Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

STRUČNÁ SPRÁVA O STAVE KYBERNETICKEJ BEZPEČNOSTI V SLOVENSKEJ REPUBLIKE

ITAPA, 16.06.2022

METRIKA

STRUČNÁ SPRÁVA O STAVE KYBERNETICKEJ BEZPEČNOSTI V SR

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?

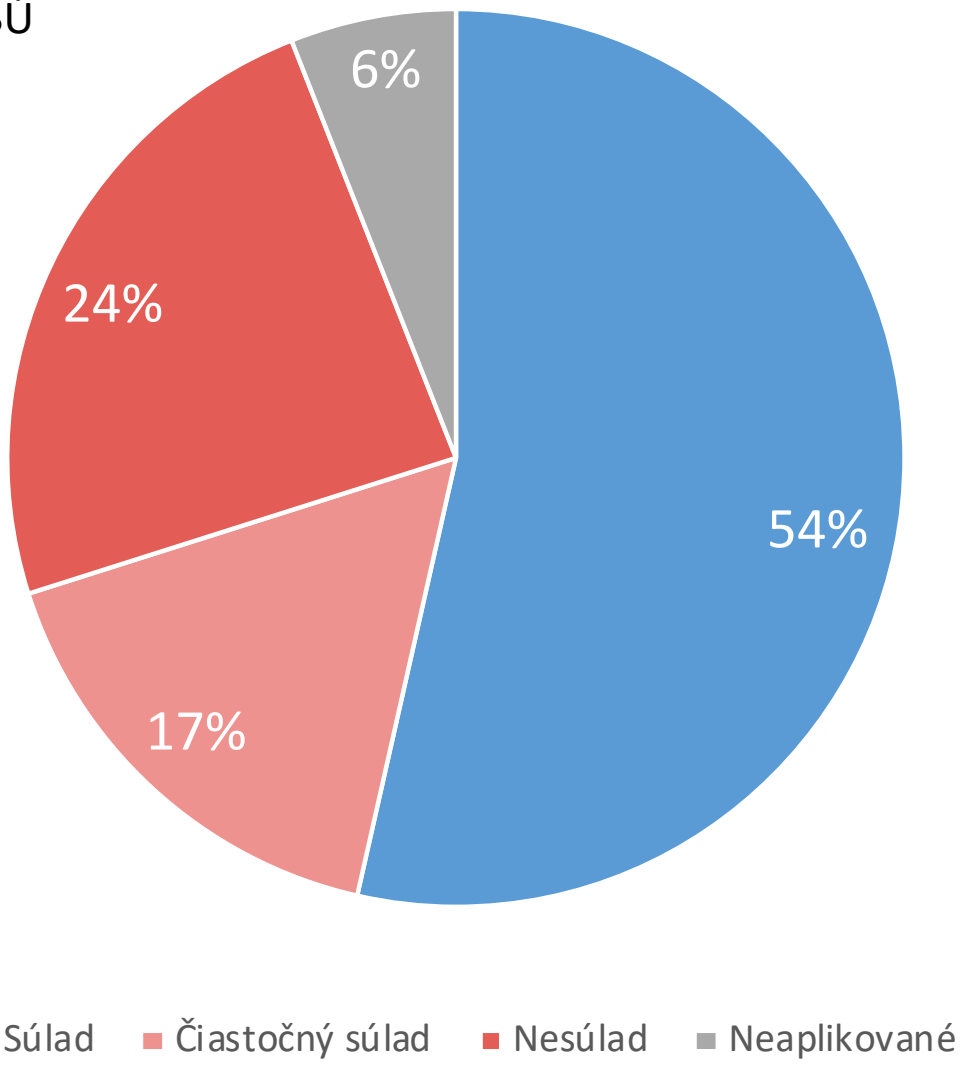
- Pomocou kvantifikácie vybraných atribútov:
  - Zraniteľnosti a hrozby (resp. trend Threat landscape)
  - Riziká (KRI)
  - Incidenty (počty, straty, objemy, čas)
  - Stav súladu (počet auditných zistení)
  - Spôsobilosti a odolnosť (implementované opatrenia, efektívnosť opatrení)
  - Posudzovanie zhody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

STAV KYBERNETICKEJ BEZPEČNOSTI

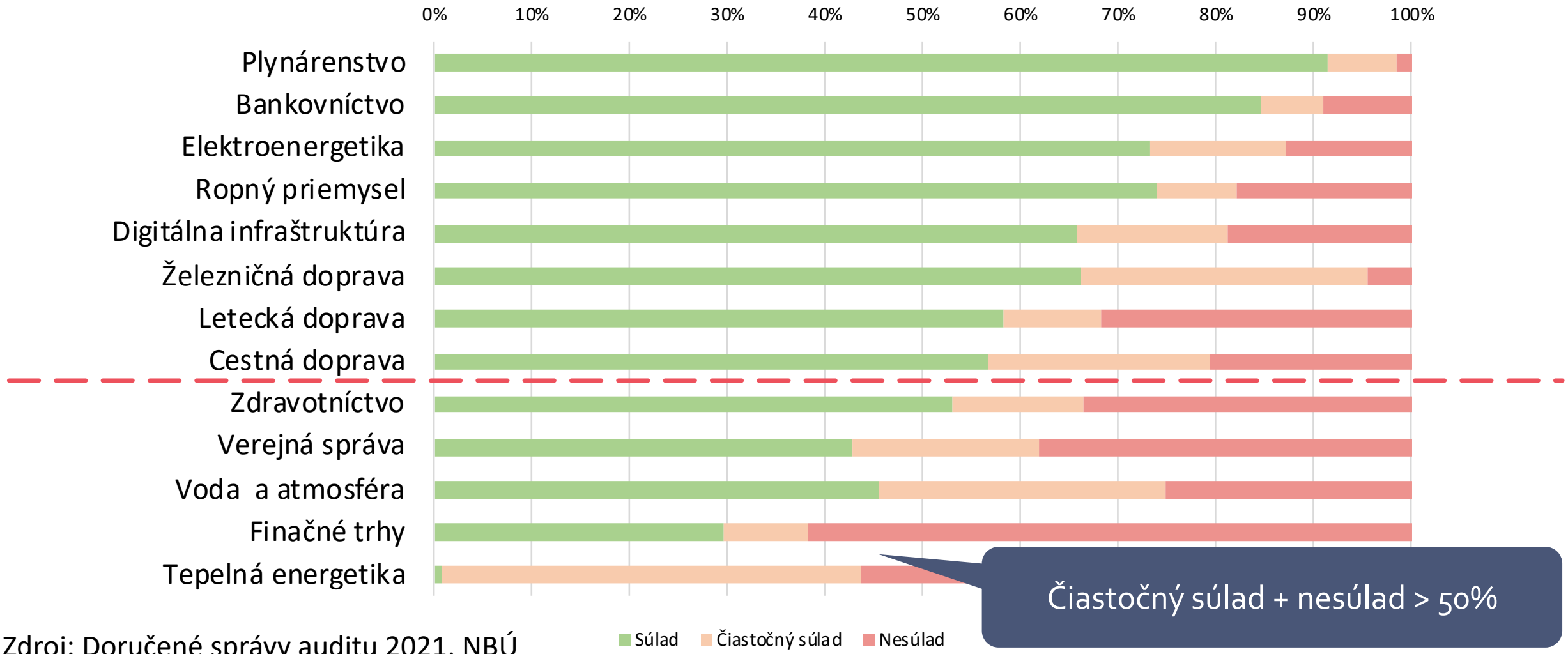
STRUČNÁ SPRÁVA O STAVE KYBERNETICKEJ BEZPEČNOSTI V SR

CELKOVÁ PRIEMERNÁ MIERA SÚLADU

Zdroj: Doručené správy auditu 2021, NBÚ



STAV SÚLADU PODĽA ODVETVÍ

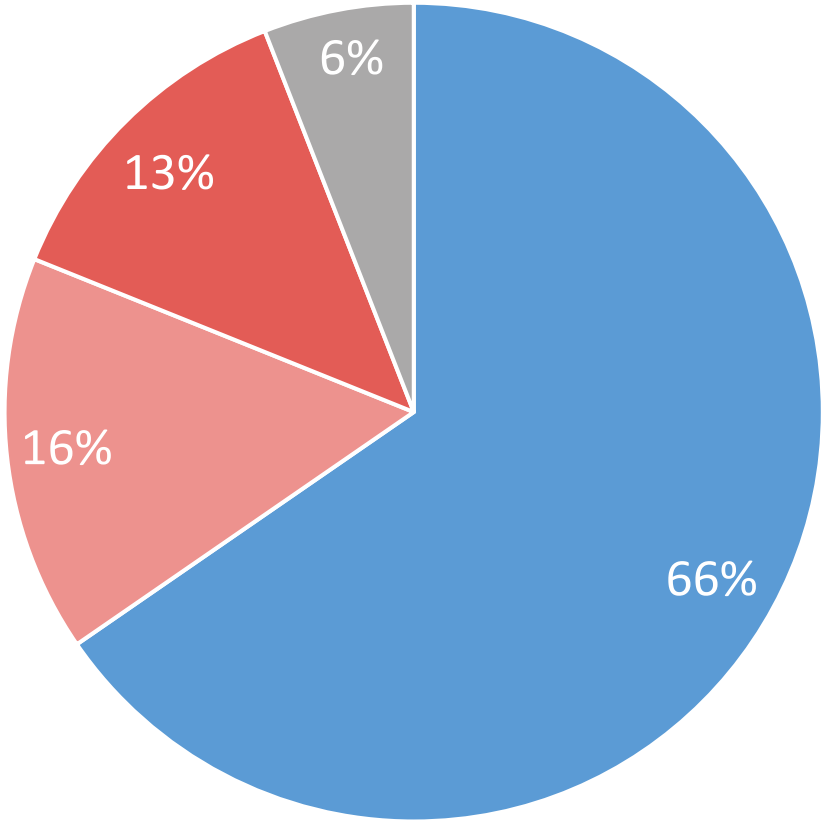


Čiastočný súlad + nesúlad > 50%

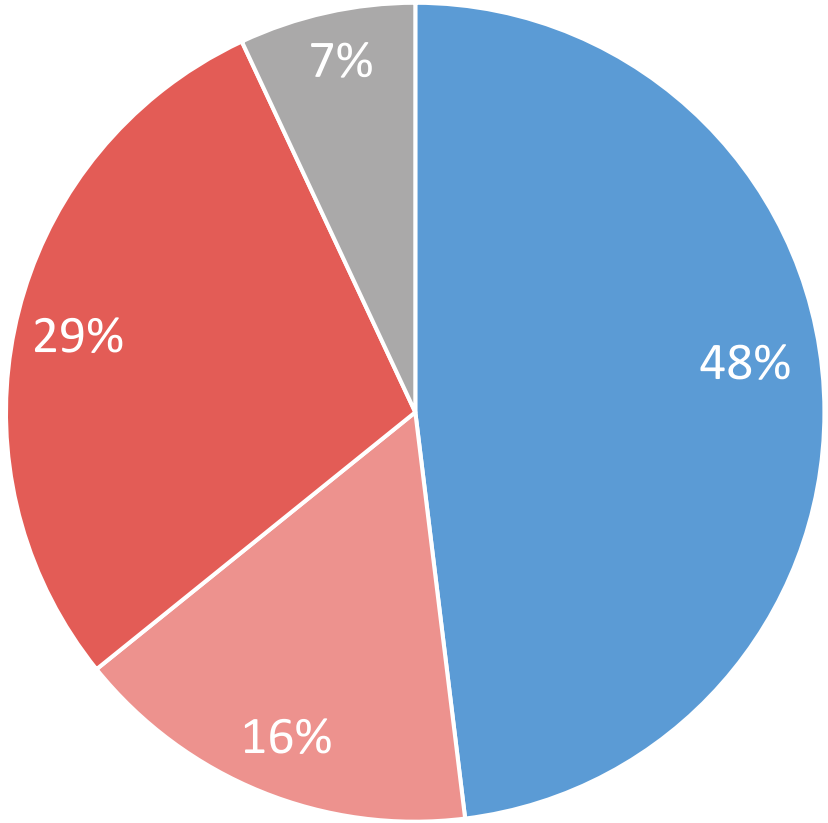
Zdroj: Doručené správy auditu 2021, NBÚ

STAV SÚLADU PODĽA TYPU VLASTNÍCTVA

Typicky PZS v súkromnom vlastníctve



Typicky PZS vo verejnom vlastníctve



NAJČASTEJŠIE NÁLEZY AUDITU

Riadenie bezpečnosti (Security governance):

- Neexistujúca stratégia KB a nedostatočná podpora najvyššieho vedenia
- Neurčený Manažér KB, prípadne neformálna rola,
- Nedostatočná, alebo chýbajúca bezpečnostná dokumentácia (aj pri PZS s certifikátmi SO27001)
- Dokumentácia často tvorená len dodávateľmi konkrétneho projektu
- Nezávislosť riadenia bezpečnosti od riadenia IT
- Neexistencia vzdelávania v oblasti informačnej bezpečnosti
- Závislosť na dodávateľoch (vendor lock)
- Neexistujúce riadenie aktív, hrozieb a rizík
- Chýbajúci vlastníci rizík a ich zodpovednosti
- Neformálne riadenie prevádzky

Výkon bezpečnosti (Security operations):

- Chýbajúci bezpečnostný monitoring
- Chýbajúce logovanie
- Nesystematické riešenie incidentov
- Nedostatky v riadení bezpečnosti sietí
- Chýbajúca topológia, segmentácia, zoznamy portov
- Nezabezpečenie a nedostatočná vybavenosť „serverovní" (často plných kvalitného ale nevyužitého HW)
- Neexistencia procesov riadenia kontinuity činností
- Nepripravenosť na krízové situácie
- Nejasné a neformálne postupy zálohovania, obnova záloh netestovaná
- (Ne)šifrovanie komunikácie, prenosov údajov a záloh

PRIESKUM STAVU KYBERNETICKEJ BEZPEČNOSTI

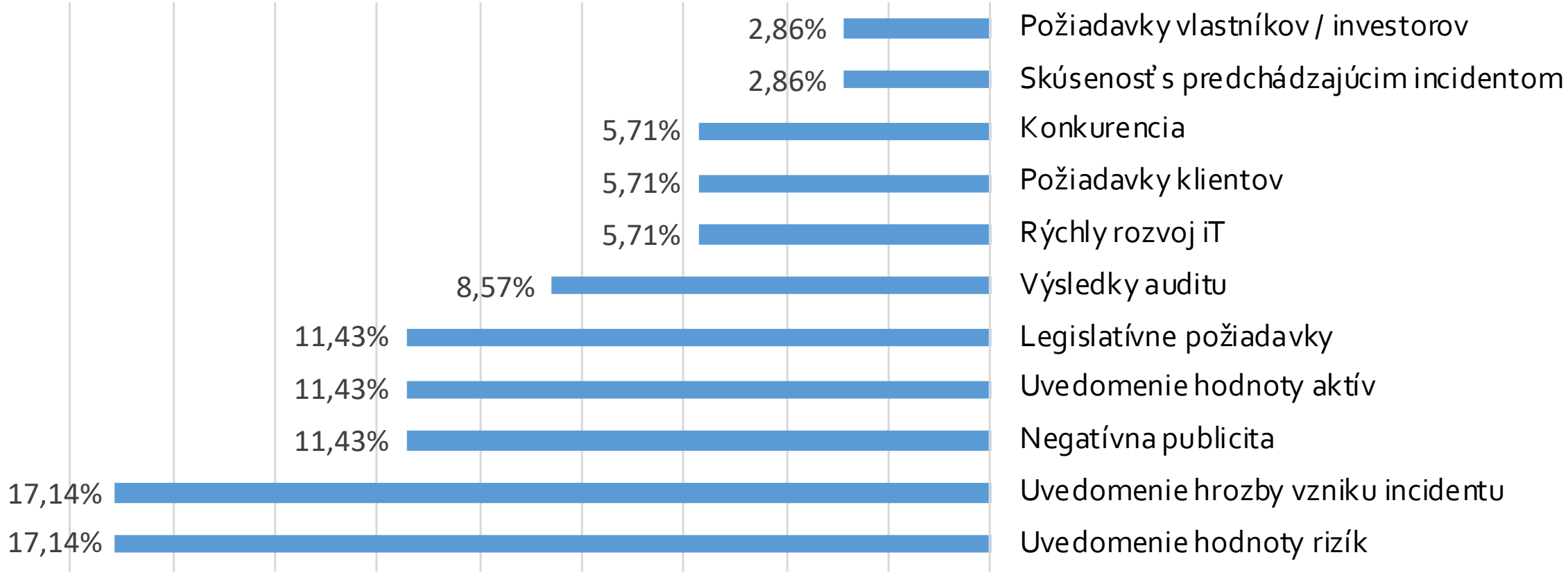
STRUČNÁ SPRÁVA O STAVE KYBERNETICKEJ BEZPEČNOSTI V SR

METODIKA PRIESKUMU

	verejnosť (obyvatelia SR)	malé a stredné podniky
metóda:	CAWI (online panel respondentov s kontrolovaným prístupom)	CATI (telefonicky prostredníctvom profesionálneho callcentra)
veľkosť vzorky:	1000	200
počet otázok:	1 screeningová + 4 sociodemografické + 13 meritórnych	1 screeningová + 4 sociodemografické + 13 meritórnych
termín zberu dát:	20.-28.4.2022	21.-29.4.2022
zloženie výskumnej vzorky:	reprezentatívne v kvótnych znakoch pohlavie, vek, vzdelanie, kraj	reprezentatívne v kvótnych veľkosť podľa počtu zamestnancov a sektor hlavnej činnosti
báza pre výber:	Štatistický úrad SR	Štatistický úrad SR
anketovanie:	online panel s kontrolovaným prístupom	školení tele-anketári
kontrola:	script, spätná náhodná kontrola	script, príposluch, spätná náhodná kontrola
štatistické spracovanie:	SPSS, excel	SPSS, excel

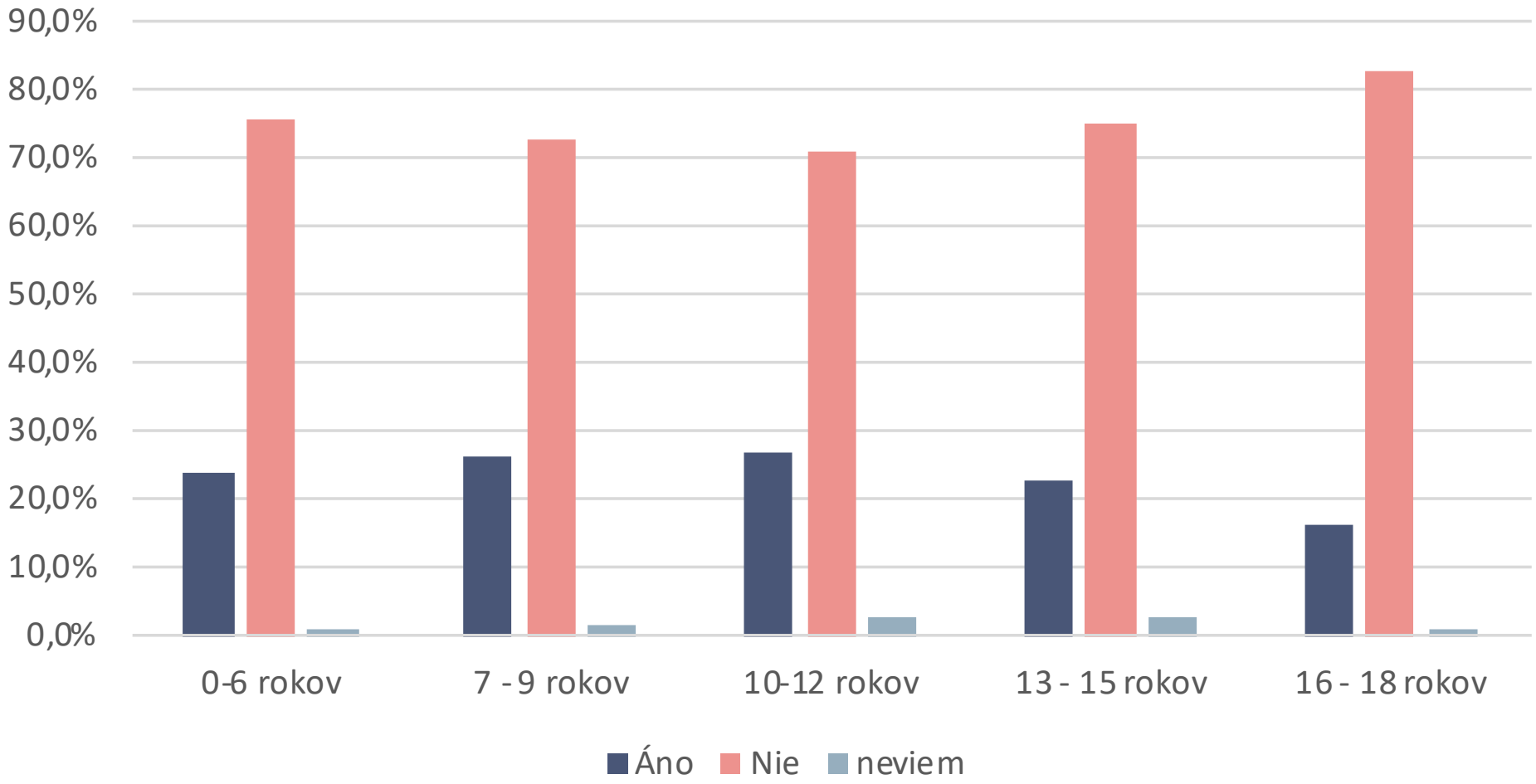
VPLYV NA ZVYŠOVANIE ÚROVNE BEZPEČNOSTI

Zdroj: Prieskum stavu KB



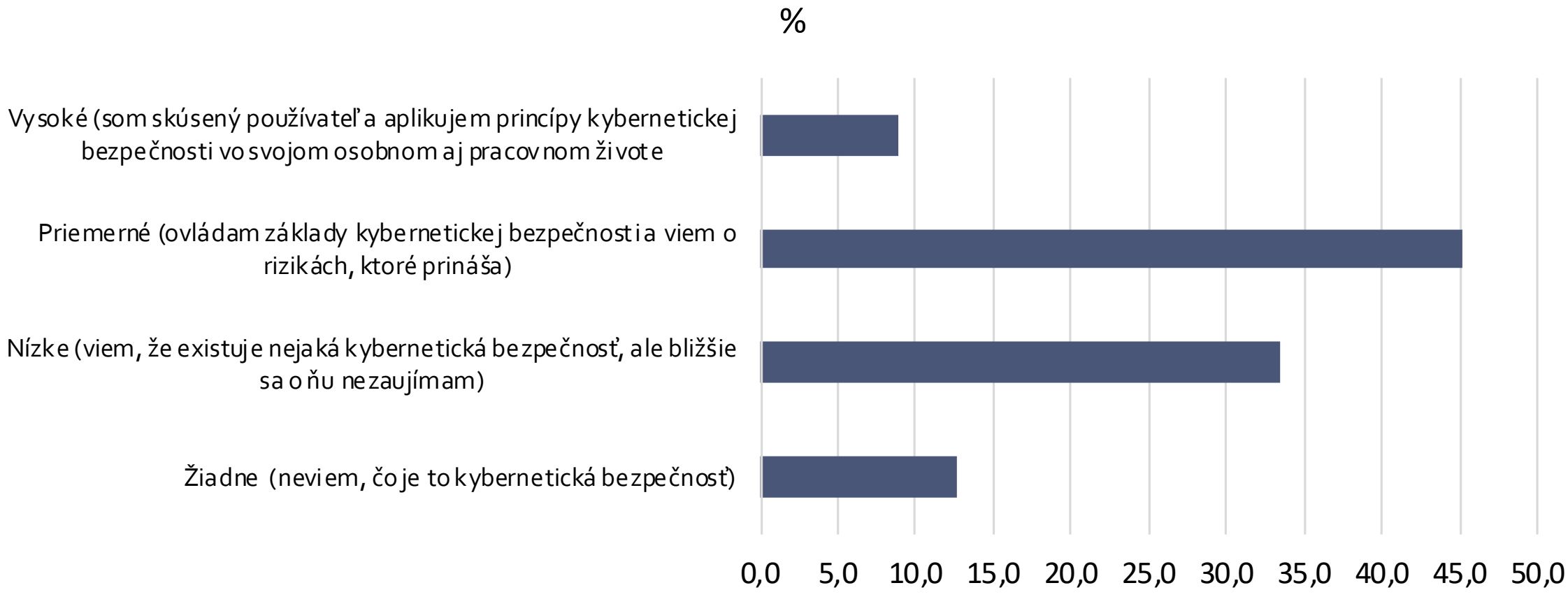
VYBRANÉ MERITÓRNE TVRDENIA PRIESKUMU

Používate vo Vašej domácnosti nástroje na kontrolu detí v digitálnom priestore (rodičovská kontrola)?



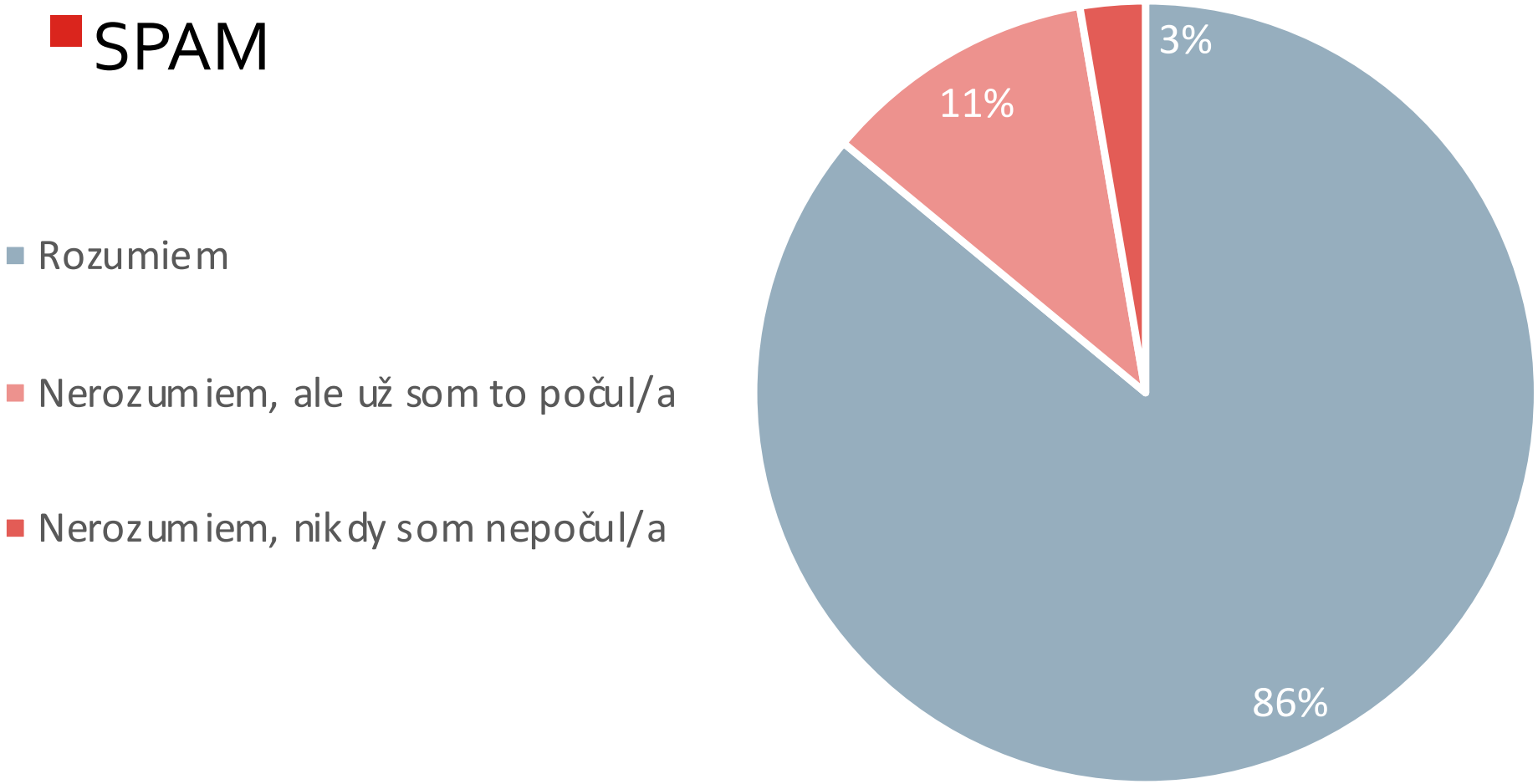
VYBRANÉ MERITÓRNE TVRDENIA PRIESKUMU

Ako hodnotíte svoje znalosti a zručnosti o kybernetickej bezpečnosti?



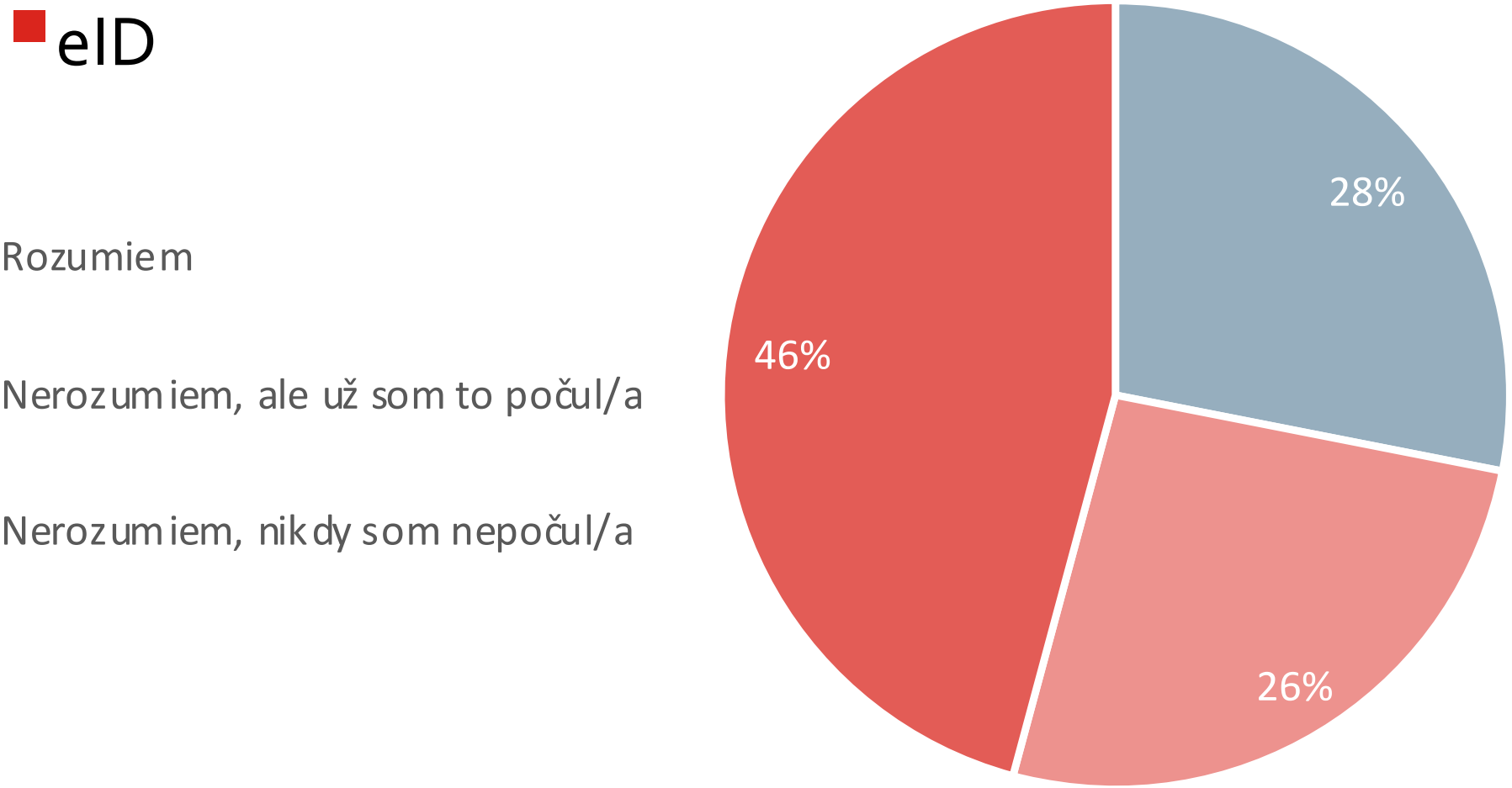
VYBRANÉ MERITÓRNE TVRDENIA PRIESKUMU

Rozumiete týmto výrazom v počítačovom prostredí?



VYBRANÉ MERITÓRNE TVRDENIA PRIESKUMU

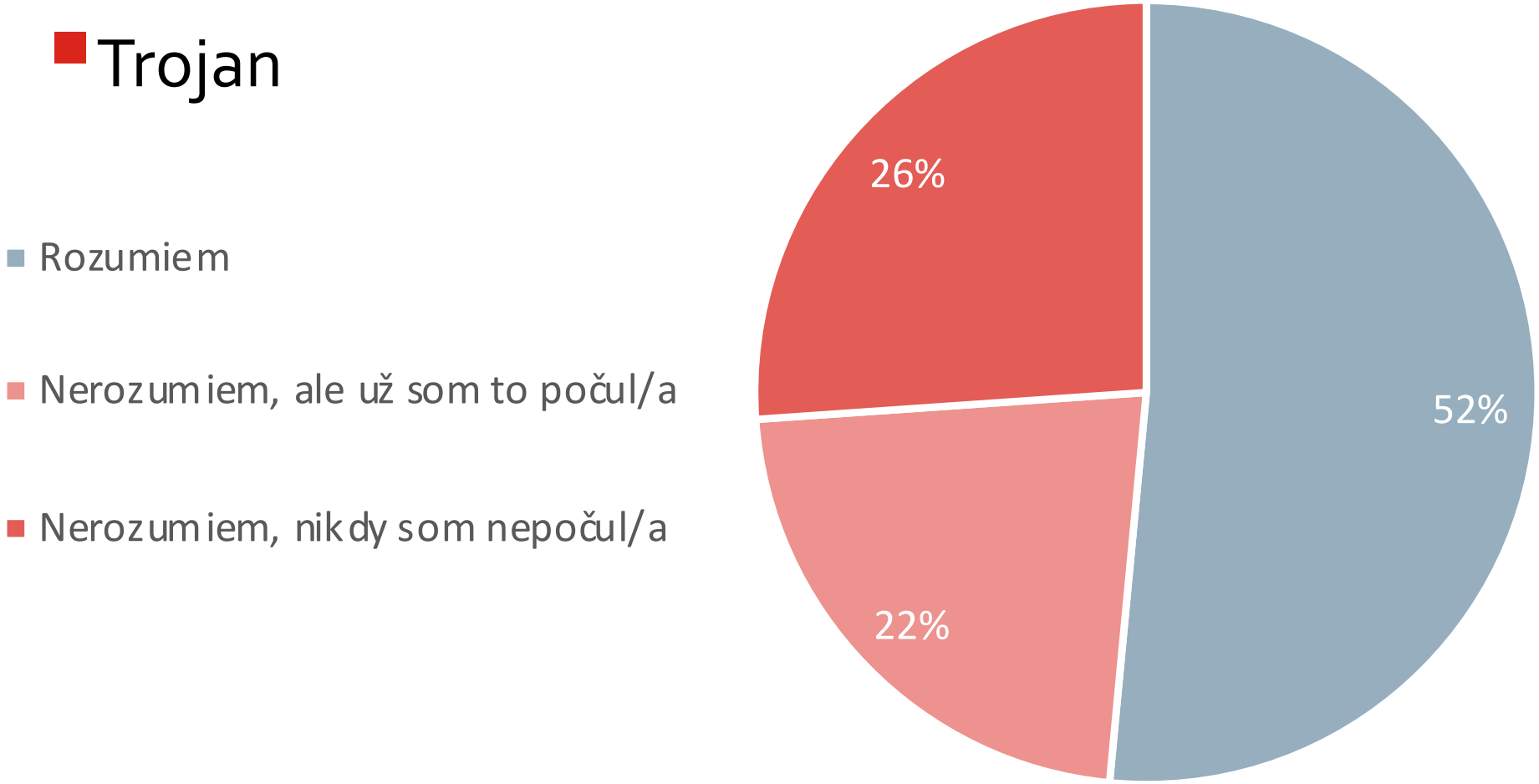
Rozumiete týmto výrazom v počítačovom prostredí?



VYBRANÉ MERITÓRNE TVRDENIA PRIESKUMU

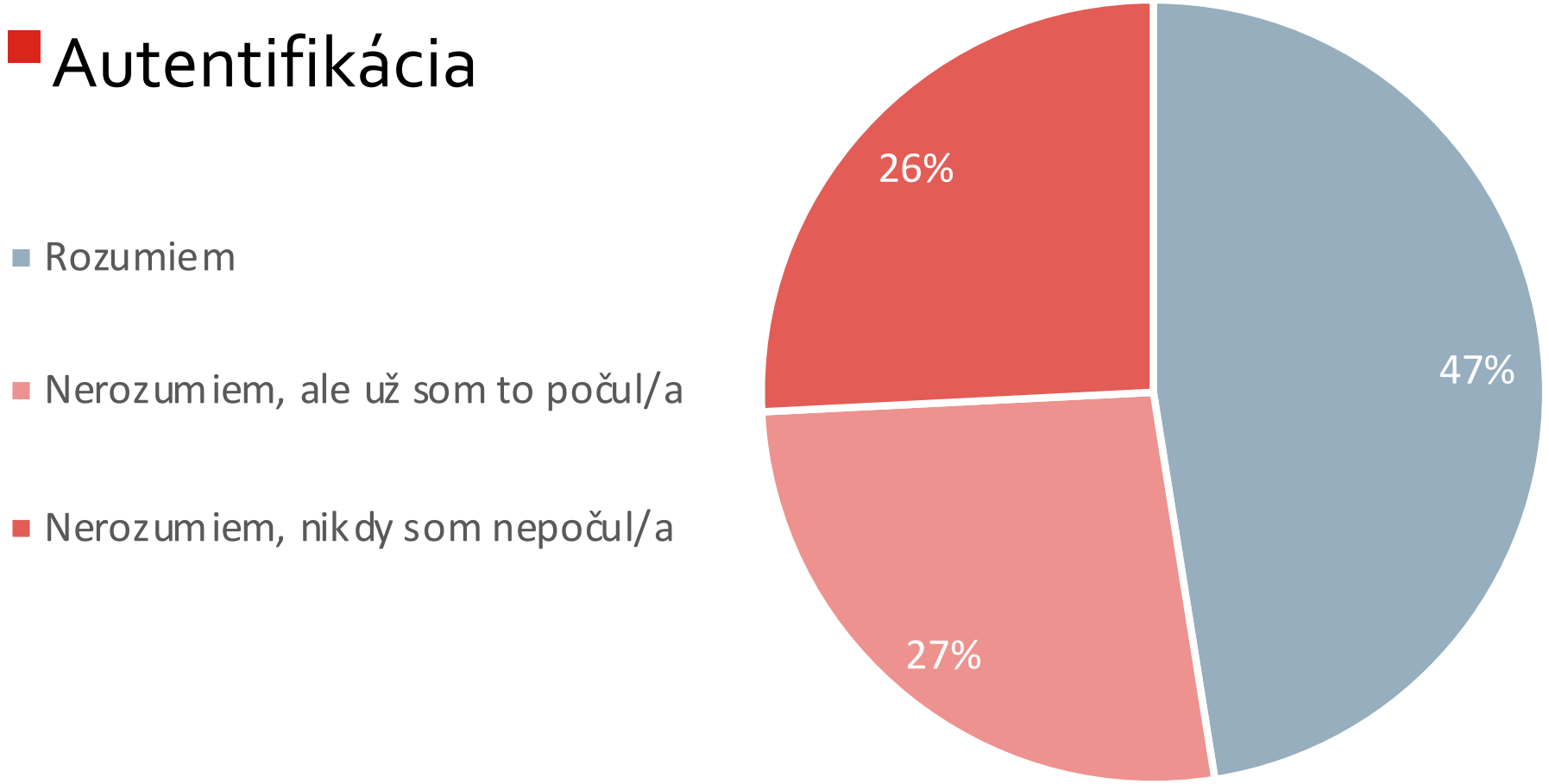
Rozumiete týmto výrazom v počítačovom prostredí?

Trojan



VYBRANÉ MERITÓRNE TVRDENIA PRIESKUMU

Rozumiete týmto výrazom v počítačovom prostredí?



ZÁVER

STRUČNÁ SPRÁVA O STAVE KYBERNETICKEJ BEZPEČNOSTI V SR

ZÁVER

- V 6. mesiaci roku 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 prispenie a najmä spôsobilosti
- Zlá situácia dlhodobo pretrváva v sektoroch verejná správa a zdravotníctvo
- (Nepríjemným) prekvapením je negatívny stav v sektore tepelná energetika

- SME (a subjekty ktorí nie sú povinnými osobami) mnohokrát 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)