Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

NCC-SK
SLOVAKIA CYBERSECURITY COORDINATION CENTRE

Najčastejšie zistenia auditu v zdravotníckych zariadeniach

Pavol Dovičovič

30.11.2023

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

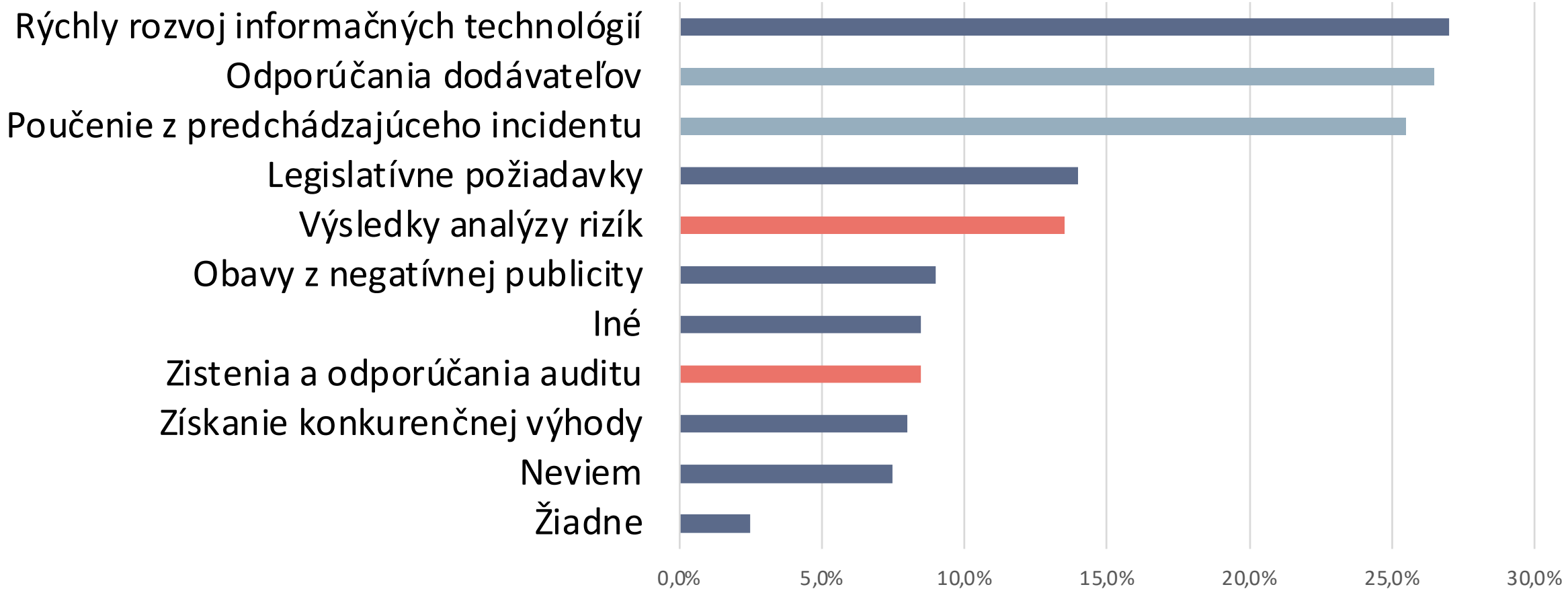
Spolufinancovaný Európskou úniou

Prečo kybernetická bezpečnosť

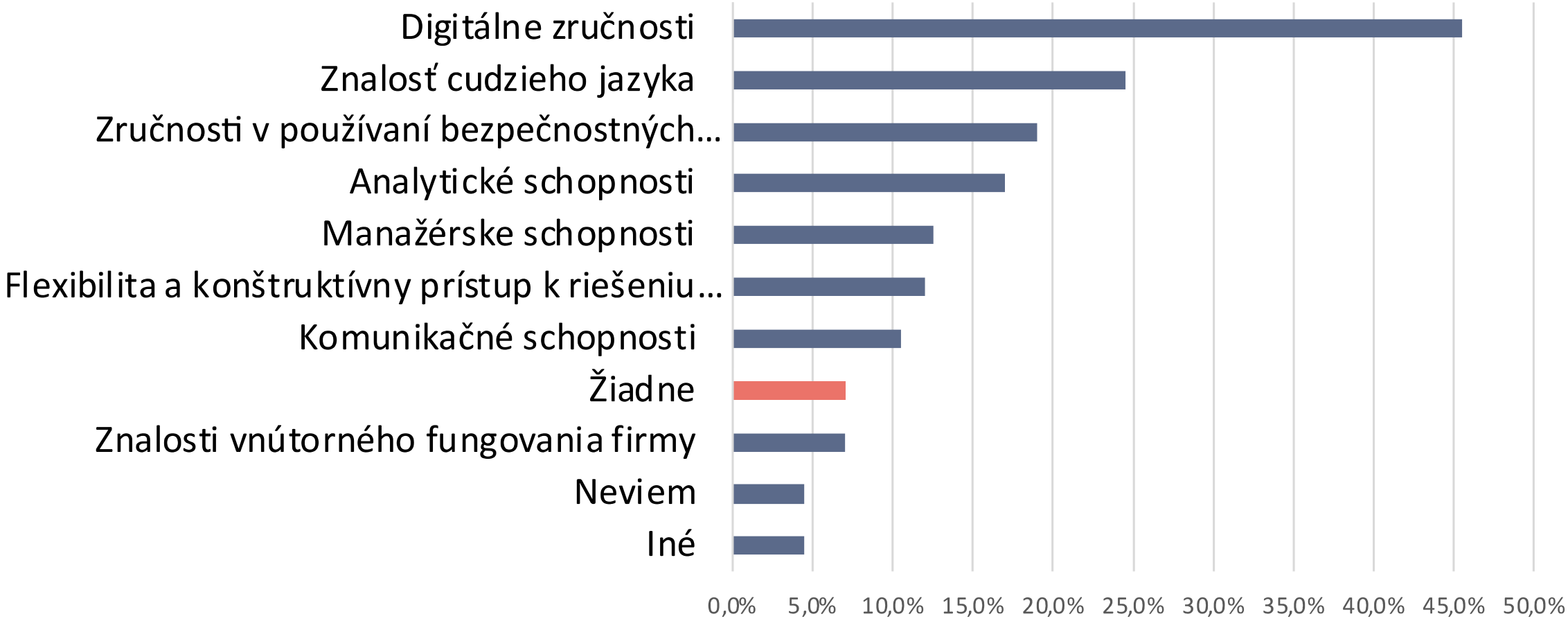
POŽIADAVKY KYBERNETICKEJ BEZPEČNOSTI

PREČO ORGANIZÁCIE ZAVÁDZAJÚ PROCESY KYBERBEZPEČNOSTI?

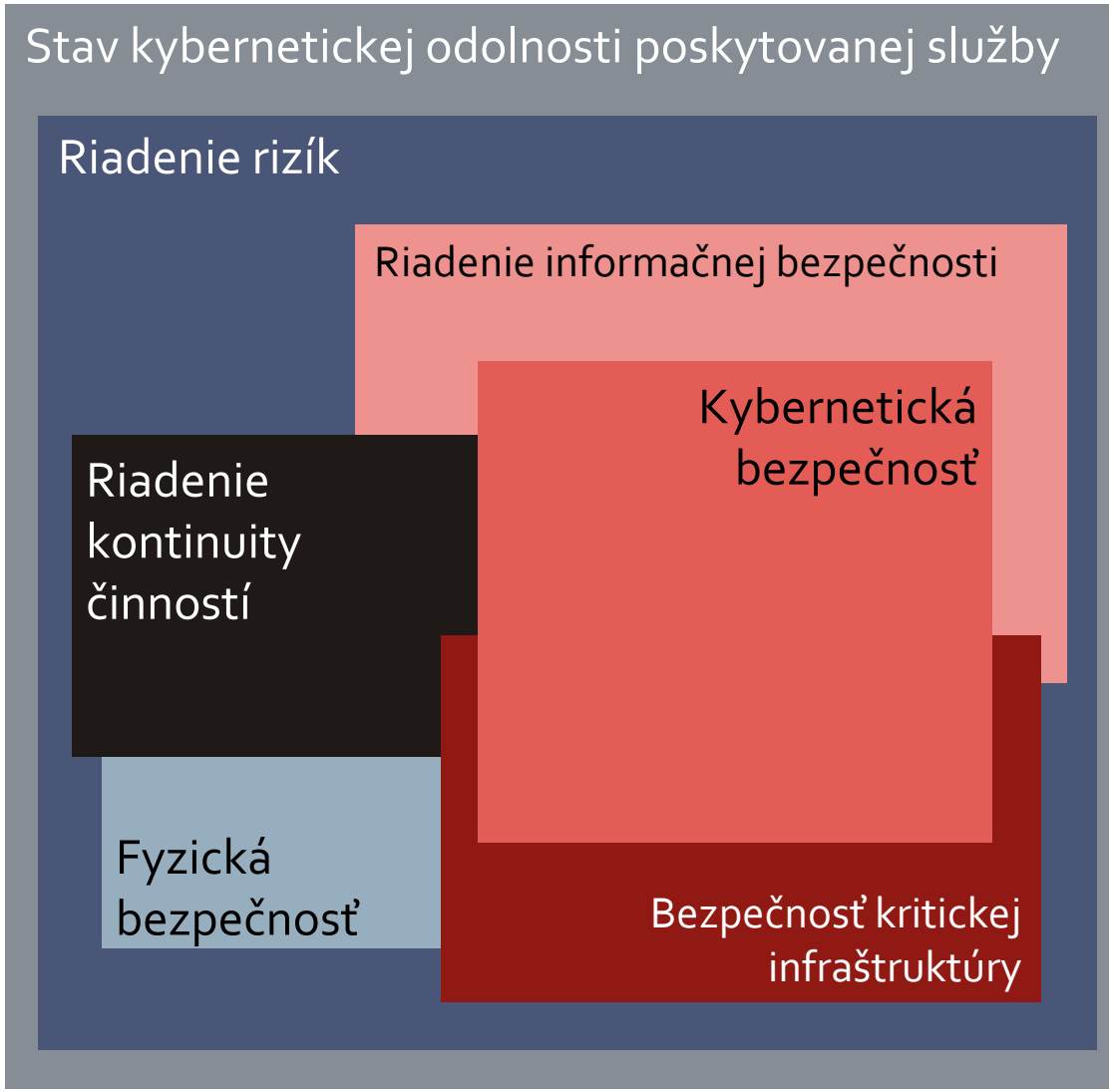
Otázka z prieskumu: Aké faktory majú vo vašej organizácii najvyšší vplyv na zvyšovanie úrovne kybernetickej bezpečnosti?



KTORÉ ZNALOSTI A SKÚSENOSTI ZAMESTNANCOV POVAŽUJETE MOMENTÁLNE NAJVIAC ZA NEDOSTATKOVÉ?



BEZPEČNOSTNÉ DOMÉNY

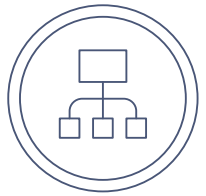


Organizácia	Technologické prostredie
Ochrana údajov	Klasifikácia informácií
Riadenie IT rizík	Manažment zraniteľností
Havarijné plánovanie	Security Governance
IT architektúra	Riadenie aktív
Riadenie prístupov	Riadenie zmien a konfigurácií
Riešenie incidentov	Service Level Management
Vzťahy a komunikácia	Biznis architektúra
Ekosystém partnerov	Vzdelávanie a povedomie

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

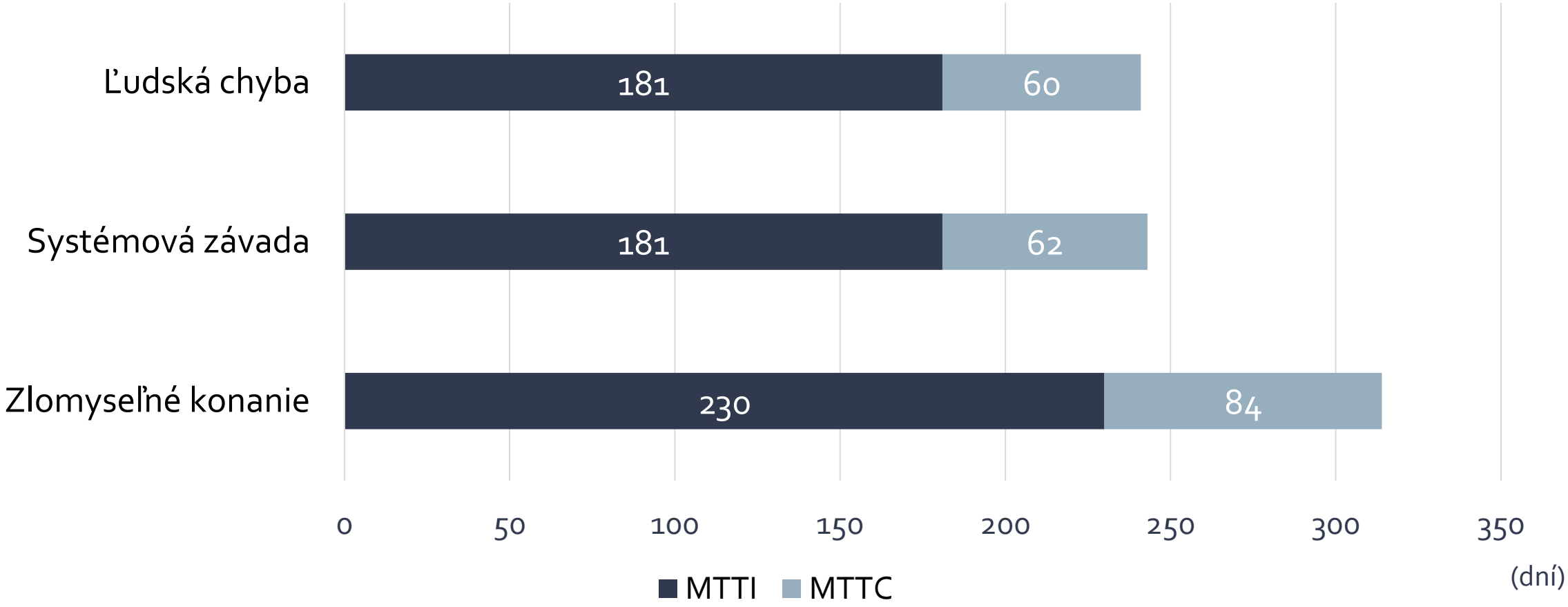


  - **Personálne opatrenia**
    - Podkategória organizačných opatrení týkajúcich sa riadenia ľudských zdrojov

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

KOĽKO TRVÁ BEŽNÝ INCIDENT?

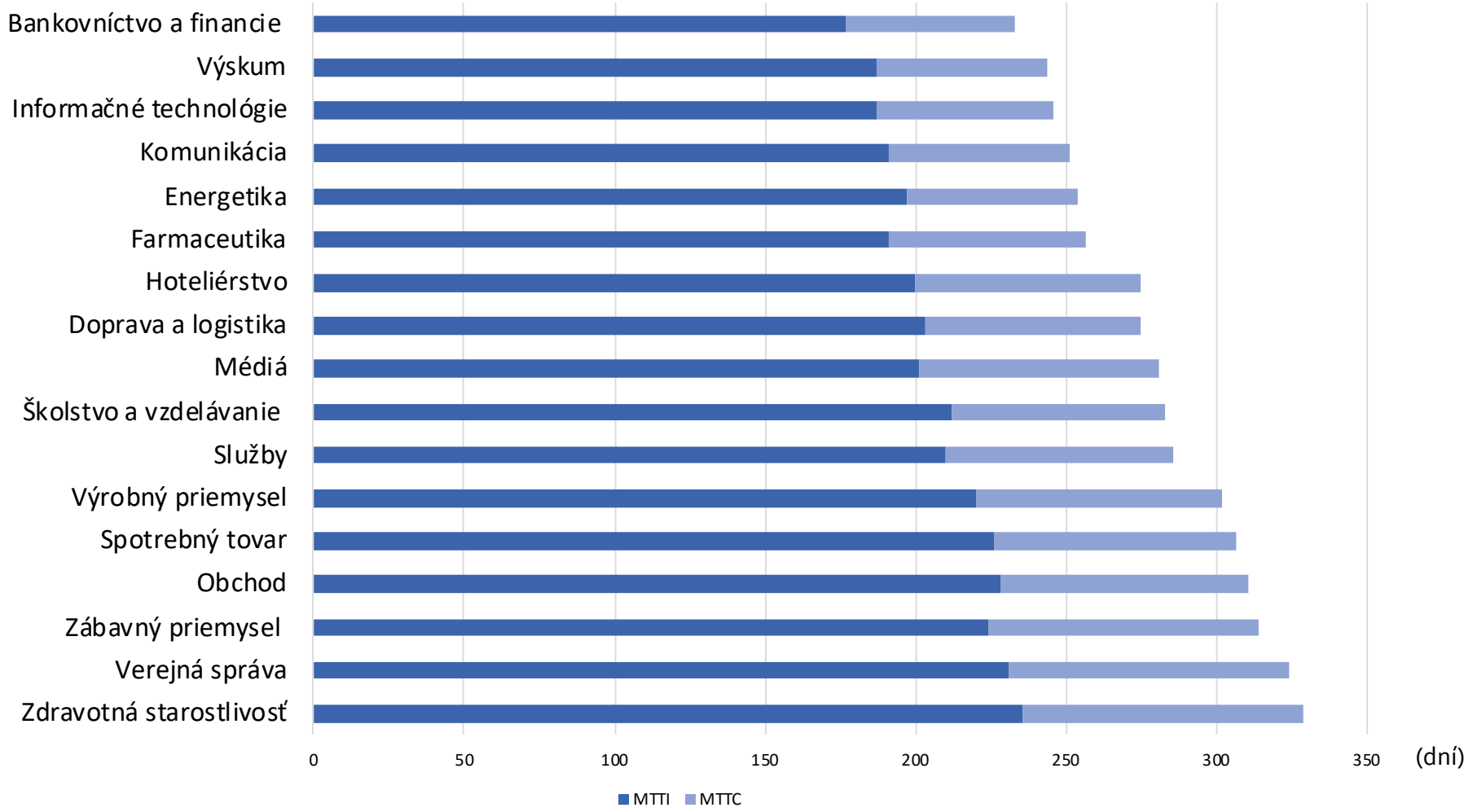
MTTI - Mean Time to Identify, **MTTC -** Mean Time to Correct



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

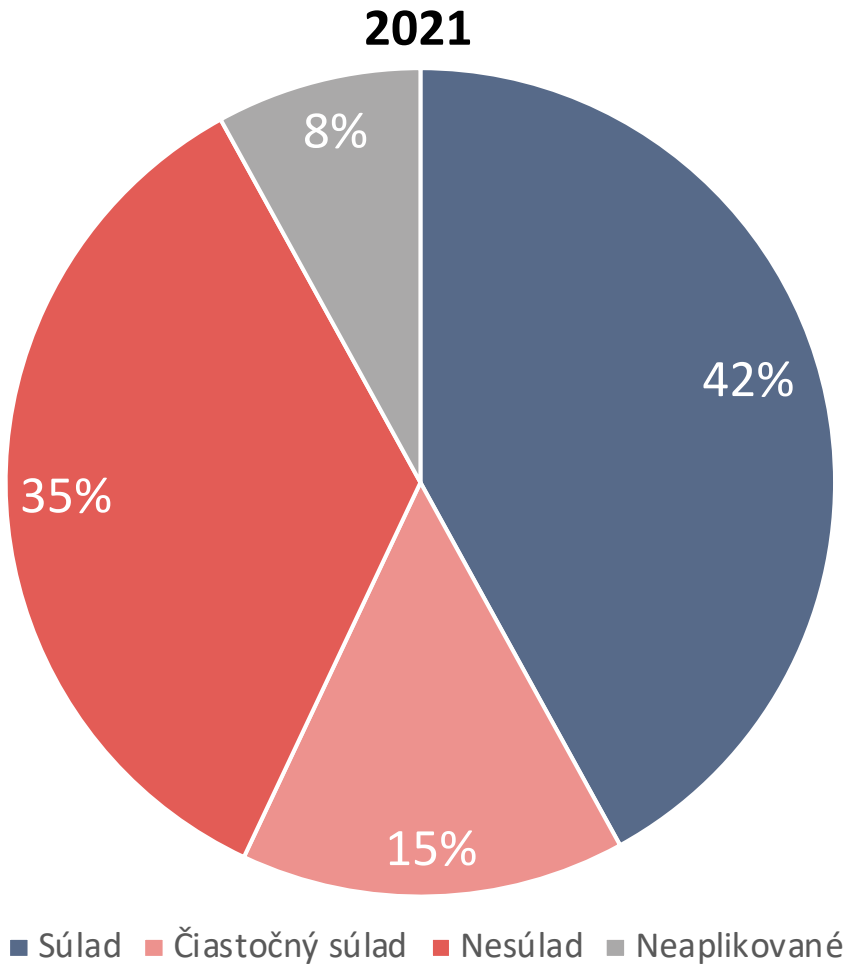


Zdroj: Ponemon Institute LLC: The Cost of a Data Breach Report

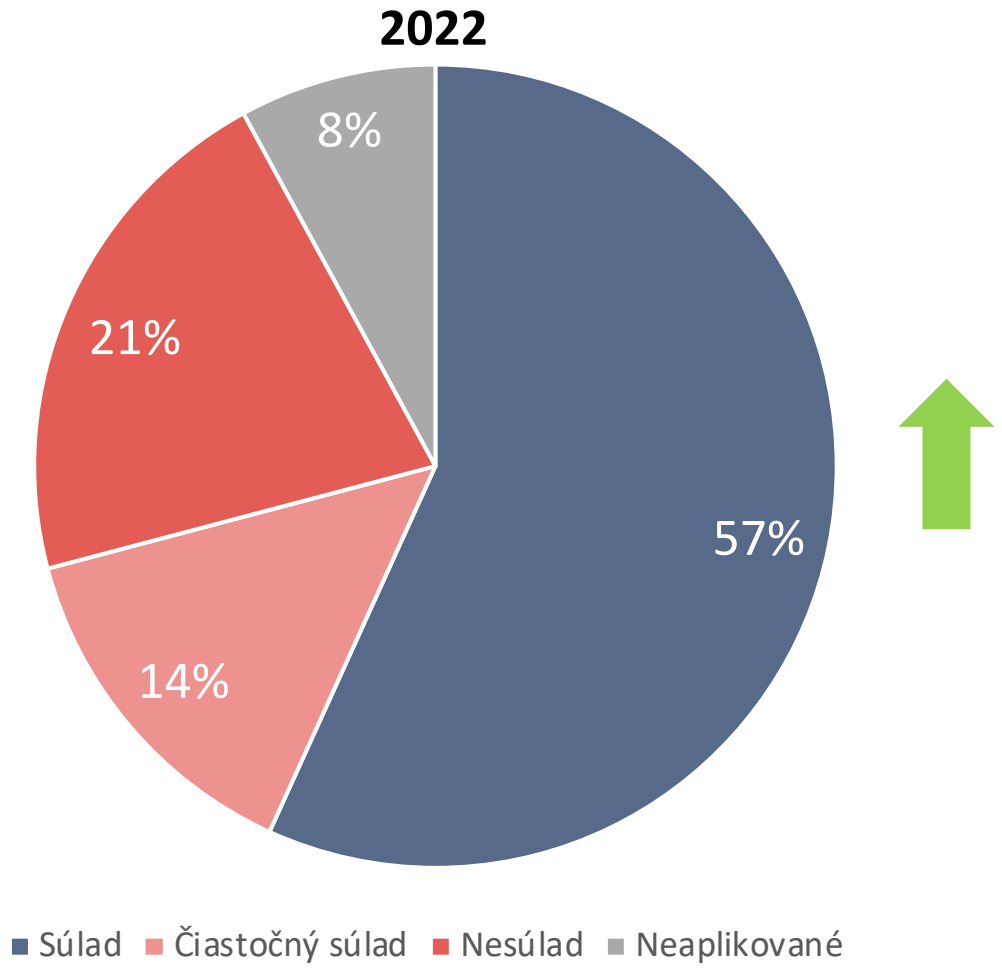
NEEXISTUJE SUBJEKT, KTORÝ BY MAL KOMPLEXNÝ PREHĽAD O STAVE KYBERNETICKEJ BEZPEČNOSTI NA SLOVENSKU

Zrejme najpresnejší objektívny prehľad má v súčasnosti NBÚ, prostredníctvom záverečných správ auditu kybernetickej bezpečnosti, v zmysle §29 Zákona č. 69/2018 Z.z.

CELKOVÁ PRIEMERNÁ MIERA SÚLADU V SR



Zdroj: Doručené správy auditu 2022, NBÚ

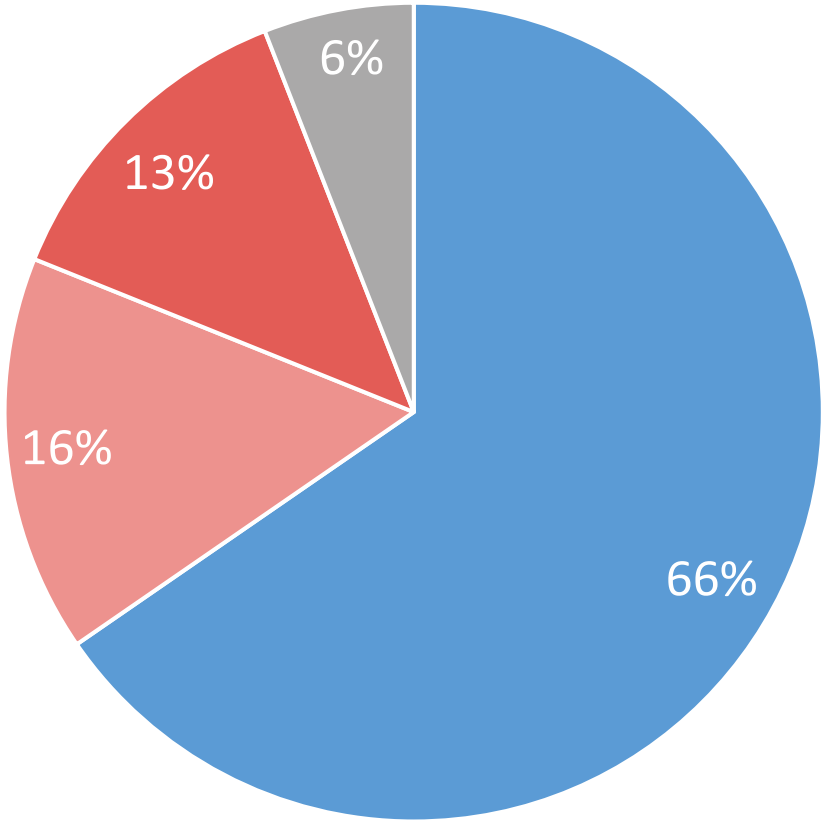


Zdroj: Doručené správy auditu 2023, NBÚ

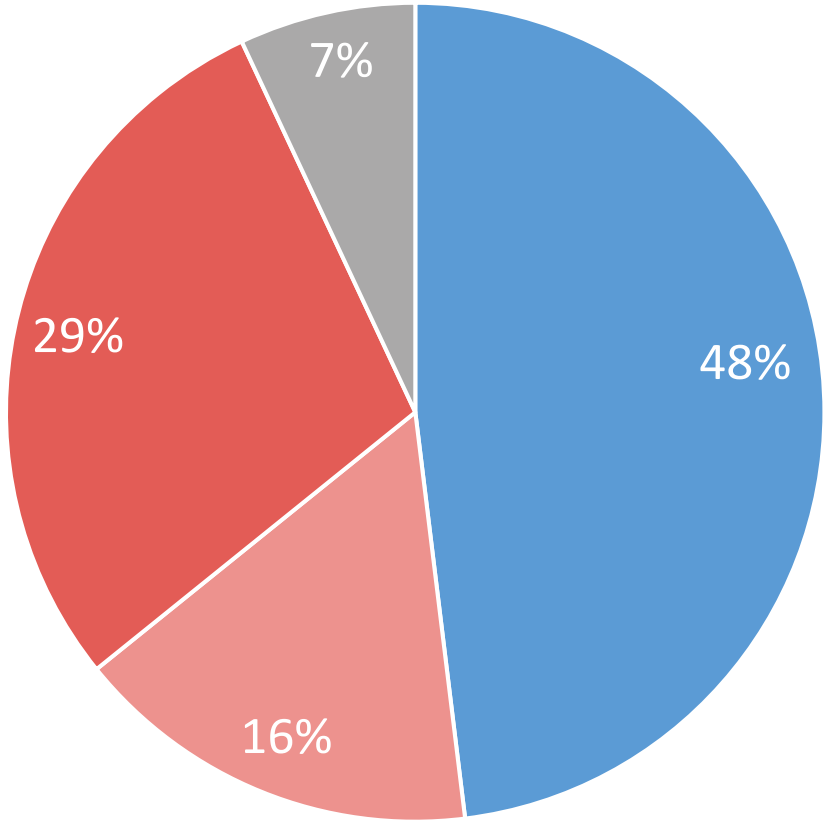
Spolufinancovaný Európskou úniou

STAV SÚLADU PODĽA TYPU VLASTNÍCTVA

Typicky PZS v súkromnom vlastníctve

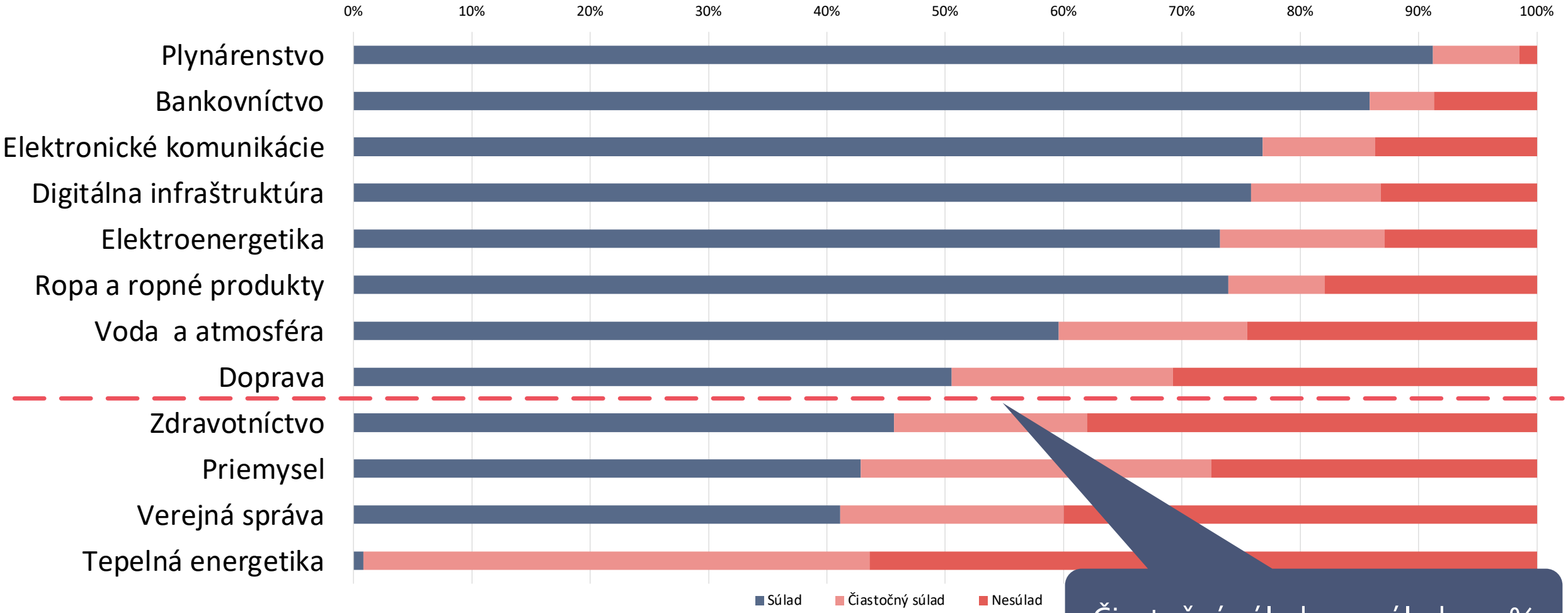


Typicky PZS vo verejnom vlastníctve



Spolufinancovaný Európskou úniou

STAV SÚLADU PODĽA ODVETVÍ (2022)



Zdroj: Doručené správy auditu 2022, NBÚ

Spolufinancovaný Európskou úniou

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

NEGATÍVNY ZÁVER

- Aj koncom roka 2023 je stav KB na Slovensku stále nejasný
  - Nie všetci „veľkí" PZS (systémy kat III.) vykonali audity
  - Nie všetci „malí" PZS (systémy kat I. a II.) odoslali samohodnotenia
- Jednotlivci preceňujú svoje prispenie a spôsobilosti
- 54 % organizácií tvrdí, že nezaznamenali kybernetický bezpečnostný incident ☺
- 68% organizácií nemá vypracované a pripravené plány kontinuity činnosti (!)
- Tretina organizácií nedáva zamestnancom možnosti na zvyšovanie ich spôsobilostí v kybernetickej bezpečnosti
- Iba polovica organizácií má vyčlenený rozpočet na kybernetickú bezpečnosť (väčšinu pokrývajú náklady na HW a SW)

Zlá situácia dlhodobo pretrváva v sektoroch
tepelná energetika, zdravotníctvo a verejná správa

POZITÍVNY ZÁVER

- Najvyšší vplyv na zvyšovanie úrovne kybernetickej bezpečnosti má uvedomenie si hodnoty rizík a hrozba incidentu
- Subjekty, ktoré nie sú povinnými osobami, vyvíjajú viac úsilia pre KB, než PZS...
- KB sa dostáva na program vedenia organizácií
- PZS sa systematicky zlepšujú v miere súladu, t.j. venujú sa implementácií opatrení
- Dramaticky rastie záujem o vzdelávanie v KB

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