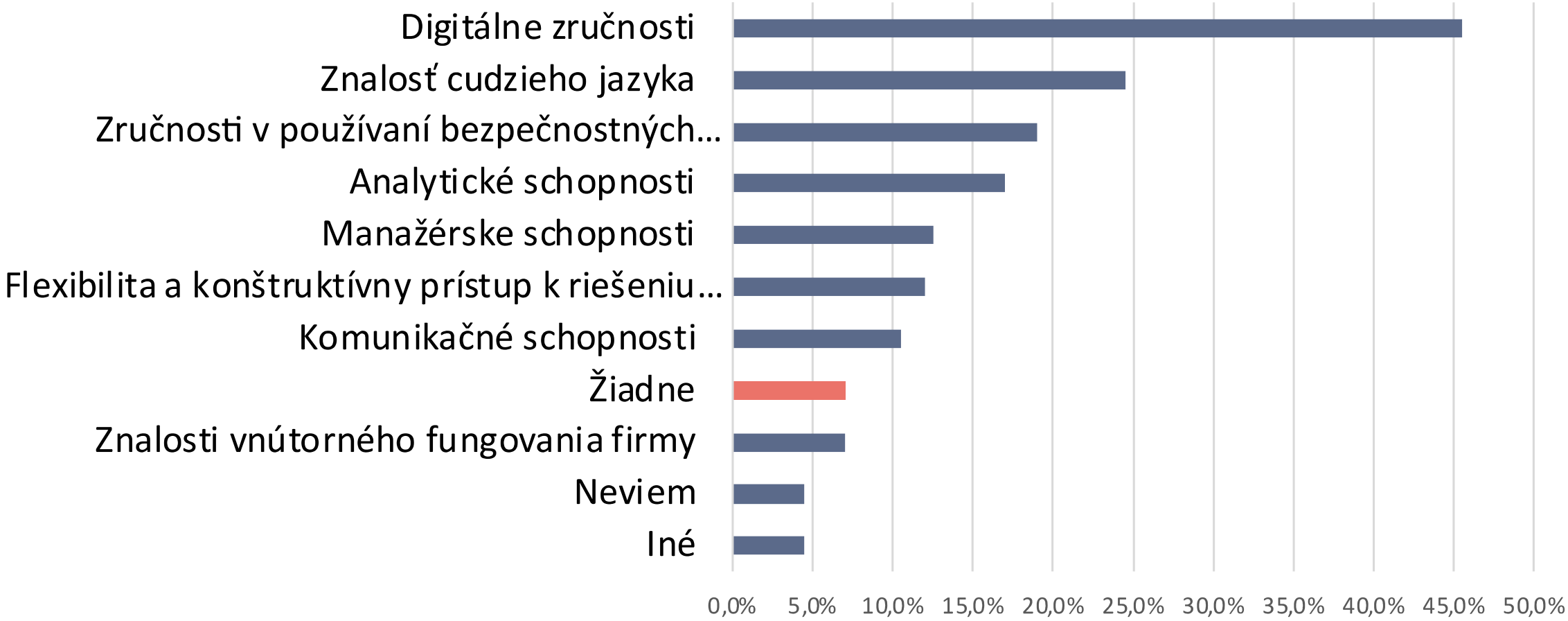
Zdroj: Doručené formuláre samohodnotenia 2022, NBÚ

Spolufinancovaný Európskou úniou

AKÉ FAKTORY MAJÚ VO VAŠEJ ORGANIZÁCII NAJVYŠŠÍ VPLYV NA ZVYŠOVANIE ÚROVNE KYBERNETICKEJ BEZPEČNOSTI?

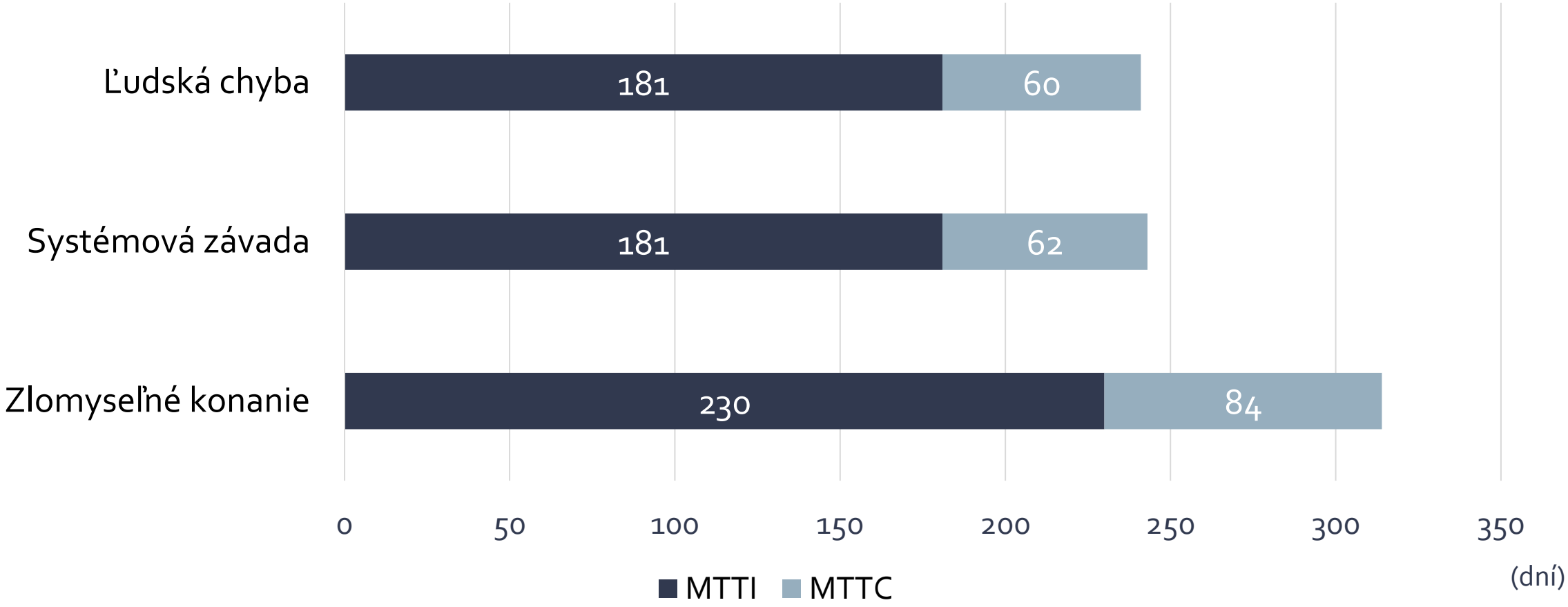


KTORÉ ZNALOSTI A SKÚSENOSTI ZAMESTNANCOV POVAŽUJETE MOMENTÁLNE NAJVIAC ZA NEDOSTATKOVÉ?



KOĽKO TRVÁ BEŽNÝ INCIDENT?

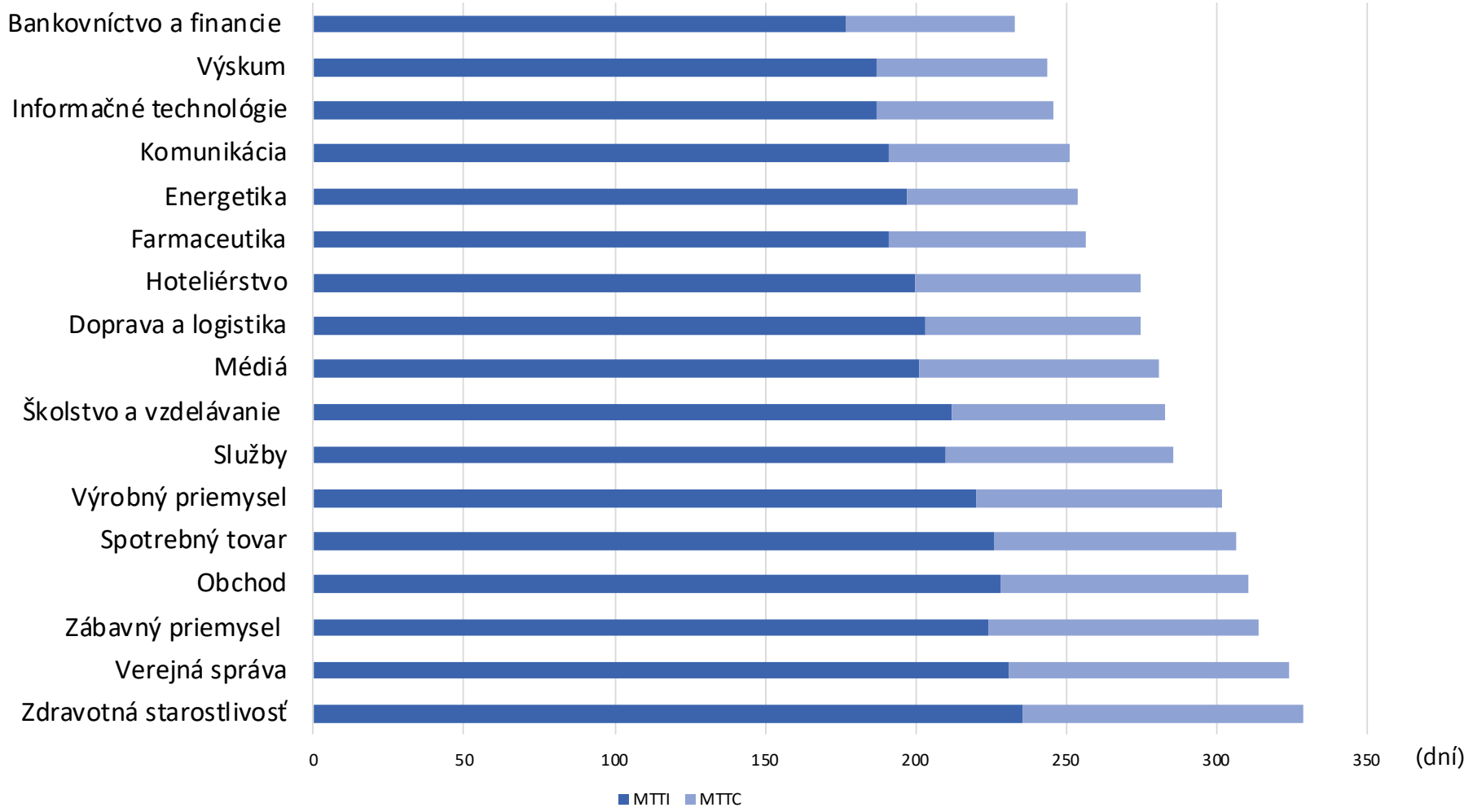
MTTI - Mean Time to Identify, **MTTC -** Mean Time to Correct



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

NAJČASTEJŠIE NÁLEZY AUDITU

Riadenie bezpečnosti (Security governance):

- Neexistujúca stratégia KB a nedostatočná podpora vedenia
- Neurčený Manažér KB
- Neexistujúce riadenie aktív, hrozieb a rizík
- Nedostatočná, alebo chýbajúca bezpečnostná dokumentácia
- Dokumentácia často tvorená len dodávateľmi konkrétneho projektu
- Nezávislosť riadenia bezpečnosti od riadenia IT
- Neexistencia vzdelávania v oblasti informačnej bezpečnosti
- Neformálne riadenie prevádzky IT

Výkon bezpečnosti (Security operations):

- Chýbajúci bezpečnostný monitoring
- Chýbajúce logovanie
- Nesystematické riešenie incidentov
- Nedostatky v riadení bezpečnosti sietí
- Chýbajúca topológia, segmentácia, zoznamy portov
- Neexistencia procesov riadenia kontinuity činností
- Nejasné a neformálne postupy zálohovania, obnova záloh netestovaná
- (Ne)šifrovanie komunikácie, prenosov údajov a záloh

Spolufinancovaný Európskou úniou

PRÁVNA ÚPRAVA KYBERBEZPEČNOSTI

POŽIADAVKY KYBERNETICKEJ BEZPEČNOSTI V SAMOSPRÁVE MIEST A OBCÍ

NÁRODNÁ PRÁVNA ÚPRAVA KYBERNETICKEJ BEZPEČNOSTI

Zákon č. 45/2011 Z.z.
o kritickej infraštruktúre

Zákon č. 69/2018 Z.z.
o kybernetickej bezpečnosti

- **Vyhláška NBÚ č. 164/2018 Z.z.**, ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby)
- **Vyhláška NBÚ č. 165/2018 Z.z.,** ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov
- **Vyhláška č.166/2018** o podrobnostiach o technickom, technologickom a personálnom vybavení CSIRT
- **Vyhláška NBÚ č. 362/2018 Z.z.,** ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení
- **Vyhláška NBÚ č. 436/2019 Z.z**. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora
- **Vyhláška NBÚ č. 493/2022 Z.z.**, ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti

Zákon č. 18/2018 Z.z.
o ochrane osobných údajov

Zákon č. 95/2019 Z.z.
o informačných technológiách vo verejnej správe

- **Vyhláška ÚPVII č. 179/2020 Z.z.**, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy

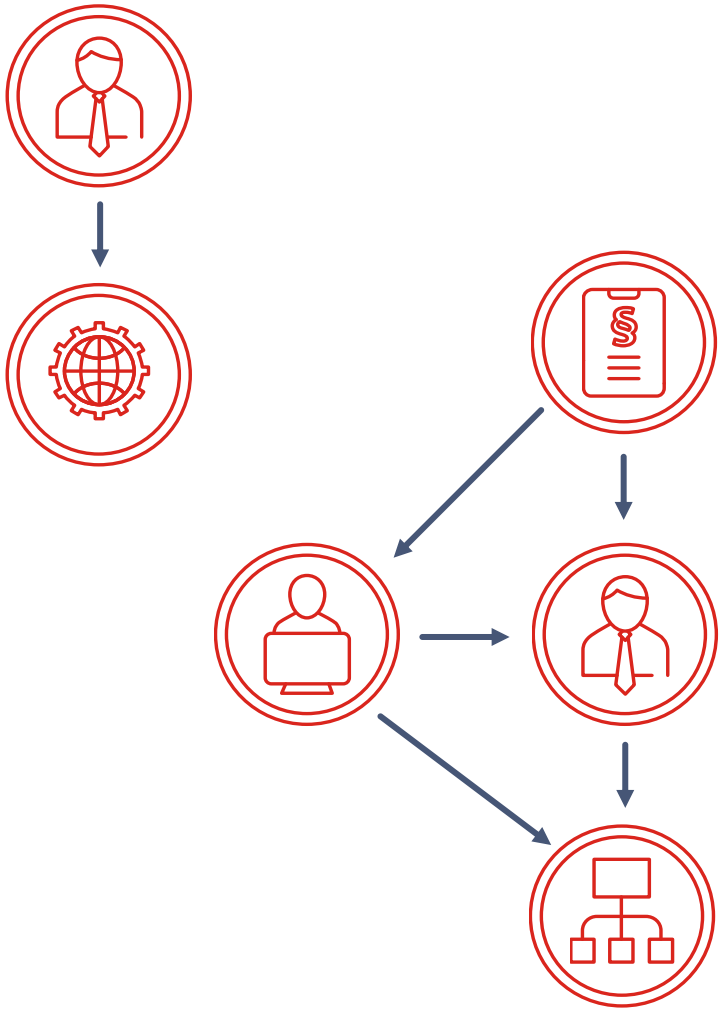
„PREVÁDZKOVATEĽ“ PODĽA ZoKB a ITVS

Zákon č. 69/2018 Z.z. **o kybernetickej bezpečnosti**:

- § 3 písm. l): Prevádzkovateľ základnej služby - orgán verejnej moci alebo osoba, ktorá prevádzkuje aspoň jednu základnú službu podľa písmena k) Zákona

Zákon č. 95/2019 Z.z. **o informačných technológiách vo verejnej správe**:

- § 2 ods. 5.: Správcom je ten orgán riadenia, ktorého za správcu informačnej technológie verejnej správy ustanoví zákon
- § 2 ods. 6.: Prevádzkovateľom je správca, osobitným predpisom ustanovený orgán riadenia alebo správcom určená osoba
- Ak zákon vo vzťahu k informačnej technológii verejnej správy správcu neustanovuje, je správcom **ten orgán riadenia, ktorý informačnú technológiu verejnej správy používa** na účely poskytovania služby verejnej správy, služby vo verejnom záujme alebo verejnej služby



Spolufinancovaný Európskou úniou

JE OBEC PREVÁDZKOVATEĽOM ZÁKLADNEJ SLUŽBY?

Sú splnené všetky kritériá §3 písm. l) Zákona 69/2018:

1. Služba je zaradená v zozname základných služieb
2. Služba závisí od sietí a informačných systémov
3. Je činnosťou aspoň v jednom sektore alebo podsektore
4. Môže byť prvkom kritickej infraštruktúry (zoznam prvkov je utajovanou skutočnosťou)

Spolufinancovaný Európskou úniou

IDENTIFIKÁCIA ZÁKLADNEJ SLUŽBY „ISVS“ PODĽA ZÁKONA č. 69/2018 Z.z.

Z Prílohy č. 1 k vyhláške č. 164/2018 Z. z. ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby) – sektor **VEREJNÁ SPRÁVA:**

Prevádzkovateľ služieb (príloha č. 1 k zákonu)	**Špecifické sektorové kritériá** (jednotlivo)	**Dopadové kritériá** (jednotlivo) Dopad kybernetického bezpečnostného incidentu v informačnom systéme alebo sieti, na ktorých fungovaní je závislé poskytovanie služby, môže spôsobiť:
Orgán verejnej moci	Služba, ktorá je na základe vyhodnotenia rizík v rámci organizácie definovaná ako podstatná služba v jednom podsektore: a) bezpečnosti, **b) informačných systémov verejnej správy,** c) obrany, d) spravodajské služby, alebo e) utajovaných skutočností vo vzťahu k fungovaniu príslušného ústredného orgánu podľa zákona.	Ohrozenie dostupnosti, pravosti, integrity alebo dôvernosti uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov, **ktoré postihuje viac ako 1 000 osôb.** Obmedzenie či narušenie prevádzky prvku kritickej infraštruktúry. Obmedzenie či narušenie prevádzky siete a informačného systému, ktoré môže mať: • negatívny vplyv na fungovanie orgánu verejnej moci, • vplyv na výkon činnosti orgánu verejnej moci pri zaisťovaní prípravy na krízové situácie, • vplyv na obmedzenie výkonu alebo ohrozenie pôsobnosti organu verejnej moci. Viac ako jedna zranená osoba vyžadujúca lekárske ošetrenie. Narušenie verejného poriadku, verejnej bezpečnosti, mimoriadnu udalosť alebo tieseň, ktorá môže vyžadovať vykonanie záchranných prác, alebo výkon činností a opatrení súvisiacich s poskytovaním pomoci v tiesni.

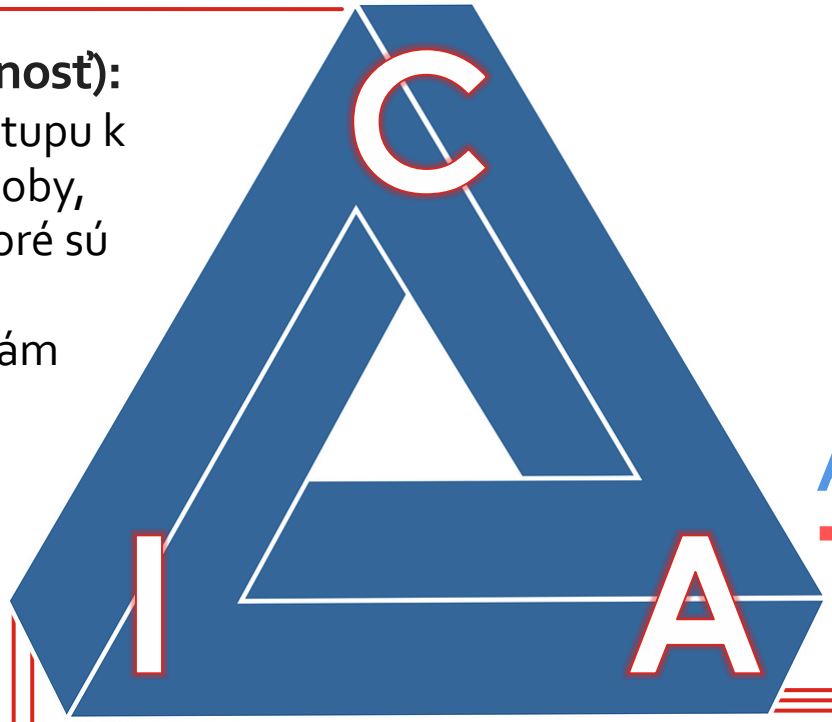
POVINNOSTI PREVÁDZKOVATEĽA ZÁKLADNEJ SLUŽBY

POŽIADAVKY KYBERNETICKEJ BEZPEČNOSTI V SAMOSPRÁVE MIEST A OBCÍ

ZÁKLADNÉ ATRIBÚTY SPOĽAHLIVOSTI INFORMÁCIÍ

Confidentiality (Dôvernosť):

- miera obmedzenia prístupu k informáciám len pre osoby, alebo skupiny osôb, ktoré sú oprávnené na prístup k príslušným informáciám



Availability (Dostupnosť)

- miera dostupnosti informácie pre používateľa a systém vo chvíli, keď je informácia potrebná a požadovaná

Integrity (Celistvosť)

- miera bezchybnosti informácie
- charakteristikami integrity sú:
  - úplnosť informácie
  - správnosť informácie

POVINNOSTI PREVÁDZKOVATEĽA ZÁKLADNEJ SLUŽBY PODĽA § 19 ZÁKONA Č. 69/2018 Z.Z.

(1)	prijať a dodržiavať všeobecné bezpečnostné opatrenia najmenej v rozsahu podľa § 20 a sektorové bezpečnostné opatrenia, ak sú prijaté.
(2)	ak sú činností vykonávané dodávateľským spôsobom, uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa zákona počas celej doby platnosti zmluvy.
(3)	informovať podnik na poskytovanie elektronických komunikačných služieb ku ktorému základná služba pripojená
(4)	informovať v nevyhnutnom rozsahu tretie strany o hlásenom kybernetickom bezpečnostnom incidente
(6a)	riešiť kybernetický bezpečnostný incident,
(6b)	bezodkladne hlásiť závažný kybernetický bezpečnostný incident,
(6c)	spolupracovať s NBÚ a ústredným orgánom pri riešení hláseného kybernetického bezpečnostného incidentu a na tento účel im poskytnúť potrebnú súčinnosť
(6d)	v čase kybernetického bezpečnostného incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní,
(6e)	oznámiť orgánu činnému v trestnom konaní alebo Policajnému zboru skutočnosti, že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka
(7)	hlásiť zmeny v údajoch podľa § 17 ods. 5 prostredníctvom jednotného informačného systému kybernetickej bezpečnosti

Spolufinancovaný Európskou úniou

DEFINÍCIA BEZPEČNOSTNÉHO OPATRENIA

Opatrenia podľa **§ 20 (1)** Zákona sú:

- **Úlohy, procesy, roly a technológie** v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov.

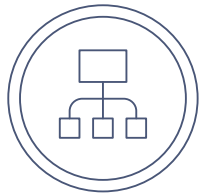
V zmysle § 19 (1) Prevádzkovateľ základnej služby je povinný do šiestich mesiacov odo dňa oznámenia o zaradení do registra prevádzkovateľov základných služieb prijať a dodržiavať:

- **Všeobecné bezpečnostné opatrenia** najmenej v rozsahu podľa §20
- **Sektorové bezpečnostné opatrenia**, ak sú prijaté

GENERICKÉ ROZDELENIE BEZPEČNOSTNÝCH OPATRENÍ

- **Technické opatrenia**
  - Opatrenia na zníženie bezpečnostných rizík pomocou prostriedkov fyzickej a technologickej povahy

- **Organizačné opatrenia**
  - Opatrenia na zníženie bezpečnostných rizík pomocou zmien procesov a úpravou dokumentácie



  - **Personálne opatrenia**
    - Podkategória organizačných opatrení týkajúcich sa riadenia ľudských zdrojov

Efektívnu bezpečnosť je možné dosiahnuť
LEN POMOCOU KOMBINÁCIE
rôznych technických a organizačných opatrení

ROZSAH BEZPEČNOSTNÝCH OPATRENÍ PODĽA KATEGÓRIE SYSTÉMOV

Bezpečnostné opatrenie podľa § 20 ods. 3 zákona	Kategória I	Kategória II	Kategória III
a) organizácia kybernetickej bezpečnosti a informačnej bezpečnosti	Odporúčané	Povinné	Povinné
b) riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti	Odporúčané	Povinné	Povinné
c) personálna bezpečnosť	Odporúčané	Povinné	Povinné
d) Riadenie prístupov	Odporúčané	Povinné	Povinné
e) riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami	Povinné	Povinné	Povinné
f) bezpečnosť pri prevádzke informačných systémov a sietí	Odporúčané	Povinné	Povinné
g) hodnotenie zraniteľností a bezpečnostné aktualizácie	Odporúčané	Povinné	Povinné
h) ochrana proti škodlivému kódu	Odporúčané	Povinné	Povinné
i) sieťová a komunikačná bezpečnosť	Odporúčané	Odporúčané	Povinné
j) akvizícia, vývoj a údržba informačných sietí a informačných systémov	Odporúčané	Odporúčané	Povinné
k) zaznamenávanie udalostí a monitorovanie	Povinné	Povinné	Povinné
l) fyzická bezpečnosť a bezpečnosť prostredia	Odporúčané	Odporúčané	Povinné
m) riešenie kybernetických bezpečnostných incidentov	Povinné	Povinné	Povinné
n) kryptografické opatrenia	Odporúčané	Odporúčané	Povinné
o) kontinuita prevádzky	Odporúčané	Odporúčané	Povinné
p) audit, riadenie súladu a kontrolné činnosti	Odporúčané	Povinné	Povinné
Manažér kybernetickej bezpečnosti (§ 20 ods. 4 písm. a) zákona)	Povinné	Povinné	Povinné

Príloha č. 3 k vyhláške č. 362/2018 Z. z. vo verzii predpisu účinnej od 01.9.2023

Spolufinancovaný Európskou úniou

KATEGORIZÁCIA BEZPEČNOSTNÝCH OPATRENÍ PRE ITVS

Vyhláška č. 179/2020 Z.z. ÚPVII ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy:

§ 2 Bezpečnostné opatrenia

1. Bezpečnostné opatrenia informačných technológií verejnej správy tvoria **minimálne bezpečnostné opatrenia** rozdelené do **Kategórie I, Kategórie II** a **Kategórie III** pre jednotlivé oblasti podľa prílohy č. 2.
2. Pri duplicite alebo nekompatibilite minimálnych bezpečnostných opatrení rôznych kategórií, ktoré môžu byť aplikované na konkrétne informačné technológie verejnej správy, majú prednosť ustanovenia upravujúce opatrenia vyššej kategórie.
3. Ak sa aplikuje bezpečnostné opatrenie aj podľa osobitného predpisu, aplikuje sa bezpečnostné opatrenie podľa zákona, **ak jeho cieľom je dosiahnuť vyššiu úroveň bezpečnosti** sietí a informačných systémov ako podľa osobitného predpisu.
4. Bezpečnostný projekt informačných systémov verejnej správy sa vypracuje a implementuje podľa prílohy č. 3.

APLIKÁCIA POVINNOSTÍ V SAMOSPRÁVE

Obec, ktorá je aj krajským mestom,

Samosprávny kraj

- Vzťahujú sa na ňu minimálne bezpečnostné opatrenia Kategórie I a Kategórie II a a Kategórie III
- Ako PZS implementuje bezpečnostné opatrenia podľa zákona č. 69/2018 Z.z.

Obec nad 6000 obyvateľov,

Obec so štatútom mesta nad 6000 obyvateľov okrem krajských miest,

Mestská časť s právnou subjektivitou

- Vzťahujú sa na ňu minimálne bezpečnostné opatrenia Kategórie I a Kategórie II
- Ako PZS implementuje bezpečnostné opatrenia podľa zákona č. 69/2018 Z.z.

Obec do 6000 obyvateľov,

Obec so štatútom mesta do 6000 obyvateľov

- Vzťahujú sa na ňu minimálne bezpečnostné opatrenia Kategórie I
- Ako PZS implementuje bezpečnostné opatrenia podľa zákona č. 69/2018 Z.z.

Obec do 1000 obyvateľov

- Vzťahujú sa na ňu minimálne bezpečnostné opatrenia Kategórie I
- alebo implementuje bezpečnostné opatrenia podľa zákona č. 69/2018 Z.z. ak ich cieľom je dosiahnuť vyššiu úroveň bezpečnosti

POŽIADAVKY NA KVALIFIKÁCIU

POŽIADAVKY KYBERNETICKEJ BEZPEČNOSTI V SAMOSPRÁVE MIEST A OBCÍ

EURÓPSKY RÁMEC ROLÍ V KB

- Zodpovednosť osôb konajúcich v kontexte kybernetickej bezpečnosti v organizácii má byť zadefinovaná jednoznačne, prostredníctvom rolí, v ktorých osoba vystupuje vo vzťahu k sieti alebo informačnému systému
- S rolami je spojená množina povinností a oprávnení pri inicializácii, návrhu, vývoji, používaní a prevádzke siete alebo informačného systému
- Znalostné štandardy pre určitú rolu sú splnené aj kolektívne ich vzájomným zdieľaním.
- Názvy pracovných pozícií a ich pracovných náplní určuje prevádzkovateľ základnej služby

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

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 〉

RÁMEC A CIEĽOVÉ SKUPINY VZDELÁVANIA V KB

Druh ďalšieho vzdelávania	Cieľová skupina	Typické dotknuté roly
Ďalšie odborné vzdelávanie	IB/KB	manažér KB, audítor KB, architekt KB, špecialista KB, analytik KB…
Upskilling, teoretické základy KB	Informatici	IT manažér, 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

Spolufinancovaný Európskou úniou

TVORBA KVALIFIKAČNÉHO ŠTANDARDU

a) **vedomosti** - poznatky nadobudnuté v priebehu vzdelávania, učenia sa alebo skúsenosťou

b) **zručnosti** - schopnosti jednotlivca uplatňovať vedomosti a využívať vedomosti na plnenie rôznych úloh a riešenie problémov

c) **kompetencie** - preukázané schopnosti jednotlivca použiť vedomosti, zručnosti a osobné, sociálne a/alebo metodologické schopnosti v pracovných alebo študijných situáciách a v odbornom a osobnom rozvoji

d) **kvalifikácia** - súhrn odborných vedomostí, zručností a kompetencií, ktoré sú potrebné na vykonávanie určitej pracovnej činnosti alebo pracovných činností

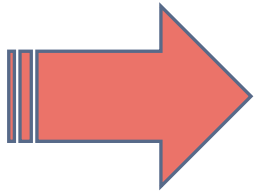
MANAŽÉR KYBERNETICKEJ BEZPEČNOSTI

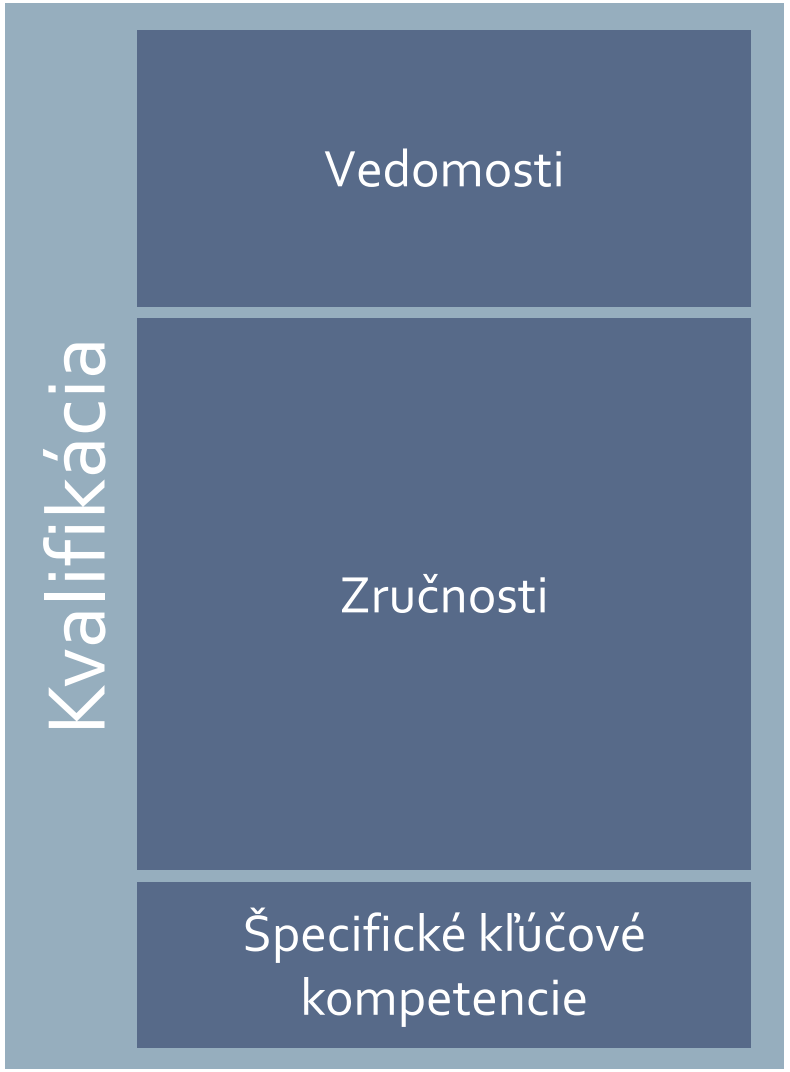
POŽIADAVKY KYBERNETICKEJ BEZPEČNOSTI V SAMOSPRÁVE MIEST A OBCÍ

VYŽADOVANÁ KVALIFIKÁCIA MKB

Príloha č. 5 k Vyhláške NBÚ č. 492/2023 Z.z. ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti:

- Riadenie bezpečnosti
- Riadenie hrozieb a rizík
- Aplikácia bezpečnostných opatrení
- Výkon operatívnych bezpečnostných činností
- Riadenie súladu





STRUČNÁ CHARAKTERISTIKA A POPIS PRACOVNÝCH ÚLOH MKB PODĽA NÁRODNÉHO ŠTANDARDU ZAMESTNANIA

- **Zaisťuje ochranu informačných aktív organizácie implementáciou a riadením procesov informačnej a kybernetickej bezpečnosti**.
- **Organizuje výkon činností organizácie súvisiacich so zaručením bezpečnosti informačných aktív v zmysle najlepšej praxe,** najmä:
  - koncepčne riadi informačnú bezpečnosť organizácie (tzv. „Information Security Governance")
  - implementuje a zabezpečuje riadny chod procesov manažmentu bezpečnostných rizík a ošetrovania bezpečnostných hrozieb
  - navrhuje a prezentuje bezpečnostné stratégie a koncepty
  - riadi návrhy, zmeny a optimalizáciu bezpečnostných riešení s víziou a konceptom ich bežného prevádzkovania
  - riadi návrhy a integráciu bezpečnostných technológií s cieľom tvorby efektívnych bezpečnostných opatrení na ochranu poskytovaných služieb organizácie
  - zabezpečuje implementáciu technických a organizačných bezpečnostných opatrení
  - z pozície garanta resp. z pozície projektového manažéra vedie bezpečnostné projekty, napr. implementáciu nových bezpečnostných technológií do prostredia organizácie
  - riadi informačnú bezpečnosť vo vzťahu s dodávateľmi a pri zaobstarávaní, projektovaní a vývoji softvéru a systémov
  - riadi bezpečnostnú architektúru organizácie, vypracúva odborné stanoviská k novým zmenám v IT infraštruktúre organizácie, ktoré môžu mať potenciálny vplyv na bezpečnosť informačných aktív organizácie
  - zabezpečuje riadenie informačných aktív organizácie v kontexte zaručenia ich bezpečnosti (tzv. IT Asset Management)
  - zabezpečuje návrh a aplikáciu metodík pre klasifikáciu informačných aktív a kategorizáciu sietí a informačných systémov
  - zabezpečuje návrh metodík a riadi procesy obnovy prevádzkových činnosti (tzv. Business Continuity Management), vrátane metodík a riadenia procesov plánovania obnovy systémov po havárii (tzv. Disaster Recovery Planning)
  - navrhuje metriky a kľúčové indikátory pre sledovanie vývoja a stavu bezpečnosti a vývoja bezpečnostných rizík (KPI, KRI)
  - zabezpečuje hodnotenie technických zraniteľností systémov
  - zabezpečuje a riadi procesy detekcie, riešenia a prevencie kybernetických bezpečnostných incidentov
  - zabezpečuje budovanie bezpečnostného povedomia pre oblasť informačnej a kybernetickej bezpečnosti a ochrany osobných údajov
  - zabezpečuje tvorbu a aktualizáciu interných bezpečnostných politík, štandardov a procedúr organizácie
  - zabezpečuje vyhodnocovanie plnenia vnútorných predpisov súvisiacich s riadením bezpečnosti informačných aktív
  - zabezpečuje poskytovanie súčinnosti internému a externému auditu informačnej a kybernetickej bezpečnosti,
  - riadi procesy zaručenia súladu (tzv. compliance management) v oblasti informačnej a kybernetickej bezpečnosti

POŽIADAVKY NA SPÔSOBILOSŤ MANAŽÉRA KB

Príloha č. 5 k Vyhláške NBÚ č. 492/2023 Z.z. ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti

Minimálna požadovaná odborná prax:

Úplné stredné všeobecné alebo úplné stredné odborné	VŠ I. stupňa (bakalárske štúdium)	VŠ 2. stupňa (inžinierske, alebo magisterské štúdium)	VŠ 3. stupňa (doktorandské, alebo postgraduálne štúdium)
• najmenej **7 rokov** praxe v oblasti informačných technológií	• najmenej **5 rokov** praxe v oblasti informačných technológií	• najmenej **3 roky** praxe v oblasti informačných technológií	• najmenej **3 roky** praxe v oblasti informačných technológií
• z toho najmenej **5 rokov** praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT	• z toho najmenej **3 roky** praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT	• z toho najmenej **1 rok** praxe v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT	• 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**

Certifikácia manažéra kybernetickej bezpečnosti

- Manažéri kybernetickej bezpečnosti sú certifikovaní v zmysle zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti, podľa certifikačnej schémy overovania odbornej spôsobilosti manažéra kybernetickej bezpečnosti
- Certifikačná schéma je záväzná pre všetky akreditované orgány posudzovania zhody, v súlade s STN EN ISO/IEC 17024: 2013 Posudzovanie zhody – Všeobecné požiadavky na orgány vykonávajúce certifikáciu osôb

POŽIADAVKY NA SPÔSOBILOSŤ MANAŽÉRA KB

Špecifické kľúčové kompetencie:

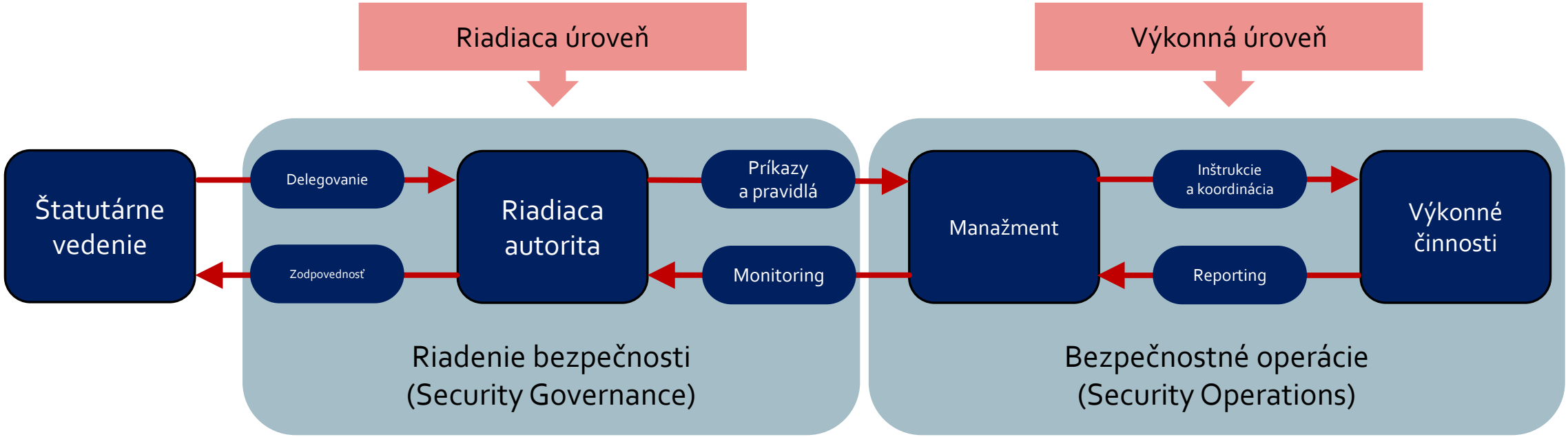
a) schopnosť prijímať rozhodnutia
b) schopnosť myslieť a konať v súvislostiach
c) schopnosť riešiť konflikty
d) schopnosť poskytovať spätnú väzbu
e) schopnosť delegovať úlohy
f) schopnosť podporovať procesy vzdelávania a odovzdávania znalostí
g) schopnosť viesť pracovný tím
h) schopnosť organizovania a plánovania práce
i) analytické myslenie
j) strategické a koncepčné myslenie
k) tvorivosť (kreativita)
l) prezentačná zručnosť

POŽIADAVKY NA SPÔSOBILOSŤ MANAŽÉRA KB V NÁRODNOM ŠTANDARDE ZAMESTNANIA

Všeobecné kľúčové kompetencie:

- Digitálna gramotnosť
- Ekonomická a finančná gramotnosť
- Komunikačné kompetencie – cudzí jazyk
- Komunikačné kompetencie – štátny/materinský jazyk
- Matematická gramotnosť
- Mediálna gramotnosť
- Občianske kompetencie
- Osobnostné a emocionálne kompetencie
- Schopnosť učiť sa
- Sociálne kompetencie
- Technická gramotnosť

KĽÚČOVÉ ROLE A VZŤAHY V RIADENÍ A VÝKONE BEZPEČNOSTI



Zdroj: ISACA, isaca.org/cobit5

Spolufinancovaný Európskou úniou

MANAŽÉR KB AKO SLUŽBA

- V zmysle Obchodného zákonníka je **štatutárny orgán spoločnosti povinný konať s odbornou starostlivosťou, v súlade so záujmami spoločnosti,** pričom zodpovedá za porušenie týchto povinností. Obdobne to platí aj pre starostov obcí a primátorov miest, ktorým táto zodpovednosť vyplýva z osobitných právnych predpisov (napr. zákon o obecnom zriadení)
- Zodpovednosť za riadenie kybernetickej bezpečnosti je potrebné vnímať v dvoch samostatných kontextoch, pričom tieto zodpovednosti si nie je možné zamieňať:
  - **A. zákonnú zodpovednosť** - zodpovednosť štatutárneho orgánu vyplývajúcu zo všeobecne záväzných právnych predpisov; nie je možné outsourcovať, resp. outsourcing štatutárny orgán zákonnej zodpovednosti nezbaví
  - **B. zmluvnú zodpovednosť** - výkon niektorých úloh v kybernetickej bezpečnosti; je možné obstarať aj ako službu vykonávanú dodávateľským spôsobom
- **Riadenie parametrov služby**:
  - parametre dodávanej služby musia byť merateľné a malo by byť možné zazmluvniť ich prostredníctvom dohody o úrovni služieb (SLA)
  - porušenie parametrov uvedených v SLA môže byť riešené vopred dohodnutým znížením platieb alebo automatickou zmluvnou pokutou, a to nezávisle od toho, či vznikla škoda
- **Zákonné zodpovednosti nie je možné zmluvne preniesť na tretiu stranu, ani sa ich efektívne vzdať**. Zmluva s dodávateľom služby nepredstavuje nahradenie zákonných zodpovednostných vzťahov a ich prenos na tretiu osobu

NCC-SK

SLOVAKIA CYBERSECURITY COORDINATION CENTRE

Financované Európskou úniou

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.

www.cybercompetence.sk, kyberkomunita.sk

www.linkedin.com/company/cybercompetence

@CybercenterSk