



Kompetenčné
a certifikačné
centrum
kybernetickej
bezpečnosti

NAJČASTEJŠIE ZISTENIA AUDITU V ZDRAVOTNÍCKYCH ZARIADENIACH

Pavol Dovičovič,

Kyberbezpečnosť pro zdravotníctví

23.02.2023



KOMPETENČNÉ A CERTIFIKAČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

- Pôsobnosť **Národného koordinačného centra** v zmysle Nariadenia EÚ č. 2021/887 o Európskej sieti centier odvetvových, technologických a výskumných kompetencií
- **Výkon činnosti orgánu posudzovania zhody**, t.j. 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





METRIKA



NAJČASTEJŠIE ZISTENIA AUDITU V ZDRAVOTNÍCKYCH ZARIADENIACH



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.



AKÁ BEZPEČNOSŤ JE PRIMERANÁ...?

- Kybernetická bezpečnosť (resp. bezpečnosť informácií):
 - Spôsobilosť systému, alebo vyspelosť procesu v kontexte bezpečnostných zraniteľností
 - Proces výkonu ochrany informačných aktív
 - Cieľová úroveň, v ktorej sú informácie považované za odolné voči hrozbám
- **Definícia:** Stav, v ktorom sú siete a informačné systémy schopné odolávať hrozbám na určitom stupni spoľahlivosti (t.j. primerane)
- Čo kybernetická bezpečnosť nie je? Pocit vlastníka informačných aktív...
- Nemýľme si „primeranú“ s „akceptovanou“ úrovňou bezpečnosti

DÁ SA ZMERAŤ ÚROVEŇ BEZPEČNOSTI?



AKO ZÍSKAŤ OBJEKTÍVNE INFORMÁCIE O ÚROVNI KYBERNETICKEJ BEZPEČNOSTI?

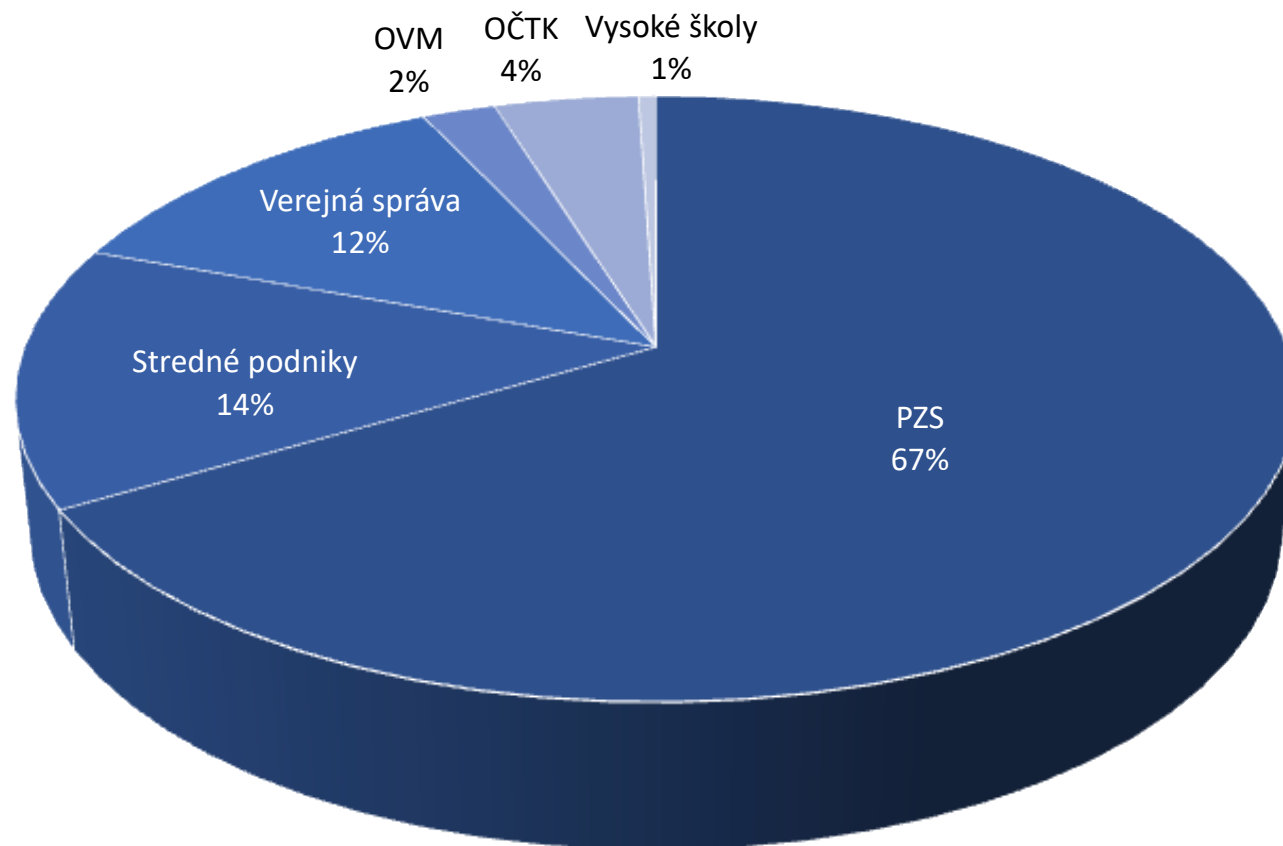
- Pomocou kvantifikácie vybraných atribútov:
 - Zraniteľnosti a hrozby (resp. trend Threat landscape)
 - Riziká (KRI)
 - Incidenty (počty, straty, objemy, čas)
 - Stav súladu (počet auditných zistení)
 - Spôsobilosti a odolnosť (implementované opatrenia, efektívnosť opatrení)
 - Posudzovanie zhody (certifikácia produktov, osôb a systémov manažérstva)
 - Úroveň znalostí a zručností (testovanie vedomostí, cvičenia)
 - Verejná mienka (prieskumy)



ODHAD POŽIADAVIEK PRACOVNÉHO TRHU

Rola / Kategória subjektu	PZS	Stredné podniky	Verejná správa	OV	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



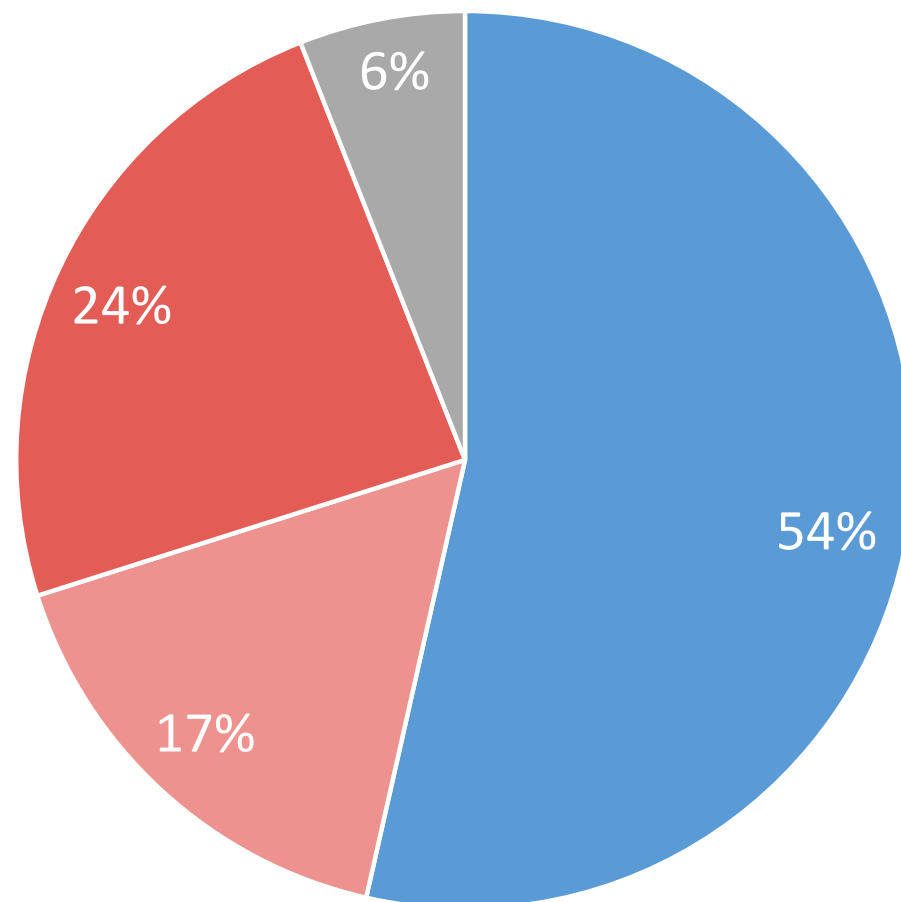
STAV KYBERNETICKEJ BEZPEČNOSTI V SR PODĽA VÝSLEDKOV AUDITU KB

NAJČASTEJŠIE ZISTENIA AUDITU V ZDRAVOTNÍCKYCH ZARIADENIACH



PRIEMERNÁ MIERA SÚLADU – VŠETCI PZS

Zdroj: Doručené správy auditu 2021, NBÚ

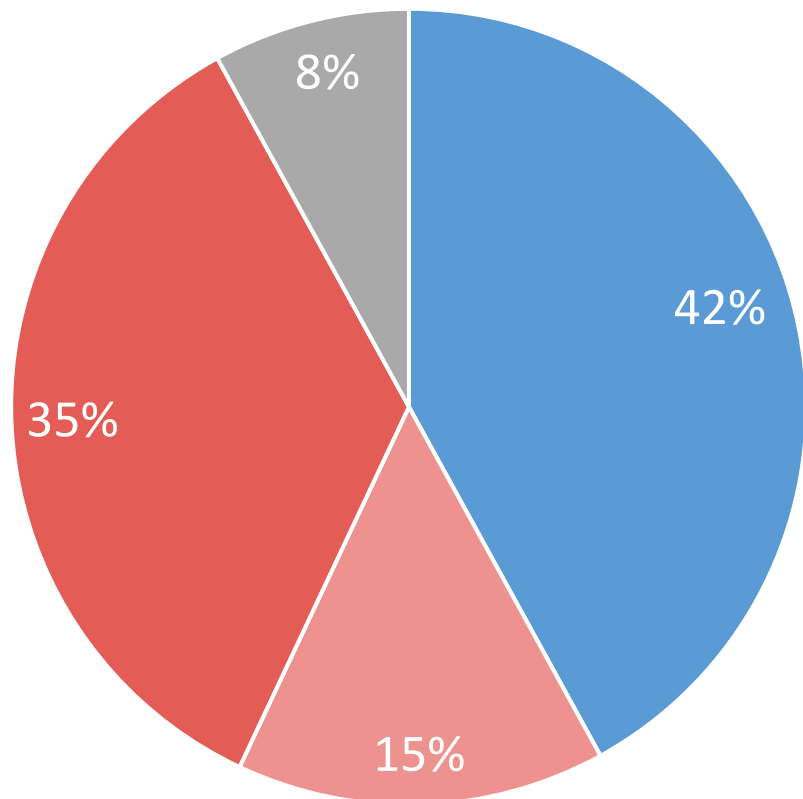


■ Súlada ■ Čiastočný súlad ■ Nesúlada ■ Neaplikované



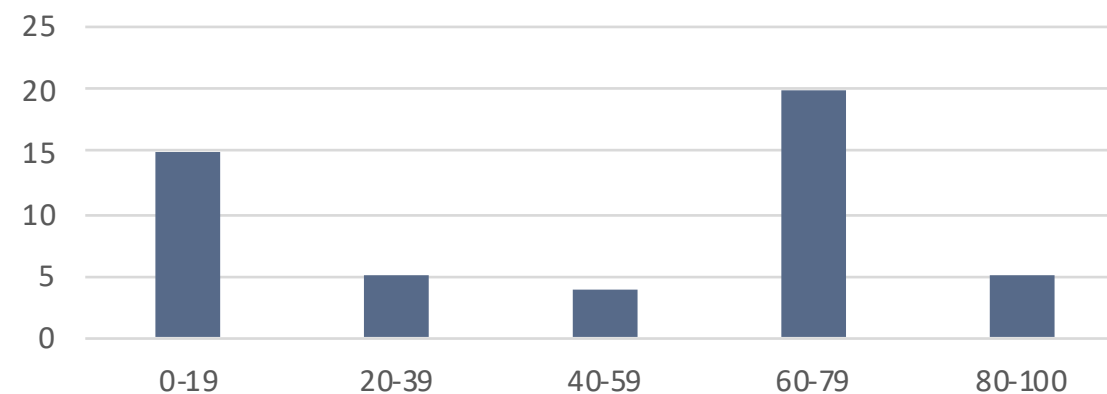
PRIEMERNÁ MIERA SÚLADU - ZDRAVOTNÍCTVO

Zdroj: Doručené správy auditu 2022, NBÚ



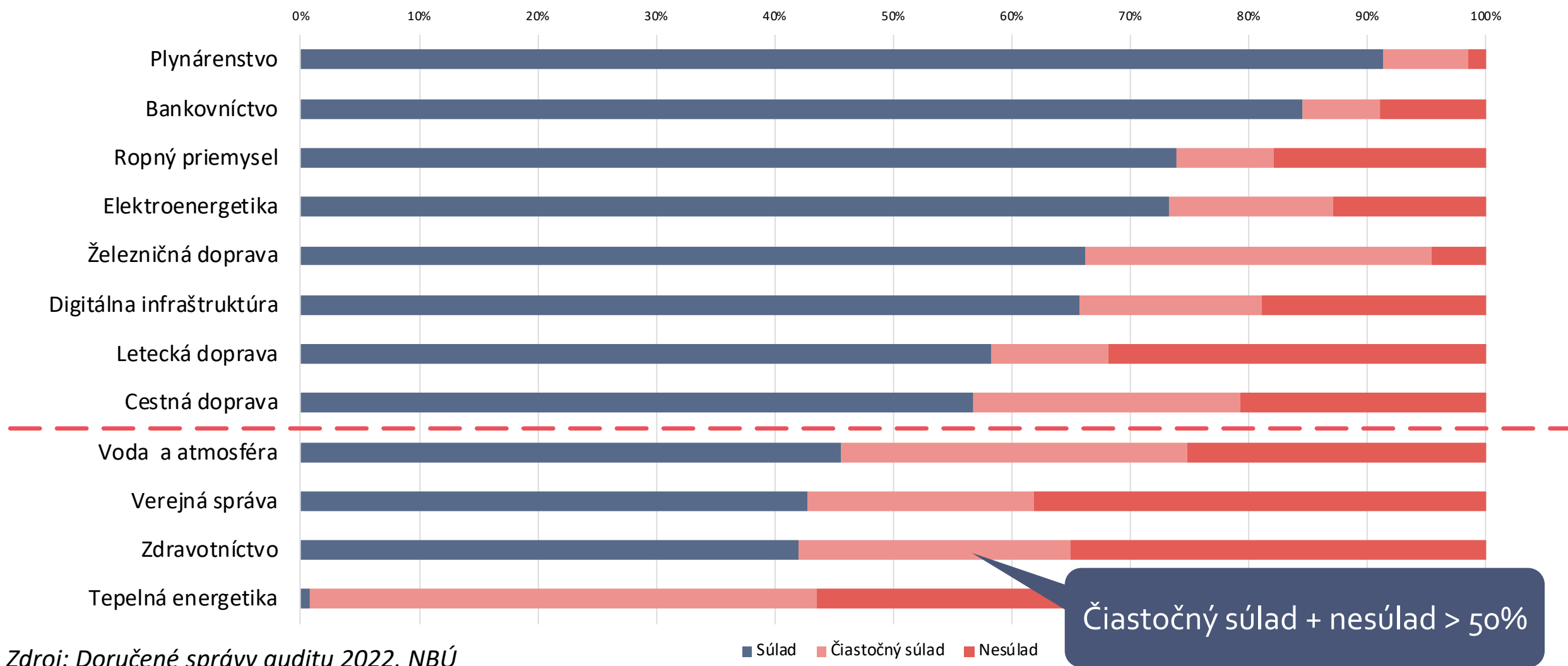
■ Súlada ■ Čiastočný súlad ■ Nesúlada ■ Neaplikované

Štatistická distribúcia miery súladu:





STAV SÚLADU PODĽA ODVETVÍ

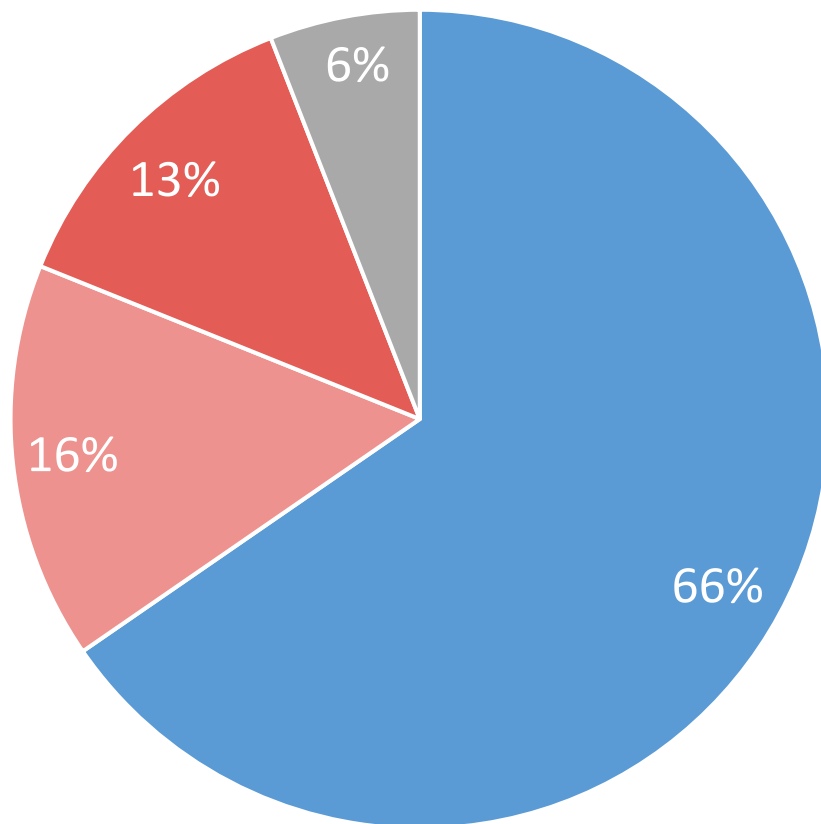


Zdroj: Doručené správy auditu 2022, NBÚ

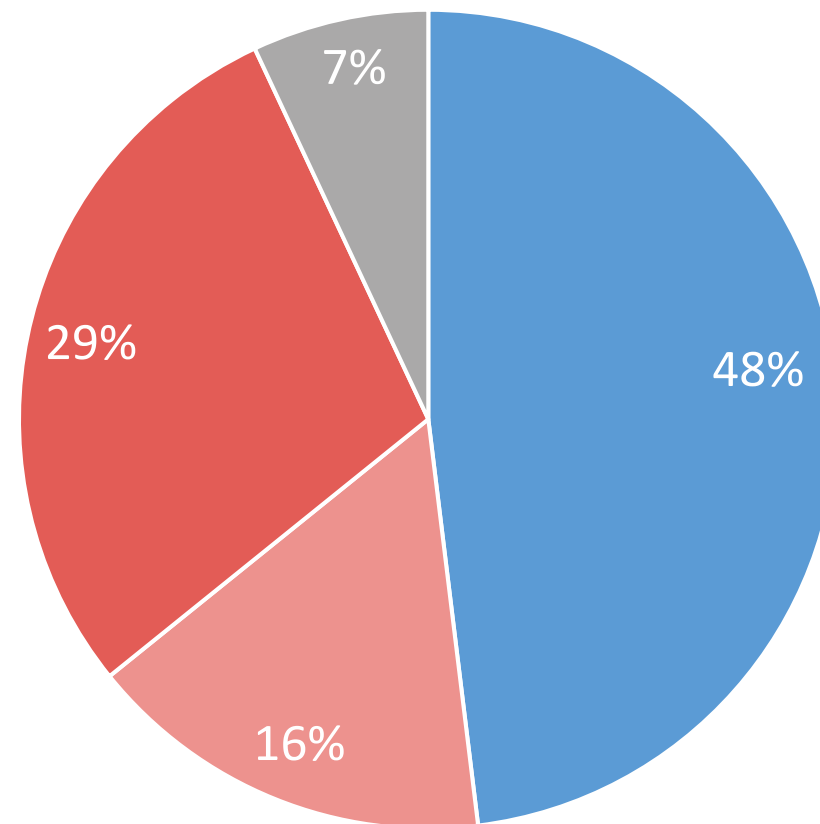


STAV SÚLADU PODĽA TYPU VLASTNÍCTVA

Typický PZS v súkromnom vlastníctve



Typický PZS vo verejnom vlastníctve



■ Súlad ■ Čiastočný súlad ■ Nesúlad ■ Neaplikované

■ Súlad ■ Čiastočný súlad ■ Nesúlad ■ Neaplikované



ZÁVER

NAJČASTEJŠIE ZISTENIA AUDITU V ZDRAVOTNÍCKYCH ZARIADENIACH



NAJČASTEJŠIE NÁLEZY AUDITU



Riadenie bezpečnosti (Security governance):

- Neexistujúca stratégia KB a nedostatočná podpora vedenia ústavu
- Nie je definovaná štruktúra riadenia, výkonu a kontroly v oblasti kybernetickej bezpečnosti
- Nie je stanovená zodpovednosť za identifikáciu a evidenciu aktív
- Nie sú stanovené pravidlá a zodpovednosti pri implementácii opatrení vyplývajúcich z analýzy 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

Výkon bezpečnosti (Security operations):

- Chýbajúci bezpečnostný monitoring
- Chýbajúce logovanie
- 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, obnova záloh netestovaná
- PZS nedostatočne rieši šifrovú ochranu informácií
- Väčšina procesov v oblasti šifrovania a managementu kľúčov nie je formalizovaná





NEGATÍVNY ZÁVER



- Koncom roka 2022 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
 - Neexistuje konsolidovaná metrika ani metodika atribúcie
- Jednotlivci preceňujú svoje príspevok 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 ktorí nie sú povinnými osobami vyvíjajú viac úsilia pre KB, než PZS...
- AP (NSKB) vyžaduje niekoľko konkrétnych úloh v súvislosti s hodnotením stavu KB SR
- V rámci ENISA beží WG, ktorá sa zaoberá prípravou indexu KB
- NBÚ/KCCKB vydá správu a prieskum KB ako ucelenú publikáciu (každoročne)





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



www.linkedin.com/company/cybercompetence



[@CybercenterSk](https://twitter.com/CybercenterSk)