



Kompetenčné
a certifikačné
centrum
kybernetickej
bezpečnosti

Ako zmenil audit vnímanie kybernetickej bezpečnosti?

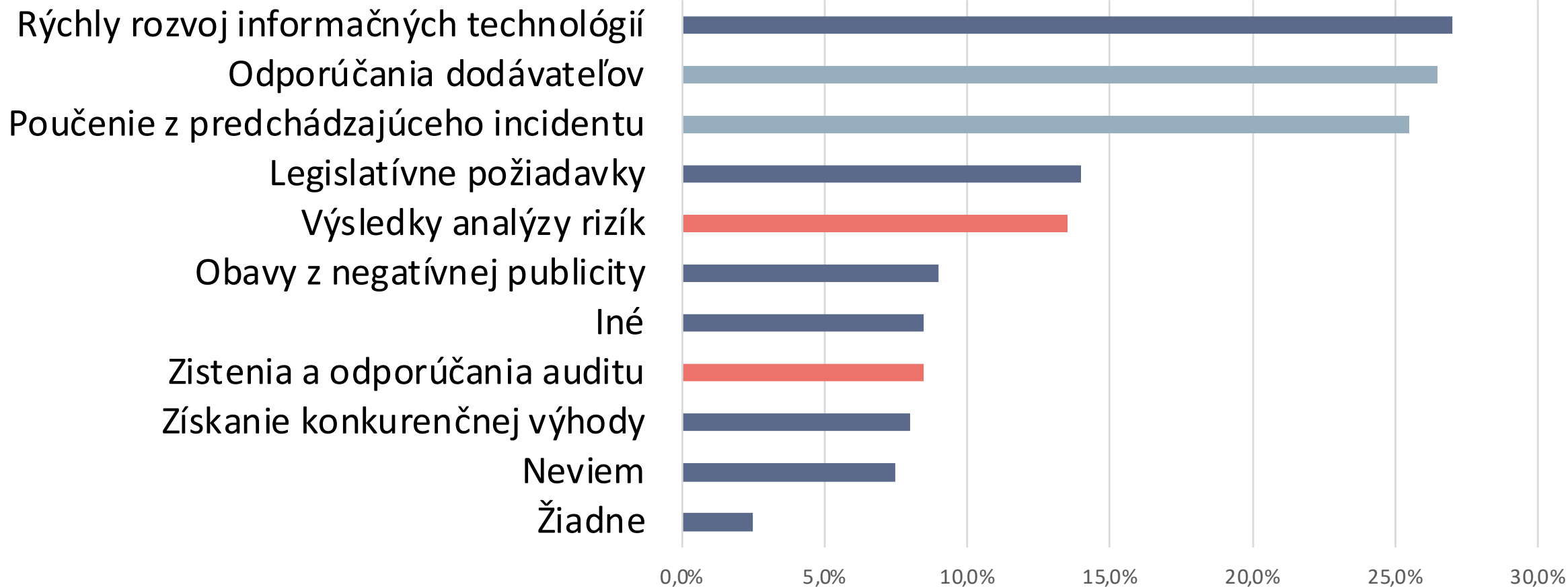
Ing. Tomáš Hettych, CISA, CISM, CGEIT, CRISC, CDPSE

COO KCCCKB

22.11.2023

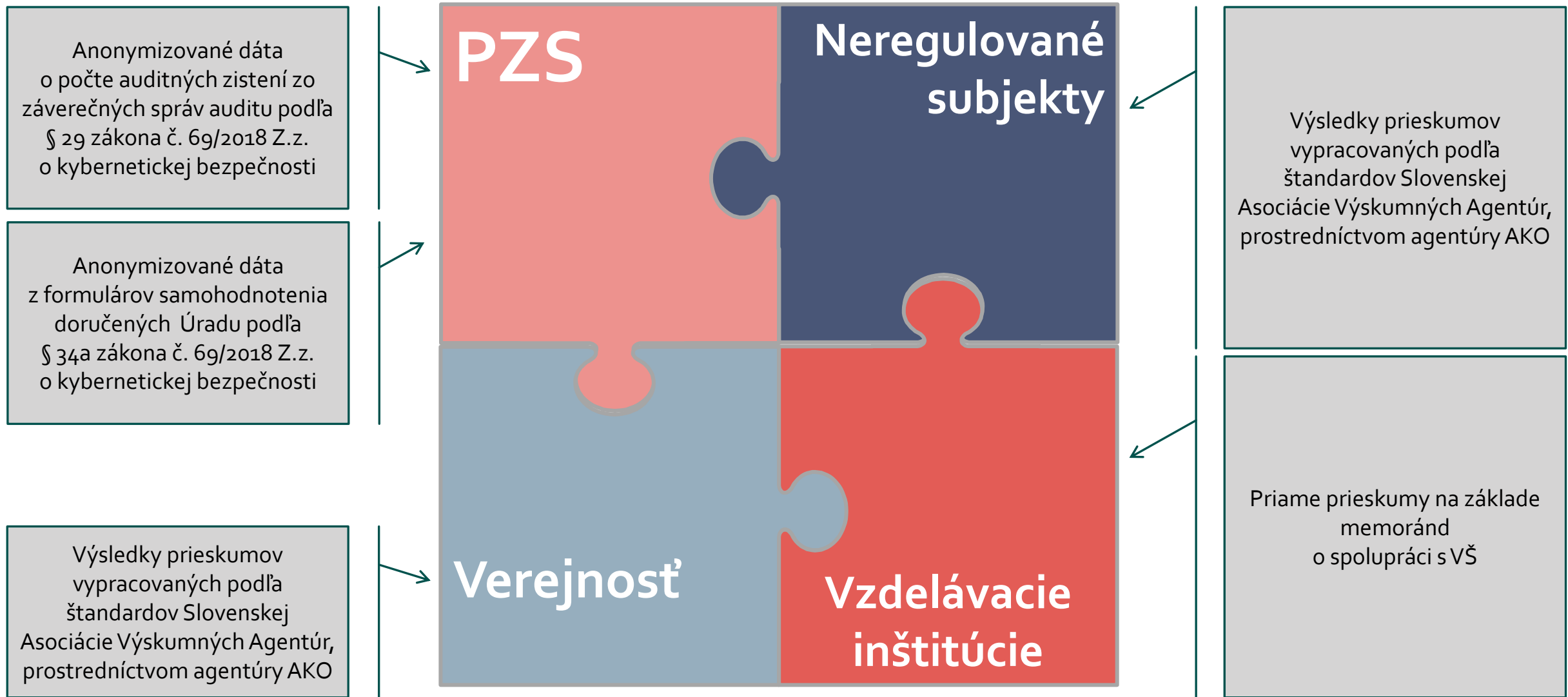


AKÉ FAKTORY MAJÚ NAJVYŠŠÍ VPLYV NA ZVYŠOVANIE ÚROVNE KYBERNETICKEJ BEZPEČNOSTI?





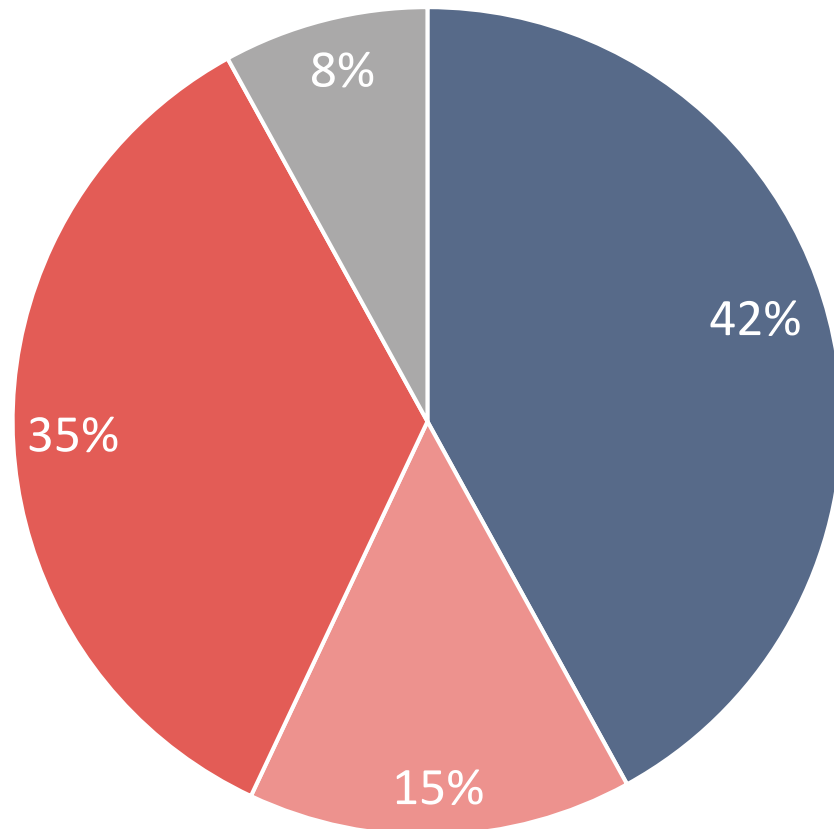
Z AKÝCH ZDROJOV VYCHÁDZAME?





CELKOVÁ PRIEMERNÁ MIERA SÚLADU V SR

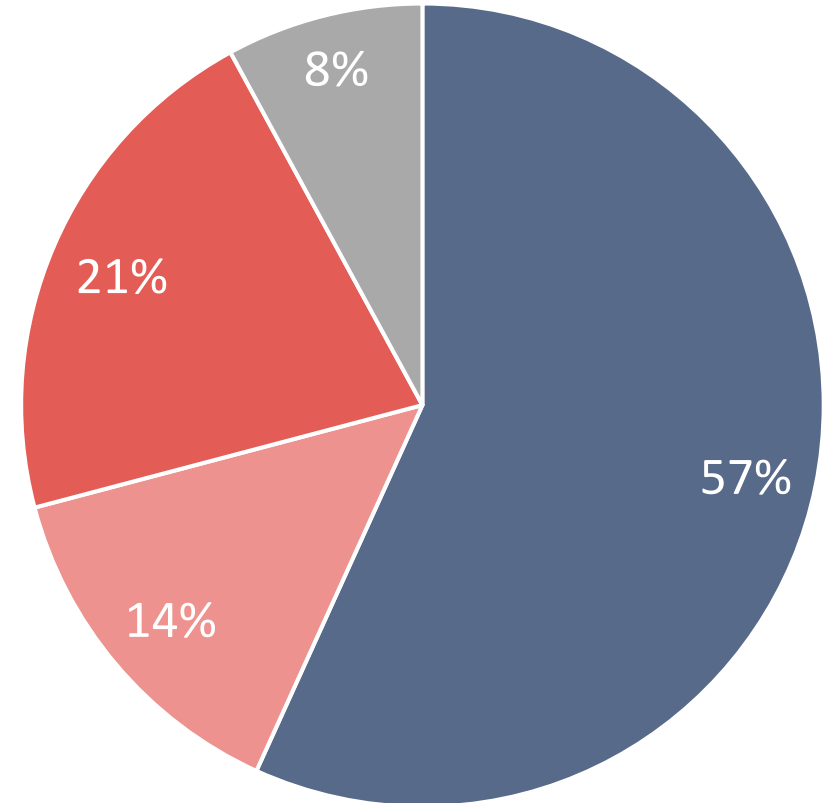
2021



■ Súlad ■ Čiastočný súlad ■ Nesúlad ■ Neaplikované

Zdroj: Doručené správy auditu 2022, NBÚ

2022

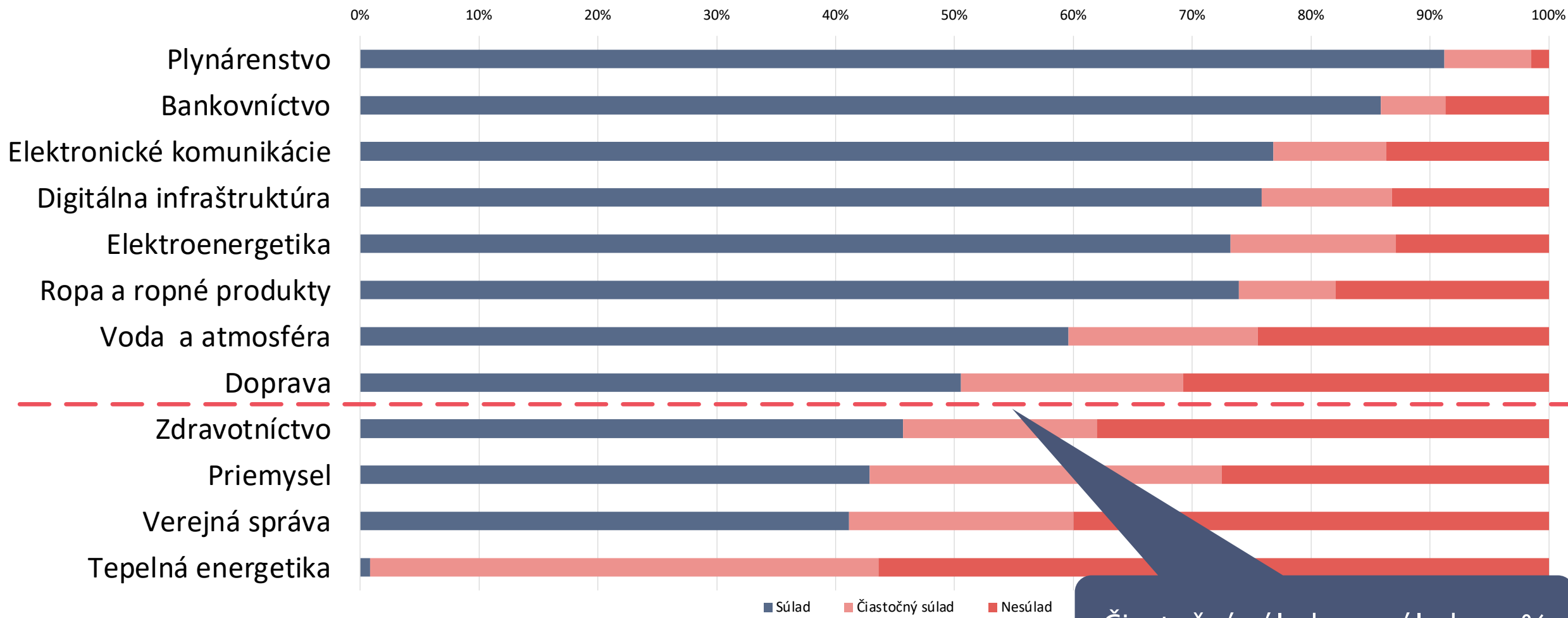


■ Súlad ■ Čiastočný súlad ■ Nesúlad ■ Neaplikované

Zdroj: Doručené správy auditu 2023, NBÚ



STAV SÚLADU PODĽA ODVETVÍ (2022)



Zdroj: Doručené správy auditu 2022, NBÚ

Čiastočný súlad + nesúlada > 50%



NAJČASTEJŠIE NÁLEZY AUDITU



Riadenie bezpečnosti (Security governance):

- Nedostatočná podpora vedenia
- Nie je definovaná štruktúra riadenia, výkonu a kontroly v oblasti KB
- Zodpovednosť za aktíva, hrozby a riziká
- Neexistencia analýzy rizík a analýzy dopadov
- Nedostatočná, alebo stále chýbajúca bezpečnostná dokumentácia
- Nezávislosť riadenia KB od riadenia IT
- Vzdelávanie v oblasti informačnej bezpečnosti
- Neformálne riadenie prevádzky a bezpečnosti 3.stranou

Výkon bezpečnosti (Security operations):



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



Ako zmenil audit vnímanie kybernetickej bezpečnosti?

Negatívny záver

- Nie všetci PZS vykonali audity a samohodnotenia
- 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)

Pozitívny záver

- Najvyšší vplyv na zvyšovanie úrovne kybernetickej bezpečnosti majú výsledky analýzy rizík, analýzy dopadov a hrozba incidentu
- Niektoré 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 jednotlivcov 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.

Ochrana vlastníckych práv

Všetky autorské práva k tomuto dokumentu sú vyhradené pre Kompetenčné a certifikačné centrum kybernetickej bezpečnosti (ďalej len „KCCKB“). Autorské práva k tomuto dokumentu má a autorské práva k tomuto dokumentu vykonáva KCCKB.

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.

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.



www.cybercompetence.sk, kyberkomunita.sk



www.linkedin.com/company/cybercompetence



@CybercenterSk