KYBERNETICKÁ BEZPEČNOSŤ 2023

Výsledky telefonického prieskumu realizovaného medzi malými a strednými podnikmi

Zber dát:
24. 4. - 2. 5. 2023

ako®
VEDIEŤ O SEBE

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

OBSAH

ÚVOD

Úvod

Rýchly rozvoj digitalizácie a neustály pokrok v používaní informačných technológií so sebou prináša aj riziká spočívajúce v rôznych kybernetických hrozbách. Incidenty sa často vyskytujú aj v podnikateľskom prostredí, kde jedným z najzraniteľnejších objektov sú malé a stredné podniky, pri ktorých sa predpokladá nižšia úroveň zabezpečenia. Či už preto, že na rozdiel od veľkých spoločností nemajú potrebné kapacity na implementáciu bezpečnostných opatrení, alebo, keďže nie sú v kategórii regulovaných subjektov, nevzťahujú sa na nich zákonné povinnosti, ktoré by ich k potrebným bezpečnostnými opatreniam prinútili.

V snahe zvýšiť úroveň kybernetickej bezpečnosti v malých a stredných podnikoch je potrebné najskôr poznať skutočný stav ich kybernetickej odolnosti a identifikovať problémové oblasti. Aj z tohto dôvodu sa Národný bezpečnostný úrad (NBÚ) spolu s Kompetenčným a certifikačným centrom kybernetickej bezpečnosti (KCCKB) rozhodli vykonať v spolupráci s renomovanou agentúrou prieskum zameraný na zistenie stavu kybernetickej bezpečnosti v malých a stredných podnikoch, ktorý sa plánuje vykonávať každoročne.

Prieskum sa uskutočnil na vzorke 200 respondentov z malých a stredných podnikov od 24. 4. do 2. 5. 2023 a zameral sa na okruhy otázok v troch oblastiach, a to stav kybernetickej bezpečnosti, úroveň znalostí zamestnancov v oblasti kybernetickej bezpečnosti a stratégia a implementácia kybernetickej bezpečnosti. K prieskumu sme spracovali aj interpretáciu výsledkov.

Aj napriek tomu, že v stave kybernetickej bezpečnosti v malých a stredných podnikoch možno, v porovnaní s minulým rokom, badať zlepšenie, z výsledkov tohtoročného prieskumu vyplýva, že problematika kybernetickej bezpečnosti je stále podceňovanou témou. Jedným z možných dôvodov je aj skutočnosť, že niektoré podniky doteraz bezprostredne nezažili kybernetický incident. Je však potrebné zdôrazniť, že keď incident už reálne nastane, tento môže byť pre malý a stredný podnik likvidačný, či už vo forme priamych finančných strát alebo vo forme straty reputácie. Preto by tieto podniky mali vo vlastnom záujme zodpovedne pristupovať k zaisteniu ochrany svojich aktív.

Výsledky prieskumu budú využité na zameranie vzdelávacích aktivít a na zvyšovanie povedomia v tejto oblasti pre malé a stredné podniky zo strany NBÚ a KCCKB a taktiež budú pokladom pre tvorbu národného indexu kybernetickej bezpečnosti.

Martin Oravský

Riaditeľ Inštitútu pre bezpečnostné štúdie
Národný bezpečnostný úrad

VÝSLEDKY PRIESKUMU

1. STAV KYBERNETICKEJ BEZPEČNOSTI V MSP

1.1 JE FIRMA OHROZENÁ KYBERNETICKÝMI ÚTOKMI?

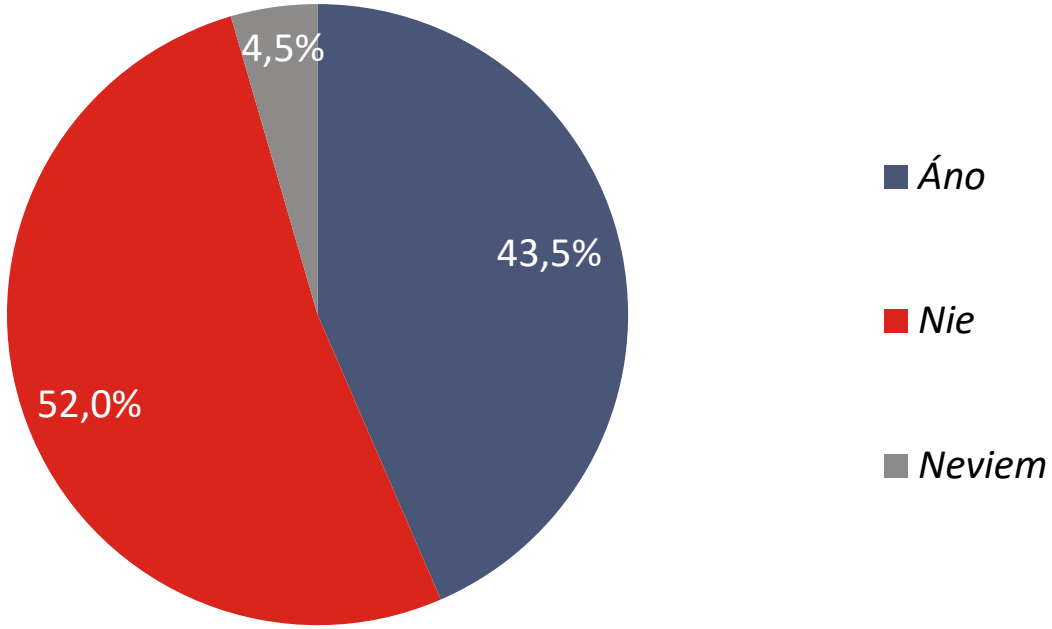
„Je alebo nie je vaša firma ohrozená kybernetickými útokmi?“

1.1 JE FIRMA OHROZENÁ KYBERNETICKÝMI ÚTOKMI?

„Je alebo nie je vaša firma ohrozená kybernetickými útokmi?"

Odpovede všetkých respondentov

N= 200



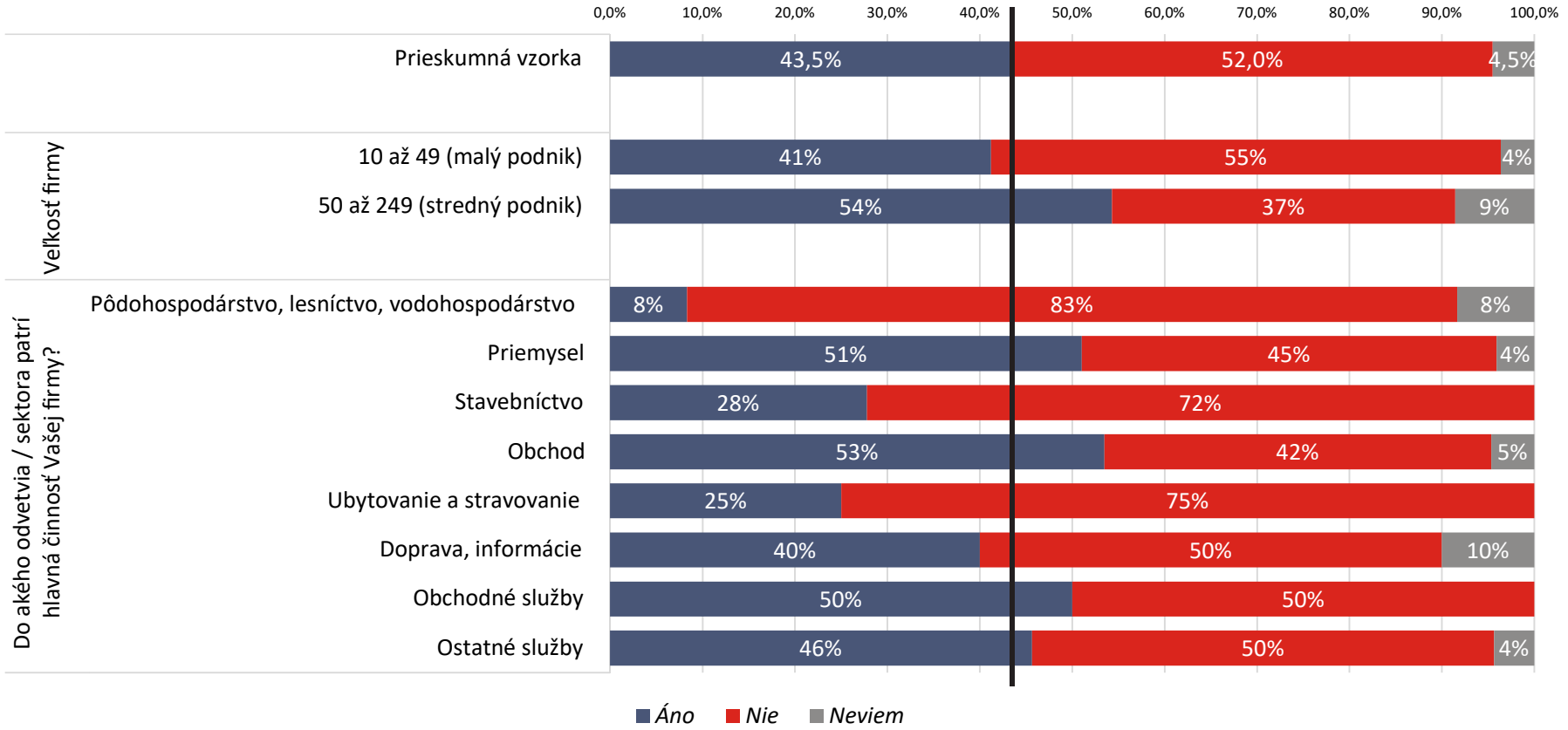
Respondent mal možnosť vybrať odpoveď z vopred preddefinovaných možností odpovedí.

Možnosť len jednej odpovede.

1.1 JE FIRMA OHROZENÁ KYBERNETICKÝMI ÚTOKMI?

„Je alebo nie je vaša firma ohrozená kybernetickými útokmi?"

Odpovede podľa štruktúry podnikov



PRIEBEŽNÉ ZHRNUTIE – VNÍMANÉ OHROZENIE KYBERNETICKÝMI ÚTOKMI

Cieľovou skupinou reprezentatívneho telefonického prieskumu boli malé (10 – 49 zamestnancov) a stredné (50 – 249 zamestnancov) podniky SR. Výsledky prieskumu sú reprezentatívne z hľadiska veľkosti podniku a sektora, v ktorom podnik primárne pôsobí.
Prieskum bol realizovaný na vzorke 200 respondentov.

Relevantná / akceptovateľná je odpoveď „áno"; avšak iba **43,5% malých a stredných podnikov** (ďalej v texte len MSP) uviedlo, že **sú ohrozené** kybernetickými útokmi. Ako dôvody tejto odpovede odhadujeme neuvedomenie si hrozieb, resp. neznalosť problematiky .

V porovnaní s priemerným výsledkom celej prieskumnej vzorky, ide častejšie o stredne veľké podniky (54% stredných podnikov oproti priemeru 43,5%).

Z hľadiska sektorov, v porovnaní s priemerným výsledkom, ohrozenie kybernetickými útokmi uvádzajú nadpriemerne podniky zo sektoru priemyslu, obchodu, obchodných služieb a ostatných služieb.

1.2 RIADENIE KYBERNETICKÝCH RIZÍK V MSP

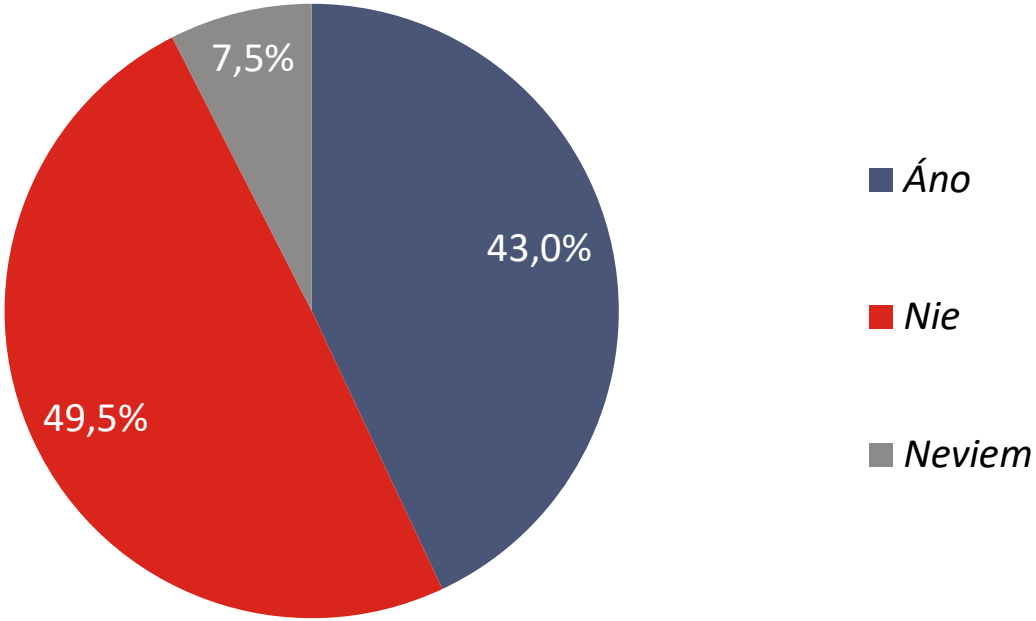
„Máte vo firemných procesoch zabezpečené RIADENIE KYBERNETICKÝCH RIZÍK vo svojej organizácii, aj keď vám to legislatíva neprikazuje?“

1.2 RIADENIE KYBERNETICKÝCH RIZÍK V MSP

„Máte vo firemných procesoch zabezpečené RIADENIE KYBERNETICKÝCH RIZÍK vo svojej organizácii, aj keď vám to legislatíva neprikazuje?"

Odpovede všetkých respondentov

N= 200



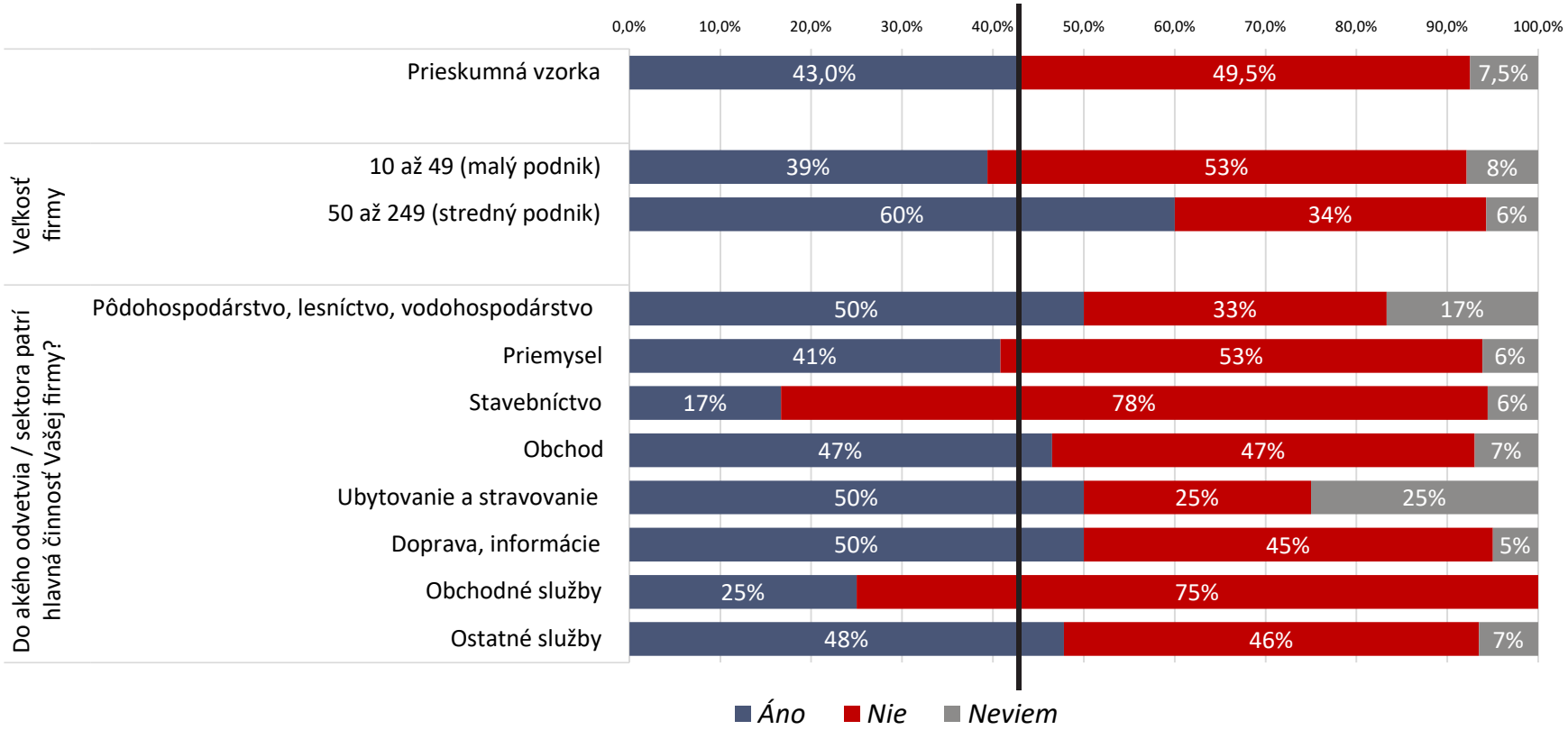
Respondent mal možnosť vybrať odpoveď z vopred preddefinovaných možností odpovedí.

Možnosť len jednej odpovede.

1.2 RIADENIE KYBERNETICKÝCH RIZÍK V MSP

„Máte vo firemných procesoch zabezpečené RIADENIE KYBERNETICKÝCH RIZÍK vo svojej organizácii, aj keď vám to legislatíva neprikazuje?“

Odpovede podľa štruktúry podnikov



1.2 RIADENIE KYBERNETICKÝCH RIZÍK V MSP

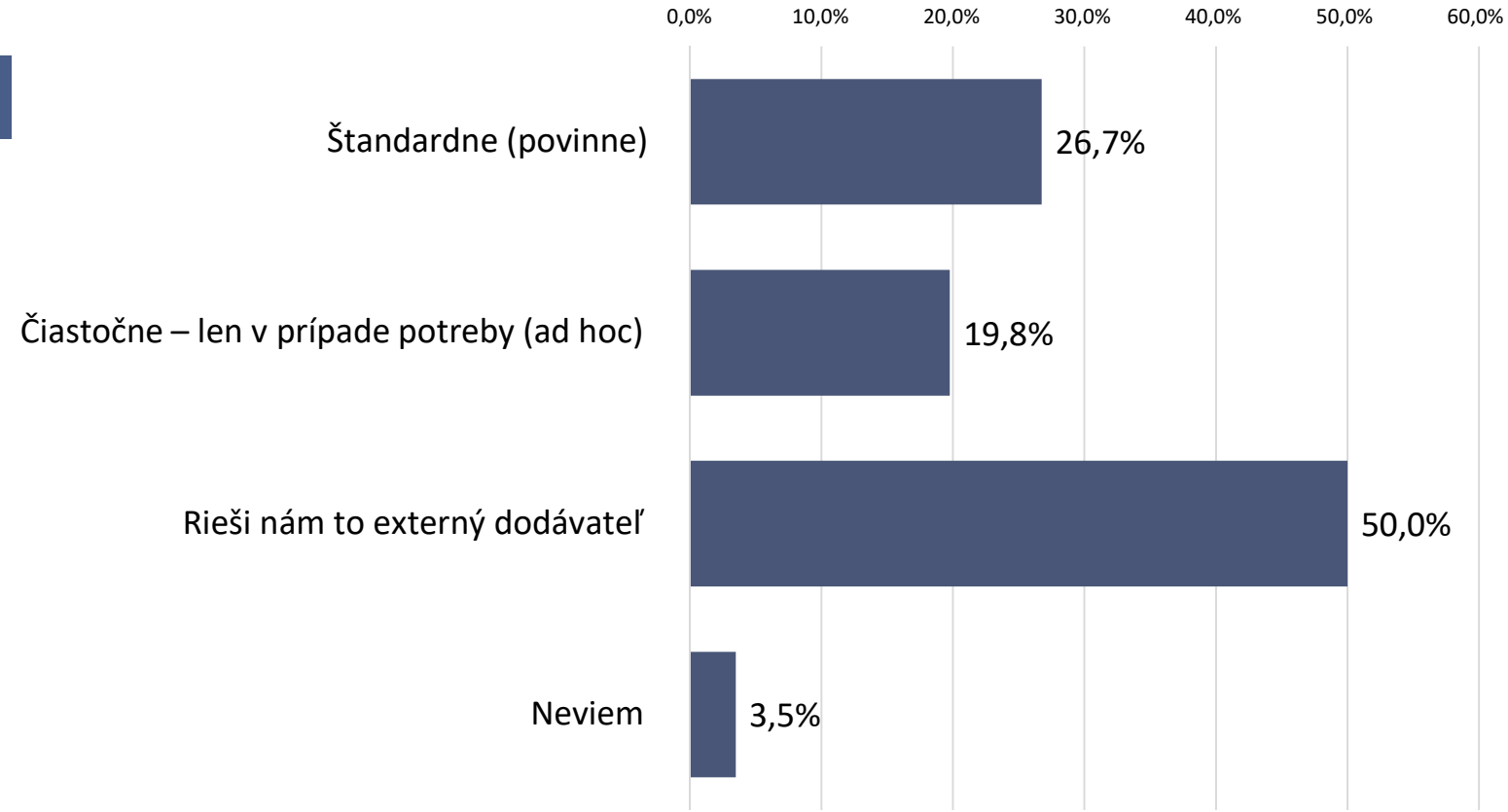
„Akým spôsobom máte zabezpečené riadenie kybernetických rizík?“

1.2 RIADENIE KYBERNETICKÝCH RIZÍK V MSP

„Akým spôsobom máte zabezpečené riadenie kybernetických rizík?"

Odpovede tých respondentov, ktorí majú vo firemných procesoch zabezpečené RIADENIE KYBERNETICKÝCH RIZÍK

N= 86



Respondent mal možnosť vybrať odpoveď z vopred preddefinovaných možností odpovedí.

Možnosť len jednej odpovede.

PRIEBEŽNÉ ZHRNUTIE – RIADENIE KYBERNETICKÝCH RIZÍK

Z výsledkov prieskumu vyplýva, že **43% malých a stredných podnikov** (ďalej v texte len MSP) **má vo firemných procesoch zabezpečené riadenie kybernetických rizík (ďalej v texte len RKR),** aj keď im to legislatíva neprikazuje. Relevantná / akceptovateľná je odpoveď „áno"; avšak: ak by MSP mal reálne implementovaný proces riadenia rizík, štatutár by o tom samozrejme bol informovaný – a odpoveď by bola kladná. Vedomé odpovede „nie" alebo „neviem" znamenajú, že riadenie rizík MSP skutočne nemá implementované.

V porovnaní s priemerným výsledkom celej prieskumnej vzorky, ide častejšie o stredne veľké podniky (RKR má 60% stredných podnikov oproti priemeru 43%).

Z hľadiska sektorov, v porovnaní s priemerným výsledkom, RKR majú vo firemných procesoch nadpriemerne zabezpečené podniky zo sektoru pôdohospodárstva, ubytovania a stravovania, dopravy a informácií, obchodu a ostatných služieb. Trend je rastúci s veľkosťou podniku (čím má podnik väčší počet zamestnancov, tým je pravdepodobnejšie, že procesy riadenia rizík sú implementované).

- Hodnotené boli len odpovede tých respondentov, ktorí odpovedali, že majú implementovaný proces riadenia kybernetických rizík (to predstavuje cca 50% MSP),
- týchto 50% zdôrazňuje, že pre nich procesy riadenia rizík rieši externý dodávateľ
- iba 25% z týchto 50% MSP rieši riadenie rizík povinne, ako štandardný proces.

Tie podniky, ktoré RKR vo firemných procesoch majú, ich majú riešené týmito spôsobmi:

- 26,7% štandardne (povinne)
- 19,8% čiastočne – len v prípade potreby (ad hoc)
- 50% tieto rieši externý dodávateľ
- Odpoveď neviem uviedlo 3,5% respondentov.

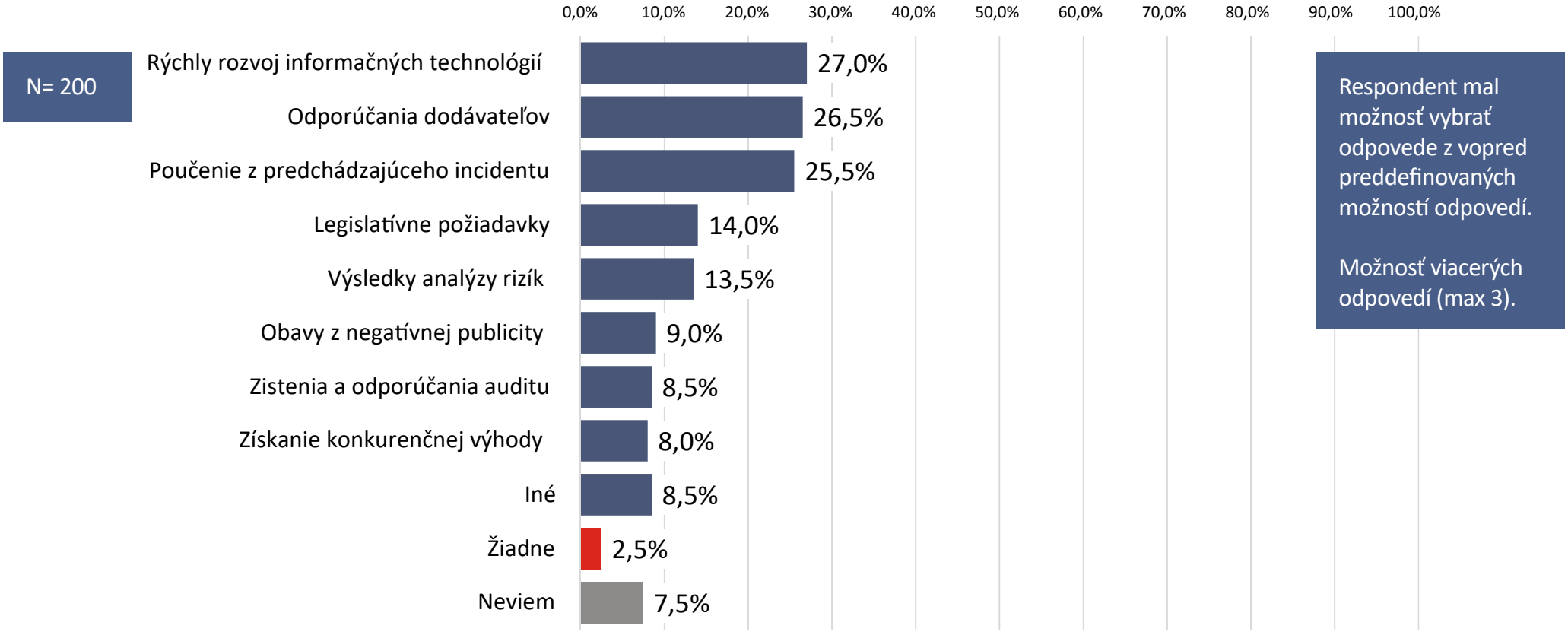
1.3 FAKTORY ZVYŠOVANIA ÚROVNE KYBERNETICKEJ BEZPEČNOSTI

„Aké sú faktory, ktoré majú vo vašej organizácii najvyšší vplyv na zvyšovanie úrovne kybernetickej bezpečnosti?"

1.3 FAKTORY ZVYŠOVANIA ÚROVNE KYBERNETICKEJ BEZPEČNOSTI

„Aké sú faktory, ktoré majú vo vašej organizácii najvyšší vplyv na zvyšovanie úrovne kybernetickej bezpečnosti?"

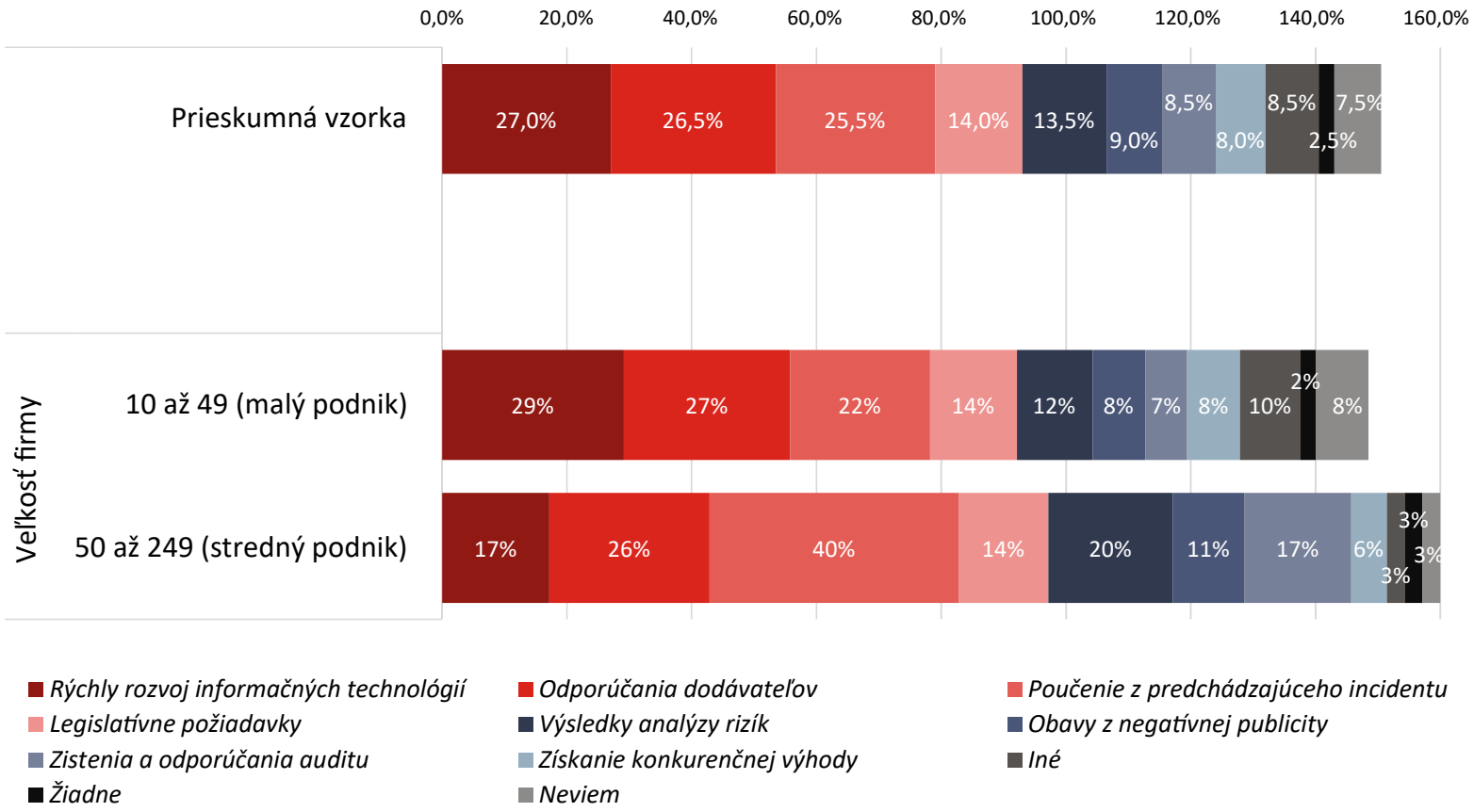
Odpovede všetkých respondentov



1.3 FAKTORY ZVYŠOVANIA ÚROVNE KYBERNETICKEJ BEZPEČNOSTI

„Aké sú faktory, ktoré majú vo vašej organizácii najvyšší vplyv na zvyšovanie úrovne kybernetickej bezpečnosti?"

Odpovede podľa štruktúry podnikov



V porovnaní s priemerným výsledkom uvádzali **stredné podniky** častejšie tieto faktory:

- Poučenie z predchádzajúceho incidentu
- Výsledky analýzy rizík
- Zistenia a odporúčania auditu

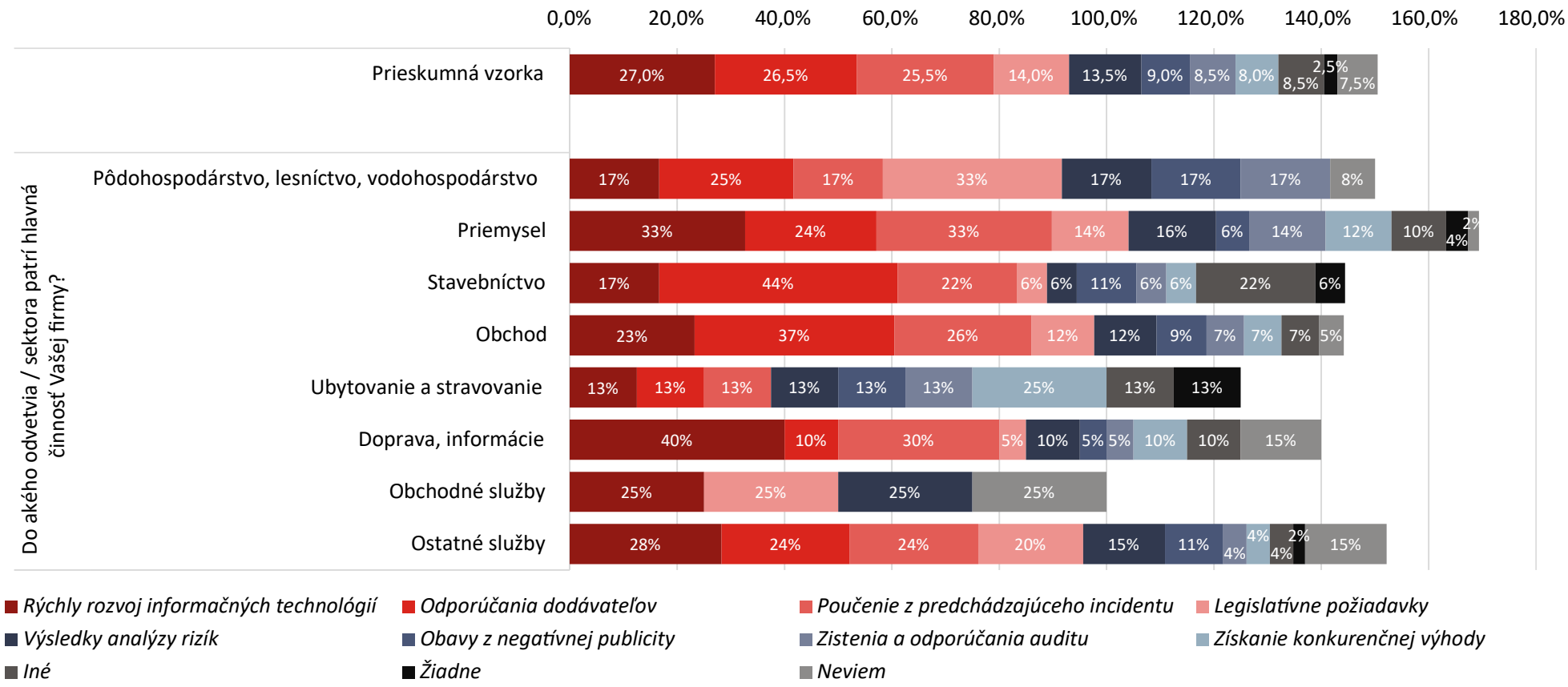
Malé podniky mierne nadpriemerne uvádzali všeobecný faktor:

- Rýchly rozvoj IT a Iné faktory

1.3 FAKTORY ZVYŠOVANIA ÚROVNE KYBERNETICKEJ BEZPEČNOSTI

„Aké sú faktory, ktoré majú vo vašej organizácii najvyšší vplyv na zvyšovanie úrovne kybernetickej bezpečnosti?"

Odpovede podľa štruktúry podnikov



PRIEBEŽNÉ ZHRNUTIE – FAKTORY ZVYŠOVANIA ÚROVNE KB

Najčastejšie označovaným **faktorom,** ktorý má vplyv **na zvyšovanie kybernetickej bezpečnosti** v podniku, je **„Rýchly rozvoj IT"** – tento faktor označilo 27% respondentov. V porovnaní s priemerným výsledkom ide častejšie o malé firmy a podniky pôsobiace v sektore doprava, informácie a priemysel.

Odporúčania dodávateľov majú výrazný vplyv na zvyšovanie úrovne kybernetickej bezpečnosti. **Faktor „Odporúčania dodávateľov" uviedlo až 26,5%,** nadpriemerne to boli podniky zo sektorov obchod a stavebníctvo.

Tretím, najčastejšie označovaným faktorom bolo **„Poučenie z predchádzajúceho incidentu",** ktorý označila štvrtina opýtaných MSP **(25,5%).** Nadpriemerne išlo o stredne veľké podniky a zo sektorov priemysel a doprava. Štvrtina podnikov už má skúsenosti s incidentom. Incidenty sa objavujú viac v stredných podnikoch (50-249 zamestnancov), ako v malých podnikoch (10-49 zamestnancov).

14% podnikov uviedlo **„legislatívne požiadavky",** nadpriemerne viac boli zastúpené firmy zo sektorov pôdohospodárstvo, obchodné a ostatné služby.

„Výsledky analýzy rizík" sú relevantným faktorom na zvyšovanie KB pre **13,5%** opýtaných podnikov. Tento faktor nadpriemerne označovali stredné podniky a firmy zo sektorov priemysel, pôdohospodárstvo a služby.

9% opýtaných uviedlo ako faktor aj „**Obavy z negatívnej publicity",** častejšie to boli stredné podniky a nadpriemerne firmy zo sektorov pôdohospodárstvo, stavebníctvo a ostatné služby.

Vplyv na zvyšovanie KB mali pre **8,5%** MSP aj **„Zistenia a odporúčania auditu".** Tento faktor mierne častejšie označovali stredné podniky, a nadpriemerne firmy zo sektorov pôdohospodárstvo a priemysel.

„Získanie konkurenčnej výhody" uviedlo 8% MSP, nadpriemerne boli zastúpené firmy zo sektorov ubytovanie a stravovanie, doprava a priemysel.

8,5% opýtaných MSP uviedlo iné faktory, **2,5%** uviedlo, že na zvyšovanie KB nemajú vplyv žiadne faktory (výrazne nadpriemerne v sektore ubytovanie a stravovanie) a 7,5% respondentov nevedelo odpovedať.

Boom povinností, súvisiacich s implementáciou požiadaviek GDPR ovplyvnil vnímanie štatutárov v zmysle presvedčenia, že majú zároveň splnené aj povinnosti v kontexte kybernetickej bezpečnosti.

Všeobecné nariadenie EÚ o ochrane údajov negatívne ovplyvnilo presvedčenie štatutárov, že opatreniami aj v kybernetickej bezpečnosti sú najmä organizačné opatrenia.

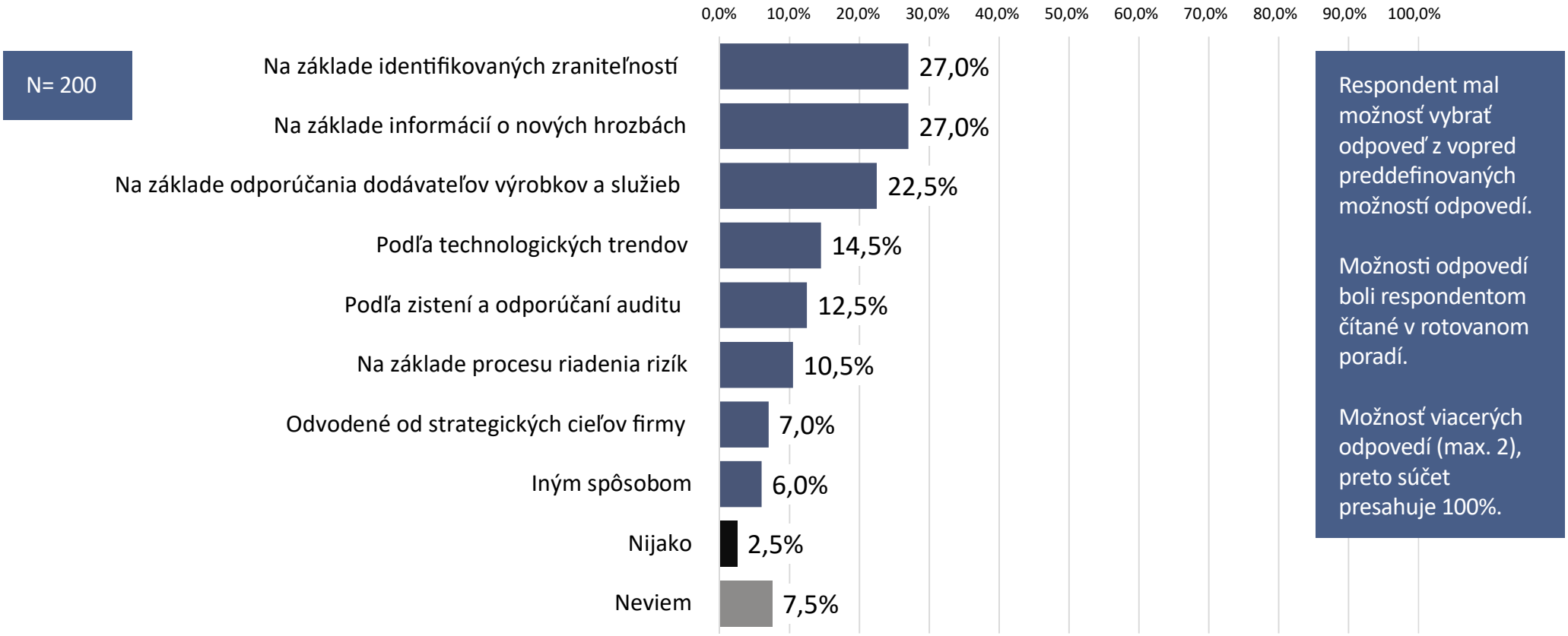
1.4 FAKTORY DEFINOVANIA PRIORÍT A SMEROVANIA KB

„Podľa čoho definujete vo vašej organizácii priority a smerovanie pre oblasť kybernetickej bezpečnosti?“

1.4 FAKTORY DEFINOVANIA PRIORÍT A SMEROVANIA KB

„Podľa čoho definujete vo vašej organizácii priority a smerovanie pre oblasť kybernetickej bezpečnosti?"

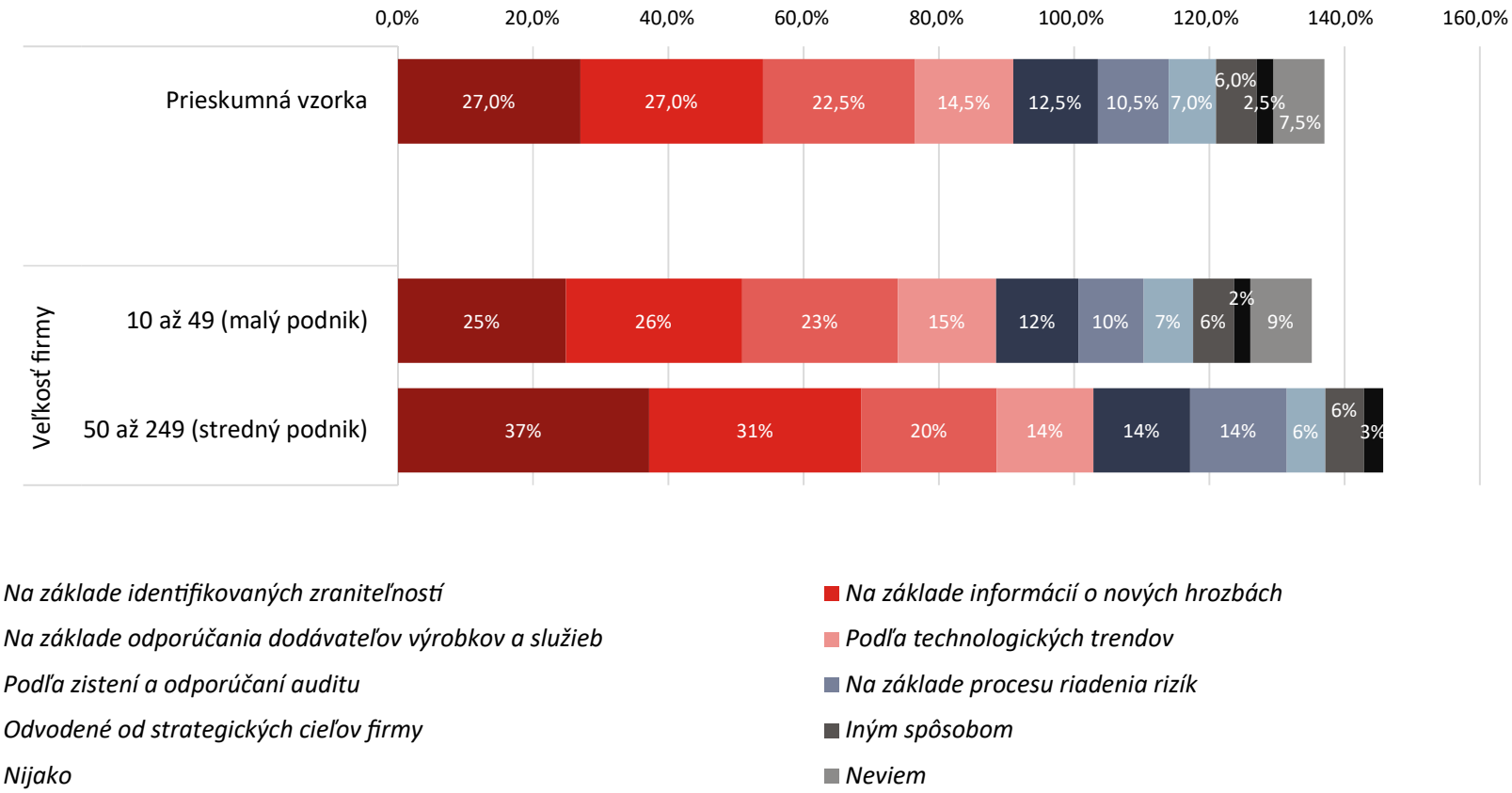
Odpovede všetkých respondentov



1.4 FAKTORY DEFINOVANIA PRIORÍT A SMEROVANIA KB

„Podľa čoho definujete vo vašej organizácii priority a smerovanie pre oblasť kybernetickej bezpečnosti?"

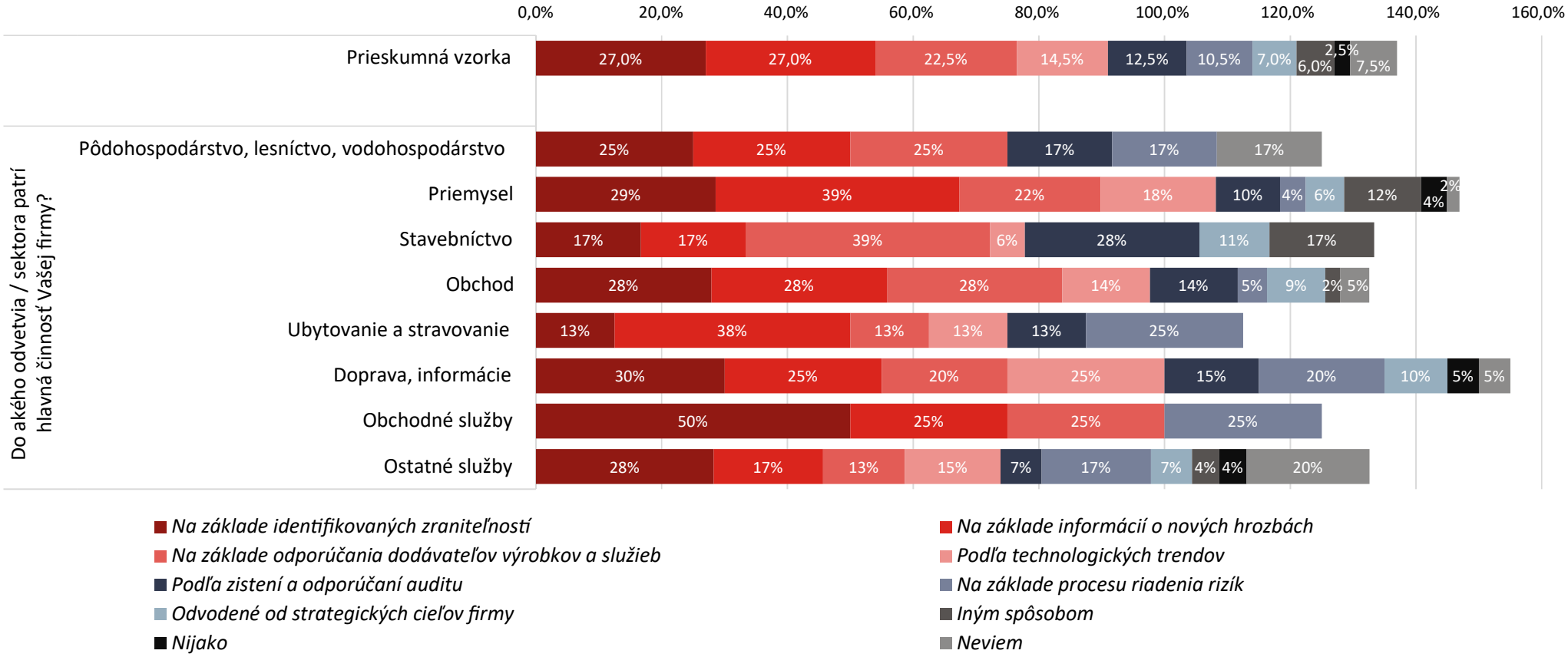
Odpovede podľa štruktúry podnikov



1.4 FAKTORY DEFINOVANIA PRIORÍT A SMEROVANIA KB

„Podľa čoho definujete vo vašej organizácii priority a smerovanie pre oblasť kybernetickej bezpečnosti?"

Odpovede podľa štruktúry podnikov



PRIEBEŽNÉ ZHRNUTIE - FAKTORY DEFINOVANIA PRIORÍT A SMEROVANIA KB

MSP definujú **priority a smerovanie pre oblasť KB** najčastejšie na základe **„identifikovaných zraniteľností" (27%).** Nadpriemerne takto odpovedali stredné podniky a firmy zo sektorov obchodné služby a doprava, informácie.

Rovnakou mierou **(27%)** boli zastúpené odpovede na základe **„informácií o nových hrozbách",** častejšie u stredne veľkých firiem; z oblastí priemysel a ubytovanie/stravovanie.

„Odporúčania dodávateľov výrobkov a služieb" rešpektuje pri definovaní priorít KB viac ako pätina MSP **(22,5%).** Medzi podnikmi, ktoré označili túto odpoveď, boli nadpriemerne zastúpené firmy zo sektorov stavebníctvo, obchod, obchodné služby a pôdohospodárstvo.

„Podľa technologických trendov" nastavuje priority KB **14,5%** opýtaných MSP. Nadpriemerne tento parameter uvádzali podniky z oblasti dopravy, informácií a priemyslu.

„Podľa zistení a odporúčaní auditu" definuje priority a smerovanie v oblasti KB v **12,5%** MSP. Oproti priemeru boli mierne viac zastúpené stredné podniky a výrazne nadpriemerne stavebné firmy a nadpriemerne firmy zo sektorov pôdohospodárstvo, doprava a obchod.

Približne desatina MSP **(10,5%)** definuje priority KB na základe **„procesu riadenia rizík".** Oproti priemeru tento variant častejšie vyberali stredné podniky a nadpriemerne firmy zo sektorov ubytovanie, doprava/informácie, obchodné a ostatné služby, pôdohospodárstvo.

Napriek tomu, že väčšina právnych a technických noriem zdôrazňuje potrebu odvodenia bezpečnostnej stratégie od strategických cieľov podniku, iba **7%** podnikov uviedlo, že definícia priorít a smerovania pre oblasť kybernetickej bezpečnosti je odvodená od strategických, rep. obchodných cieľov. Kyberbezpečnosť typicky nie je súčasťou strategických cieľov MSP. Oproti priemeru mierne viac rezorty stavebníctvo, doprava a obchod. Štatutári MSP nevedia stanoviť dôveryhodnosť zdrojov, na základe ktorých môžu definovať priority a smerovanie pre oblasť kybernetickej bezpečnosti. (odpovede sú najmä typu „Neviem ako som sa to dozvedel a neviem prečo to robím")

6% opýtaných MSP uviedlo iné faktory, **2,5%** uviedlo, že n**a zvyšovanie KB nemajú vplyv žiadne faktory** (nadpriemerne v sektore doprava, informácie) a 7,5% respondentov nevedelo odpovedať.

Definícia priorít a smerovania pre oblasť kybernetickej bezpečnosti nie je u MSP pragmatická a preventívna (t.j. nie je odvodená od strategických cieľov, ani od riadenia rizík, alebo od zistení auditu).

1.5 TYPY KYBERNETICKÝCH INCIDENTOV V MSP

„Zo všetkých zaznamenaných kybernetických incidentov vo vašej organizácii, koľko percent bolo:

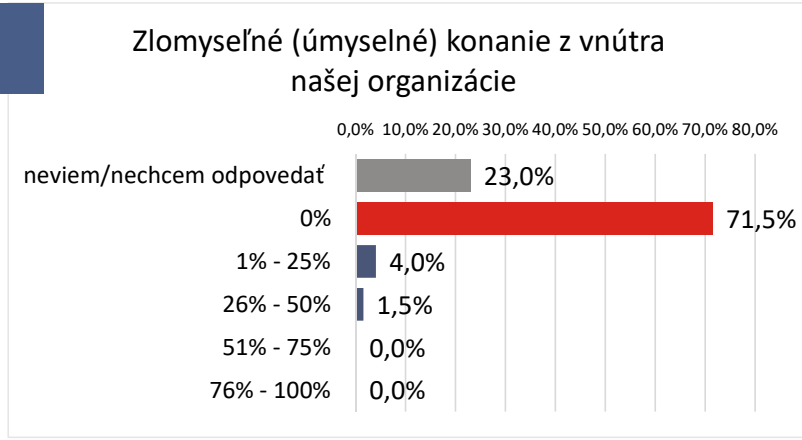
1. Zlomyseľné (úmyselné) konanie z vnútra našej organizácie (napr. interného zamestnanca) .....%
2. Zlomyseľné (úmyselné) konanie z vonkajšieho prostredia (niekto mimo našej organizácie).....%
3. Systémové zlyhanie .....%
4. Ľudská chyba .....%

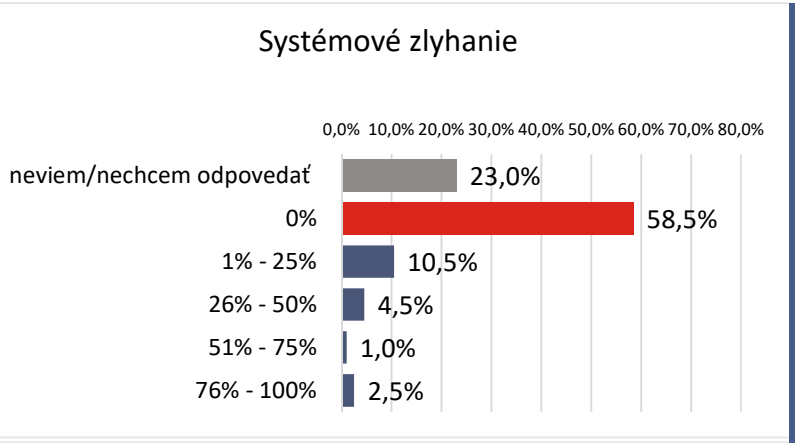
1.5 TYPY KYBERNETICKÝCH INCIDENTOV V MSP

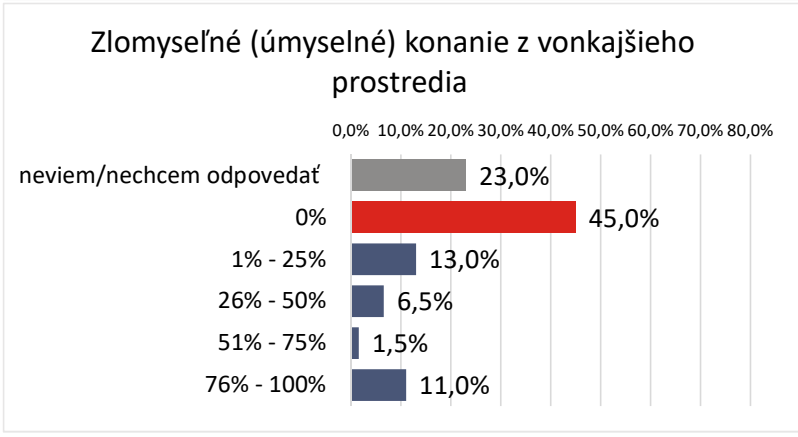
„Zo všetkých zaznamenaných kybernetických incidentov vo vašej organizácii, koľko percent bolo približne:

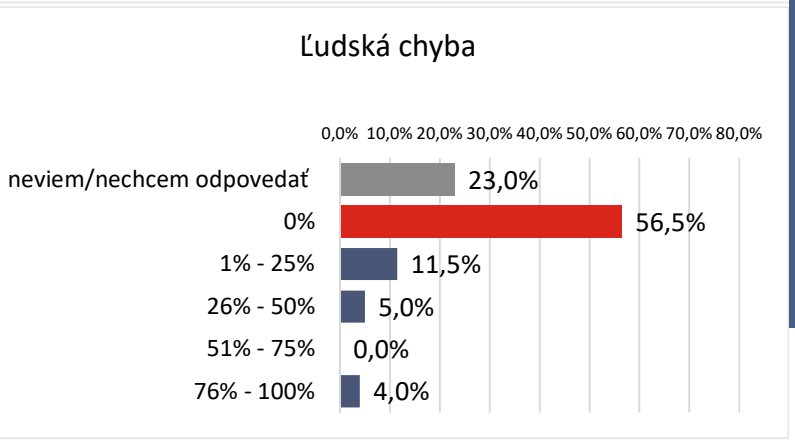
Odpovede všetkých respondentov

N= 200









Respondent sa vyjadroval ku každej možnosti spontánne.

Odpovede boli kategorizované.

Možnosti odpovedí boli respondentom čítané v rotovanom poradí.

Súčet percentuálnych hodnôt všetkých možností mohol presahovať 100%.

PRIEBEŽNÉ ZHRNUTIE - TYPY KYBERNETICKÝCH INCIDENTOV V MSP

- Z odpovedí vyplýva, že respondenti nie bezpodmienečne rozlišujú pojem **„incident“,**
- respondenti vnímajú len incidenty, ktoré sú zjavné (ktoré spôsobili reálny dopad), do úvah nezahŕňajú incidenty, ktoré potenciálne prebiehajú alebo ktoré doteraz neboli identifikované,
- Podniky usudzujú, že prevládajú útoky z vonkajšej strany sieťového perimetra,
- Podvedomé vnímanie kategorizácie zdroja incidentov (úmyselné konanie, ľudská chyba, systémové zlyhanie) sa zhoduje s globálne ustálenou kategorizáciou.

2. ÚROVEŇ ZNALOSTÍ A SKÚSENOSTI ZAMESTNANCOV V OBLASTI KYBERNETICKEJ BEZPEČNOSTI V MSP

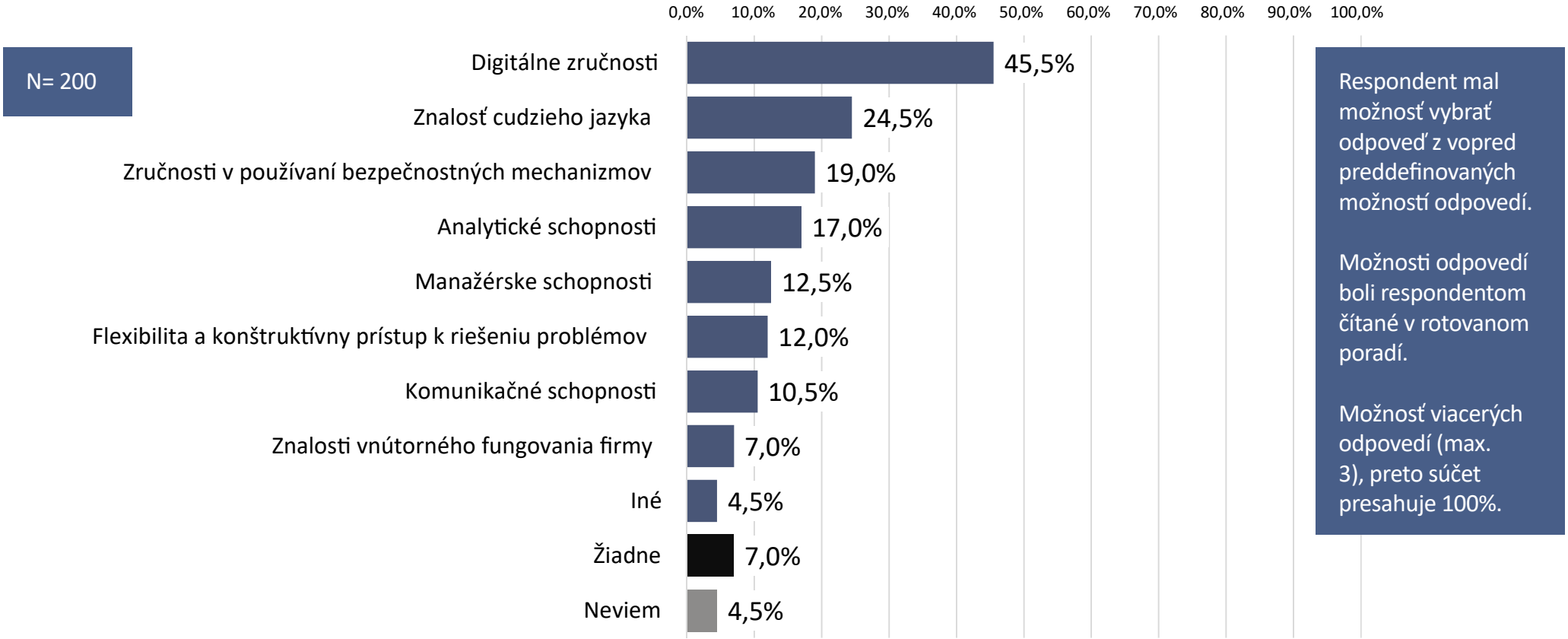
2.1 ÚROVEŇ ZNALOSTÍ A SKÚSENOSTI ZAMESTNANCOV V OBLASTI KYBERNETICKEJ BEZPEČNOSTI

„Ktoré znalosti a skúsenosti zamestnancov vašej firmy považujete momentálne najviac za nedostatkové?“

2.1 KTORÉ ZNALOSTI A SKÚSENOSTI ZAMESTNANCOV SÚ NEDOSTATKOVÉ

„Ktoré znalosti a skúsenosti zamestnancov vašej firmy považujete momentálne najviac za nedostatkové?"

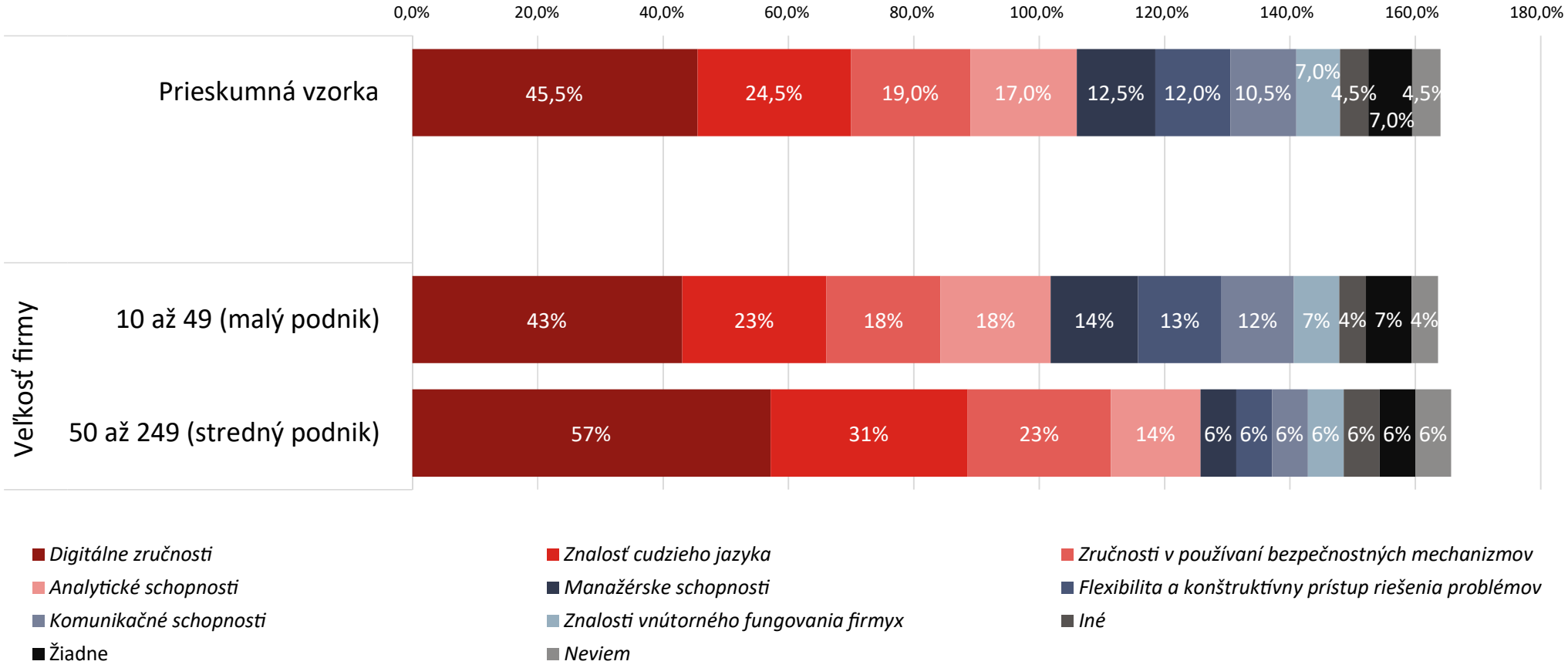
Odpovede všetkých respondentov



2.1 KTORÉ ZNALOSTI A SKÚSENOSTI ZAMESTNANCOV SÚ NEDOSTATKOVÉ

„Ktoré znalosti a skúsenosti zamestnancov vašej firmy považujete momentálne najviac za nedostatkové?"

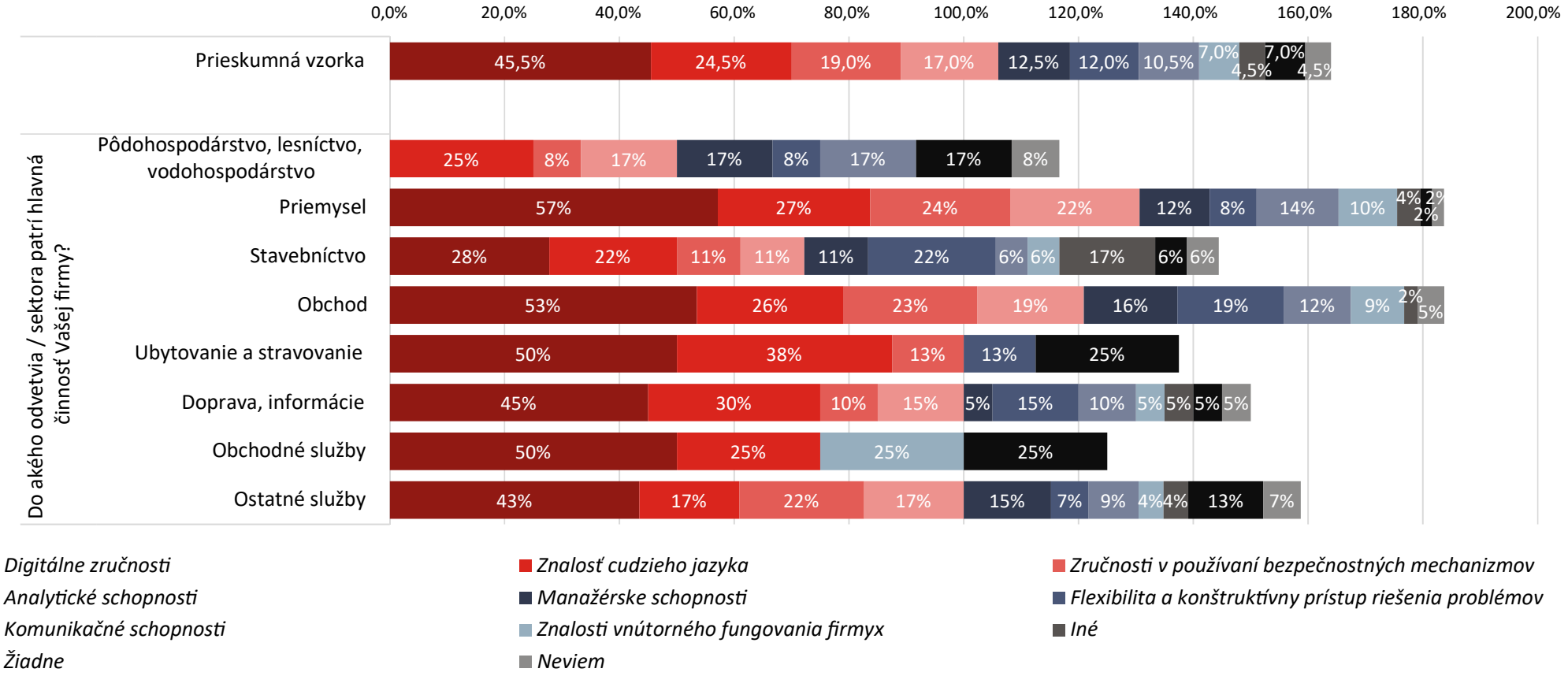
Odpovede podľa štruktúry podnikov



2.1 KTORÉ ZNALOSTI A SKÚSENOSTI ZAMESTNANCOV SÚ NEDOSTATKOVÉ

„Ktoré znalosti a skúsenosti zamestnancov vašej firmy považujete momentálne najviac za nedostatkové?"

Odpovede podľa štruktúry podnikov



PRIEBEŽNÉ ZHRNUTIE - KTORÉ ZNALOSTI A SKÚSENOSTI SÚ NEDOSTATKOVÉ

1. Medzi najviac **nedostatkové znalosti** zamestnancov sú správne považované najmä **digitálne zručnosti** u takmer polovice opýtaných MSP **(45,5%).** Z tých podnikov, ktoré digitálne zručnosti označili ako najviac nedostatkové, boli nadpriemerne zastúpené stredne veľké podniky; zo sektorov priemysel, obchod, ubytovanie a obchodné služby. Zamestnanci kladú pasívny odpor bezpečnostným opatreniam, pretože pri ich používaní sú bezprostredne konfrontovaní s nedostatkom vlastných bežných digitálnych zručností.
2. Znalosť **cudzieho jazyka – 24,5%;** nadpriemerne v stredných podnikoch a firmách zo sektorov ubytovanie/stravovanie, doprava/ informácie a priemysel.
3. **Zručnosti v používaní bezpečnostných mechanizmov uviedlo ako nedostatkové 19% opýtaných.** Častejšie to boli stredne veľké firmy; podniky z oblastí priemysel, obchod a ostatné služby.
4. **Analytické** schopnosti označilo ako nedostatkové **17%** podnikov, nadpriemerne zo sektorov priemysel a obchod.
5. **Manažérske zručnosti** u osminy opýtaných podnikov **(12,5%).** Z tých podnikov, ktoré manažérske zručnosti označili ako najviac nedostatkové, boli mierne nadpriemerne zastúpené malé podniky; zo sektorov pôdohospodárstvo, obchod, ubytovanie a ostatné služby.
6. **Flexibilita** a konštruktívny prístup k riešeniu problémov za nedostatočnú znalosť považuje **12%** MSP – oproti priemeru sú to najmä firmy z oblasti stavebníctva, obchodu a dopravy.
7. **Komunikačné** schopnosti – **10,5%;** mierne nadpriemerne chýbajú u zamestnancov v malých podnikoch a firmách z oblasti pôdohospodárstva, priemyslu a obchodu.
8. Znalosť **vnútorného fungovania** firmy – **12,5%;** nedostatkové nadpriemerne v sektoroch priemysel, obchod a obchodné služby.

Až **7%** z opýtaných **nevidí žiadne nedostatkové znalosti** svojich zamestnancov.

2.2 ŠKOLENIA ZAMESTNANCOV V OBLASTI KYBERNETICKEJ BEZPEČNOSTI

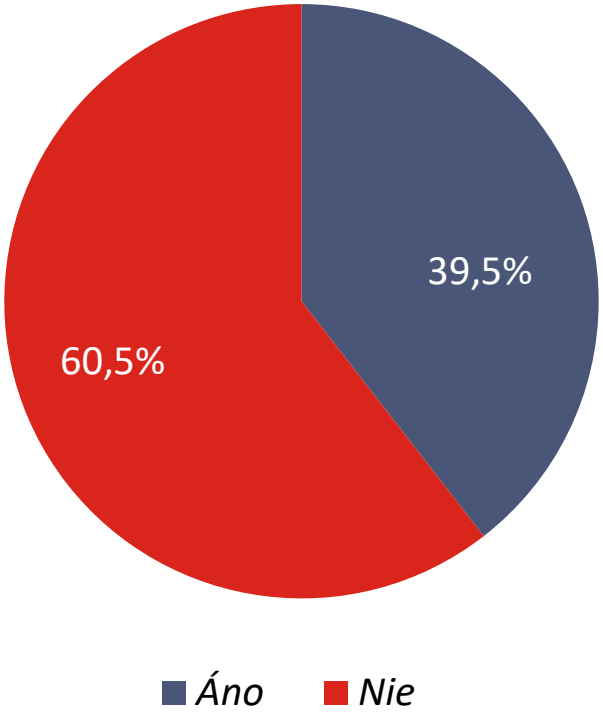
„Poskytujete svojim zamestnancom možnosti školenia na zvyšovanie ich znalostí a schopností v oblasti kybernetickej bezpečnosti?“

2.2 ŠKOLENIA ZAMESTNANCOV V OBLASTI KYBERNETICKEJ BEZPEČNOSTI

„Poskytujete svojim zamestnancom možnosti školenia na zvyšovanie ich znalostí a schopností v oblasti kybernetickej bezpečnosti?"

Odpovede všetkých respondentov

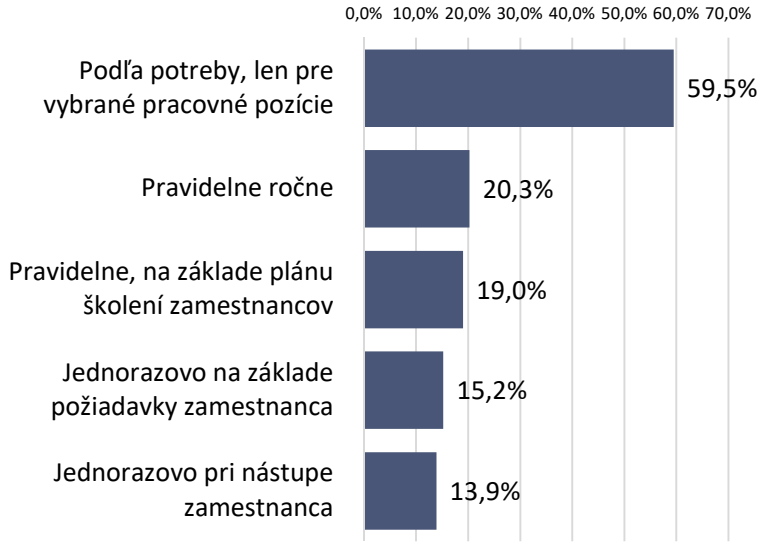
N= 200



Respondent mal možnosť vybrať odpoveď z vopred preddefinovaných možností odpovedí. Možnosť viacerých odpovedí.

Ak áno, na základe akého podnetu, akej požiadavky?

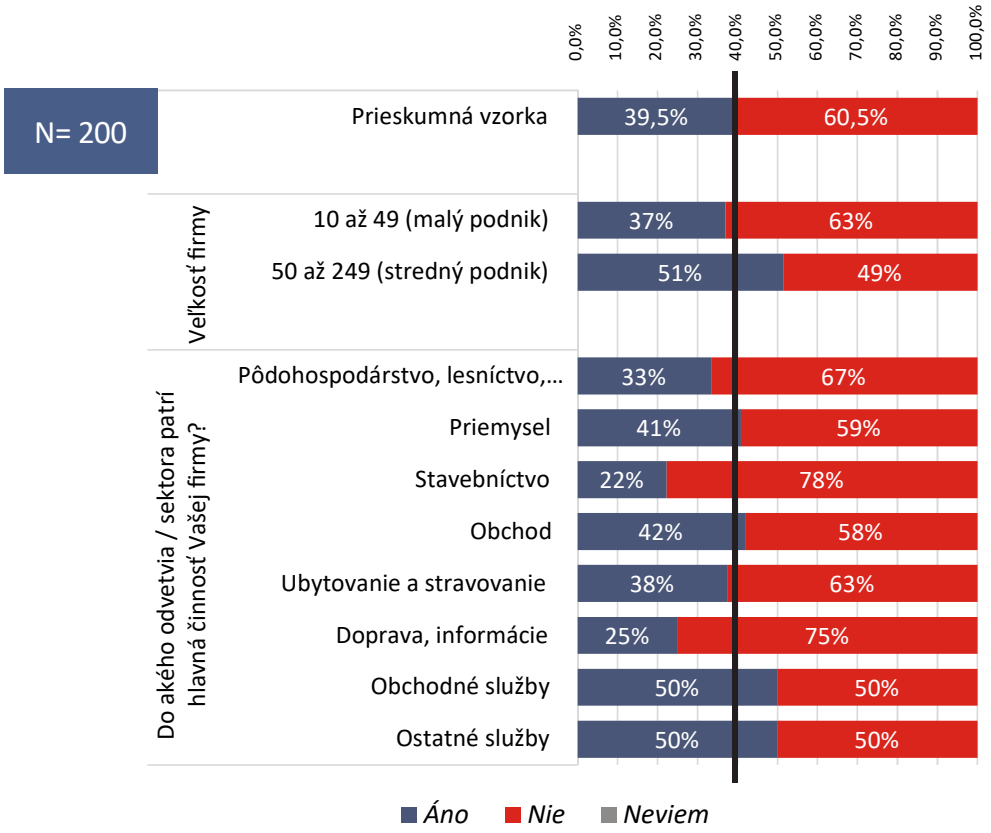
N= 79

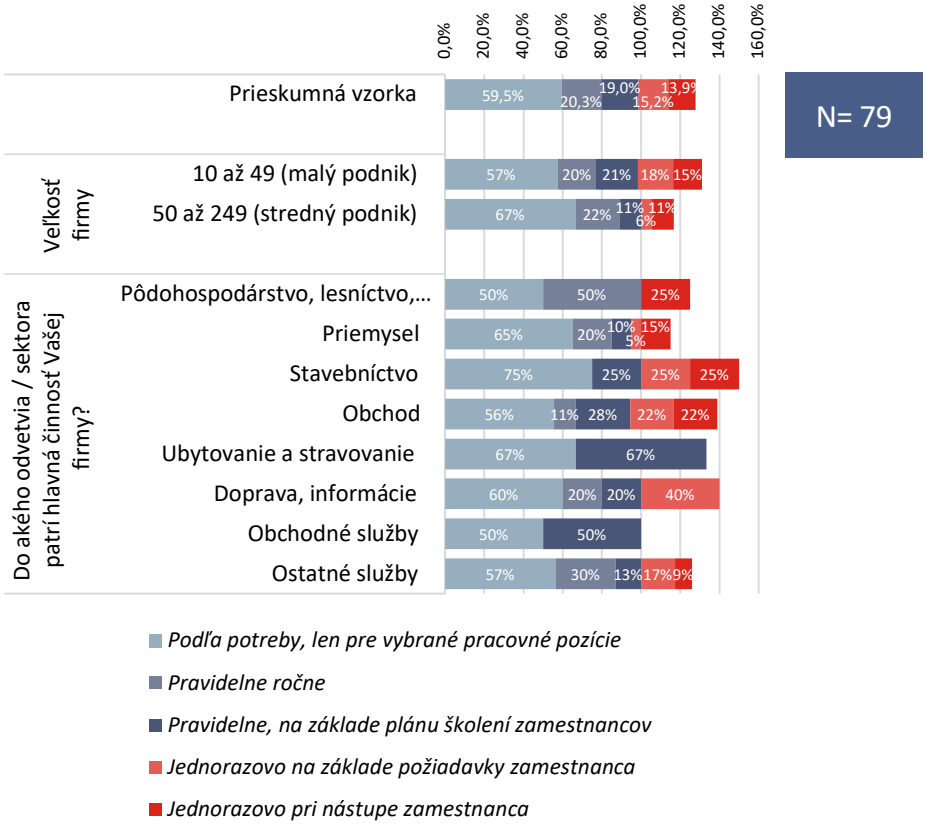


2.2 ŠKOLENIA ZAMESTNANCOV V OBLASTI KYBERNETICKEJ BEZPEČNOSTI

„Poskytujete svojim zamestnancom možnosti školenia na zvyšovanie ich znalostí a schopností v oblasti kybernetickej bezpečnosti?"

Odpovede podľa štruktúry podnikov



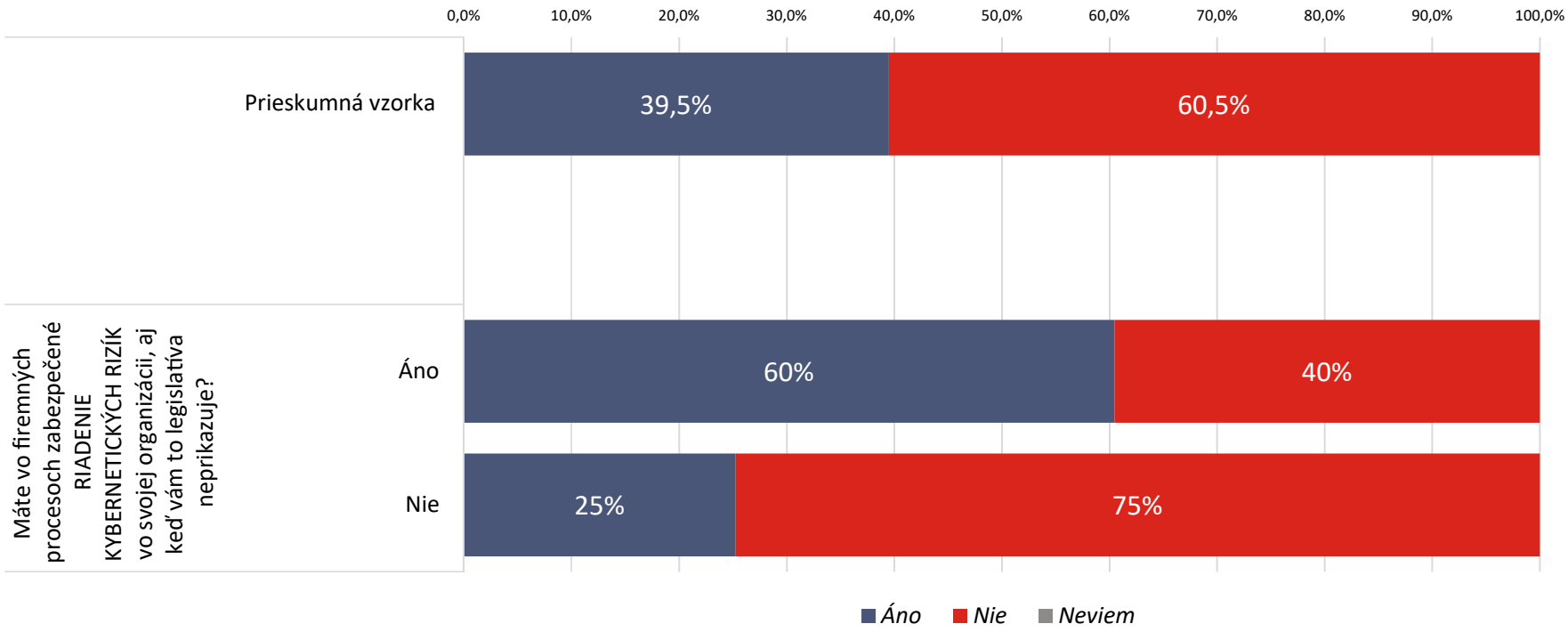


2.2 ŠKOLENIA ZAMESTNANCOV V OBLASTI KYBERNETICKEJ BEZPEČNOSTI

„Poskytujete svojim zamestnancom možnosti školenia na zvyšovanie ich znalostí a schopností v oblasti kybernetickej bezpečnosti?“

Odpovede podľa toho, či majú zabezpečené riadenie kybernetických rizík

N= 200



PRIEBEŽNÉ ZHRNUTIE - ŠKOLENIA ZAMESTNANCOV V OBLASTI KB

Štyri z desiatich MSP (39,5%) deklarujú, že **poskytujú zamestnancom školenia** na zvyšovanie ich znalostí a schopností **v oblasti kybernetickej bezpečnosti.** Oproti minulému roku bol zaznamenaný nárast o osem percentuálnych bodov (z 31,9% na 39,5%).

Oproti priemernému výsledku ide častejšie o tie MSP, ktoré majú zabezpečené riadenie kybernetických rizík, i keď im to legislatíva neprikazuje; o stredne veľké podniky a podniky pôsobiace v sektoroch obchodné a ostatné služby. V odpovediach je nezvyčajne vysoké percento negatívnych odpovedí (60,5%), avšak: vzhľadom na to, že povinnosť vzdelávania nie je zákonnou povinnosťou MSP, z negatívnych odpovedí nevyplývajú sankcie a preto odpovede možno považovať za pravdivé.

V tých MSP, v ktorých takéto školenia v oblasti KB poskytujú, ide najčastejšie o a**d hoc školenia len pre vybrané** pracovné pozície (59,5%). Podniky, ktoré v predchádzajúcich odpovediach uviedli, že vykonávajú riadenie rizík, väčšinou tvrdia, že vykonávajú aj školenia; avšak: pokiaľ by však odpovede na otázku riadenie rizík boli pravdivé, respondenti nemohli by pripustiť, že viac ako 40% zamestnancov neabsolvuje žiadne školenie v kybernetickej bezpečnosti.

Pätina opýtaných realizuje pravidelné školenia **raz ročne (20,3%).**

Pravidelne, na základe plánu školení zamestnancov poskytuje **19%** MSP.

15,2% MSP uviedlo, že zamestnancov školia **jednorazovo na základe požiadavky zamestnanca.** Takmer 2/3 respondentov si myslí, že školenia v kybernetickej bezpečnosti potrebujú len špecialisti.

13,9% respondentov uviedlo, že zamestnancov v oblasti KB školia jednorazovo pri nástupe.

3. STRATÉGIA A IMPLEMENTÁCIA KYBERNETICKEJ BEZPEČNOSTI V MSP

3.1 PODĽA AKÝCH TECHNICKÝCH / PRÁVNYCH NORIEM POSTUPUJÚ

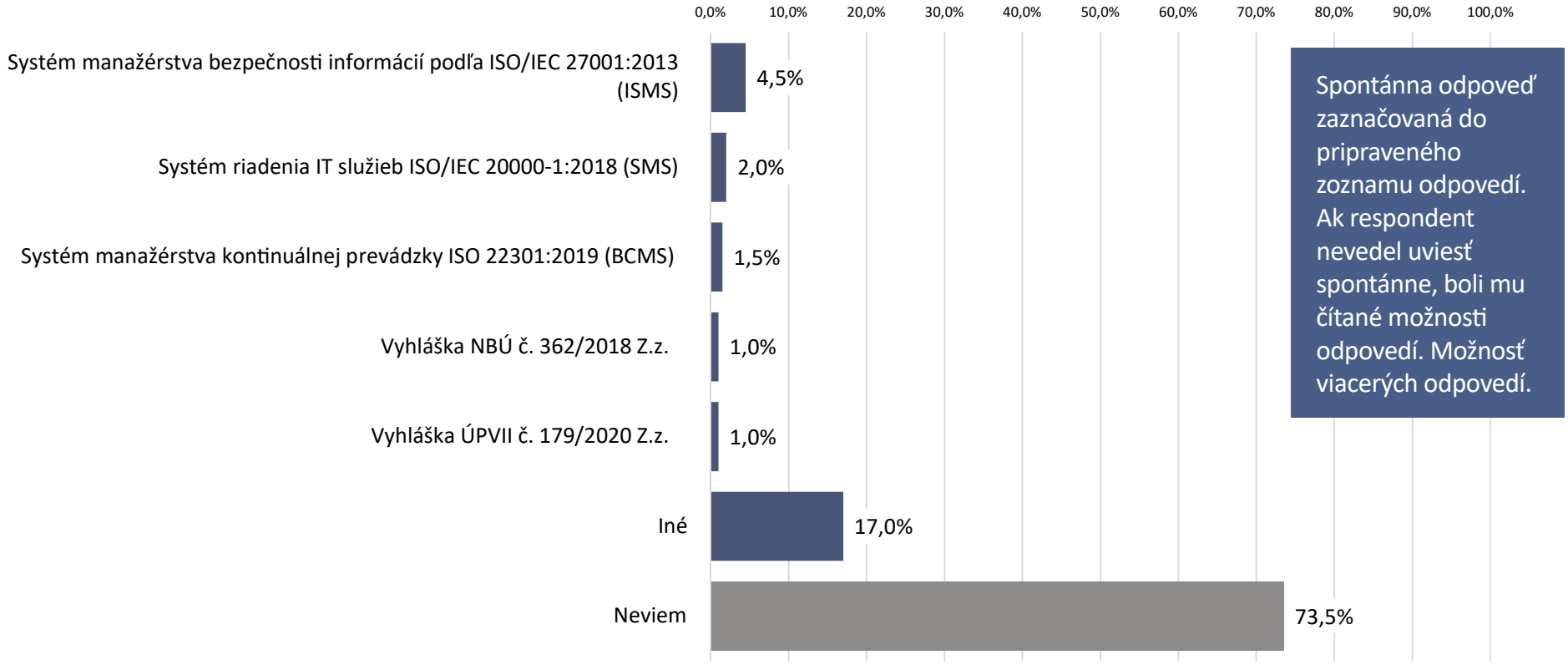
„Podľa ktorej technickej alebo právnej normy postupujete pri implementácii bezpečnostných opatrení v kybernetickej bezpečnosti?"

3.1 PODĽA AKÝCH TECHNICKÝCH / PRÁVNYCH NORIEM POSTUPUJÚ

„Podľa ktorej technickej alebo právnej normy postupujete pri implementácii bezpečnostných opatrení v kybernetickej bezpečnosti?"

Odpovede všetkých respondentov

N= 200

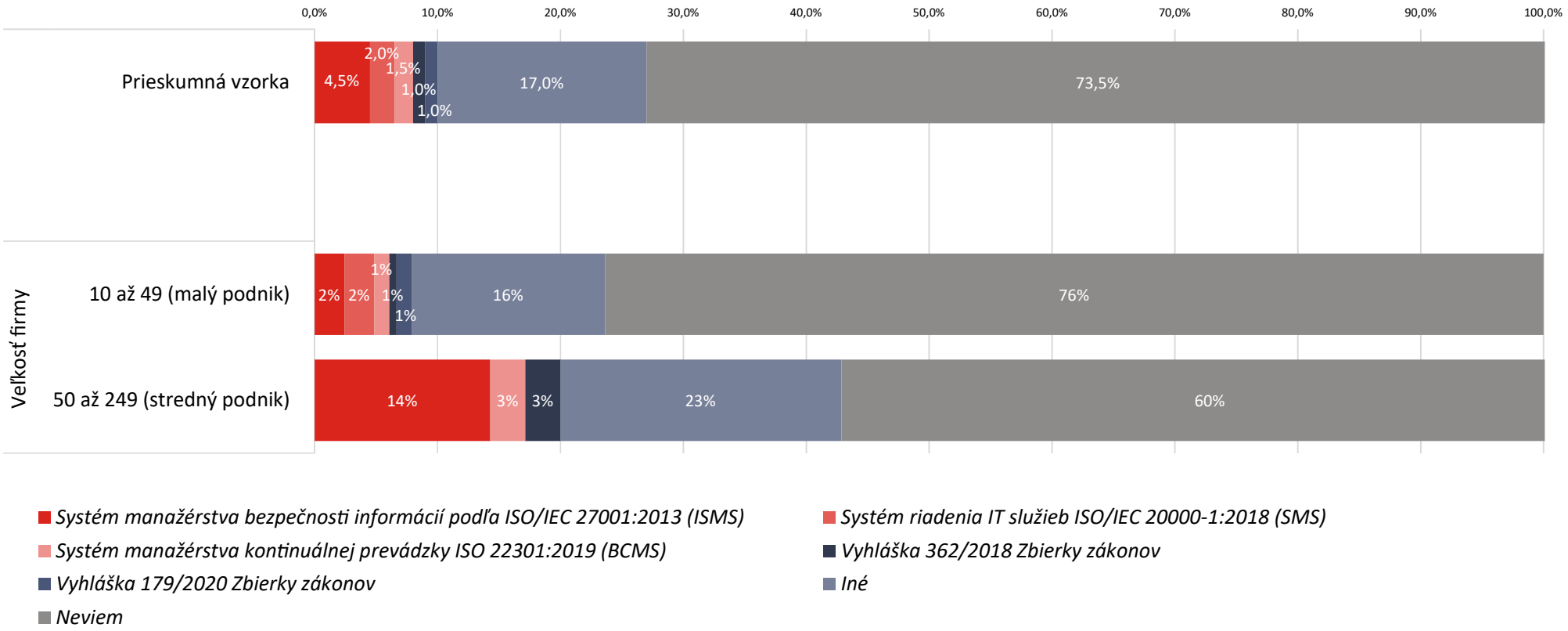


Spontánna odpoveď zaznačovaná do pripraveného zoznamu odpovedí. Ak respondent nevedel uviesť spontánne, boli mu čítané možnosti odpovedí. Možnosť viacerých odpovedí.

3.1 PODĽA AKÝCH TECHNICKÝCH / PRÁVNYCH NORIEM POSTUPUJÚ

„Podľa ktorej technickej alebo právnej normy postupujete pri implementácii bezpečnostných opatrení v kybernetickej bezpečnosti?"

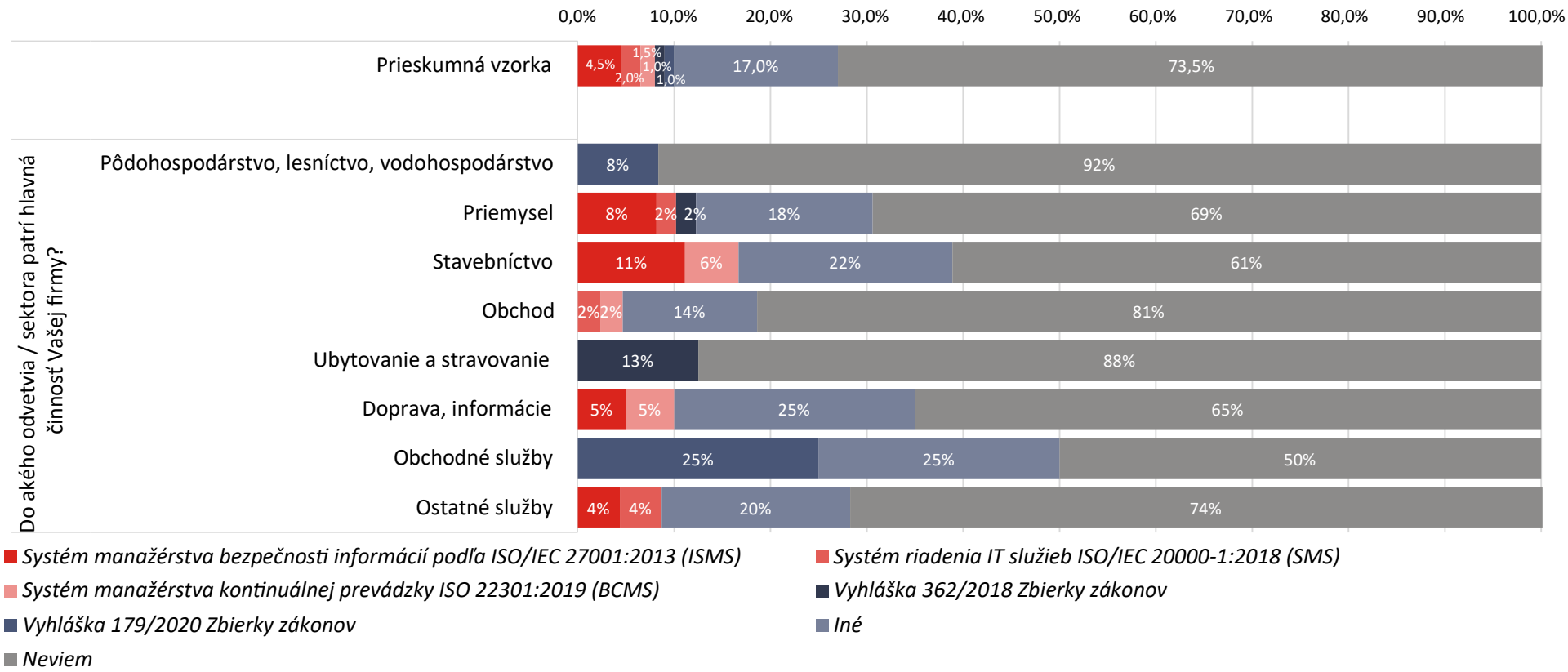
Odpovede podľa štruktúry podnikov



3.1 PODĽA AKÝCH TECHNICKÝCH / PRÁVNYCH NORIEM POSTUPUJÚ

„Podľa ktorej technickej alebo právnej normy postupujete pri implementácii bezpečnostných opatrení v kybernetickej bezpečnosti?"

Odpovede podľa štruktúry podnikov



PRIEBEŽNÉ ZHRNUTIE – VYUŽÍVANÉ TECHNICKÉ / PRÁVNE NORMY

V navrhovaných odpovediach boli uvedené všetky relevantné právne a technické predpisy z ktorých by sa podniky mohli inšpirovať pri implementácii opatrení. Negatívnym zistením je, že ani jeden z uvedených predpisov nie je súčasťou všeobecného povedomia.

Takmer tri štvrtiny (73,5%) opýtaných MSP **nevedeli** uviesť, podľa ktorej technickej alebo právnej normy postupujú pri implementácii bezpečnostných opatrení v kybernetickej bezpečnosti.

- Systém manažérstva bezpečnosti informácií podľa ISO/IEC 27001:2013 (ISMS) pri implementácii bezpečnostných opatrení v KB využíva 4,5% opýtaných MSP. Nadpriemerne stredne veľké podniky; zo sektorov priemysel a stavebníctvo.
- Podľa Systému riadenia IT služieb ISO/IEC 20000-1:2018 (SMS) postupuje 2% respondentov. Nadpriemerne často sú to firmy z oblasti ostatných služieb.
- Systém manažérstva kontinuálnej prevádzky ISO 22301:2019 (BCMS) využíva 1,5% opýtaných. Nadpriemerne stredne veľké podniky; zo sektorov stavebníctvo a doprava.
- Podľa Vyhlášky NBÚ č. 362/2018 Z. z. postupuje 1% opýtaných MSP. Nadpriemerne stredne veľké podniky; firmy z oblasti ubytovania a stravovania.
- Podľa Vyhlášky ÚPVII č. 179/2020 Z. z. postupuje 1% oslovených MSP. Nadpriemerne často sú to firmy z oblasti obchodných služieb a pôdohospodárstva.
- Iné technické a legislatívne normy uviedlo 17% opýtaných.

3.2 ANALÝZA RIZÍK V OBLASTI KYBERNETICKEJ BEZPEČNOSTI

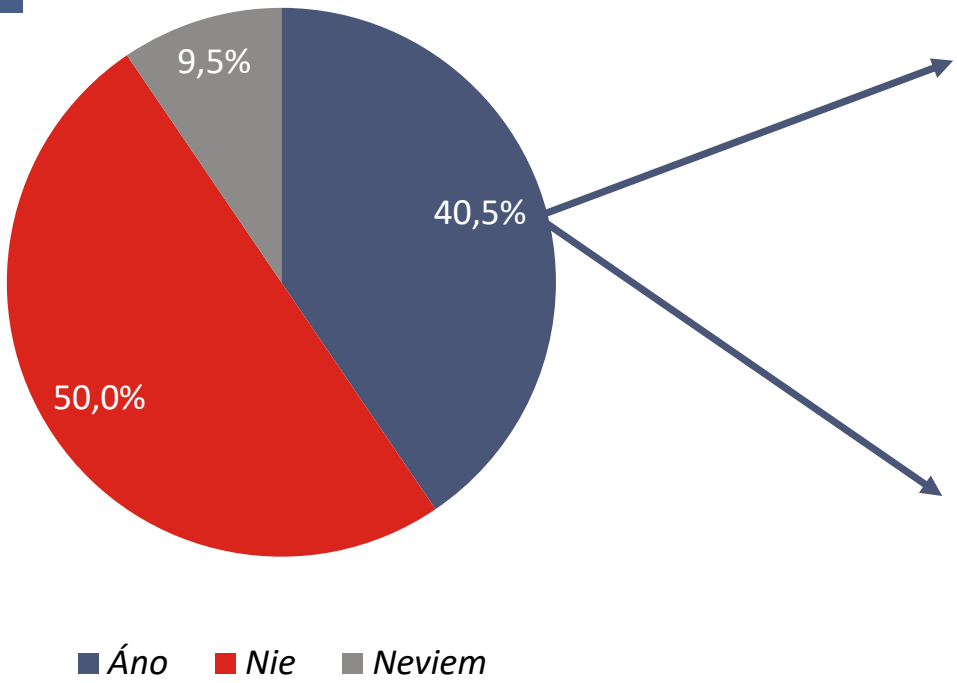
„Má vaša firma vypracovanú analýzu rizík v oblasti kybernetickej bezpečnosti?“

3.2 ANALÝZA RIZÍK V OBLASTI KYBERNETICKEJ BEZPEČNOSTI

„Má vaša firma vypracovanú analýzu rizík v oblasti kybernetickej bezpečnosti?"

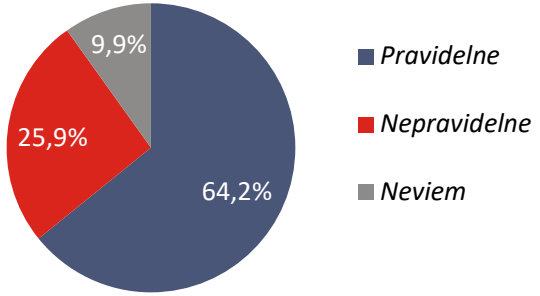
Odpovede všetkých respondentov

N= 200

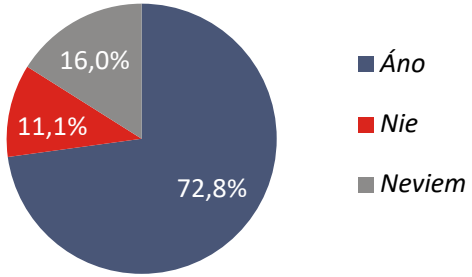


Ak áno: Ako často analýzu rizík aktualizujete?

N= 81



Ak áno: Je táto analýza založená na štandardizovanom procese riadenia rizík?



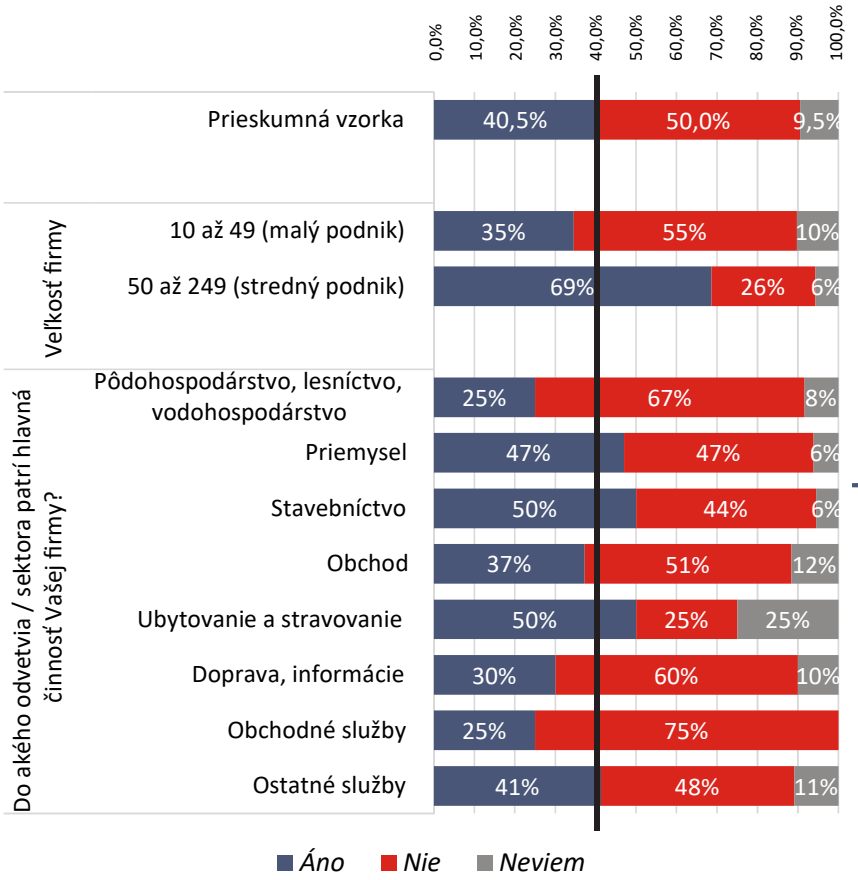
Respondent mal možnosť vybrať odpoveď z vopred preddefinovaných možností odpovedí. Možnosť len jednej odpovede.

3.2 ANALÝZA RIZÍK V OBLASTI KYBERNETICKEJ BEZPEČNOSTI

„Má vaša firma vypracovanú analýzu rizík v oblasti kybernetickej bezpečnosti?"

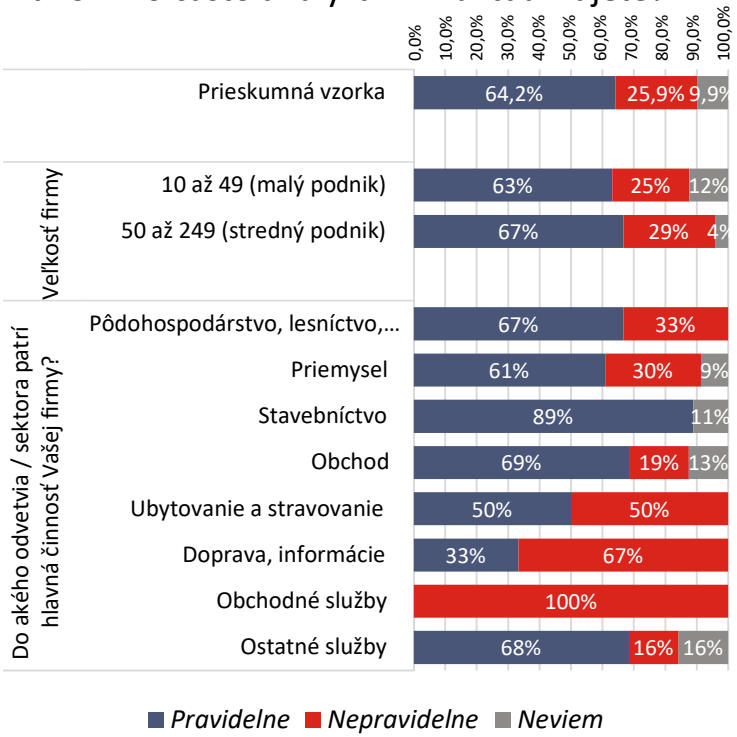
Odpovede podľa štruktúry podnikov

N= 200



Ak áno: Ako často analýzu rizík aktualizujete?

N= 81

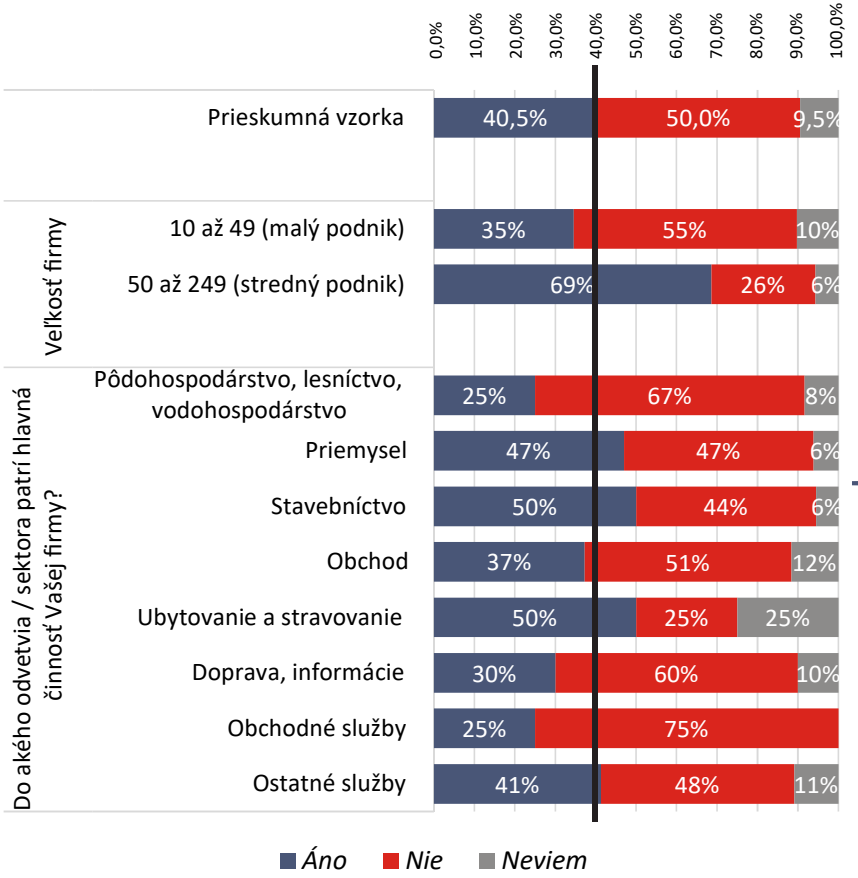


3.2 ANALÝZA RIZÍK V OBLASTI KYBERNETICKEJ BEZPEČNOSTI

„Má vaša firma vypracovanú analýzu rizík v oblasti kybernetickej bezpečnosti?"

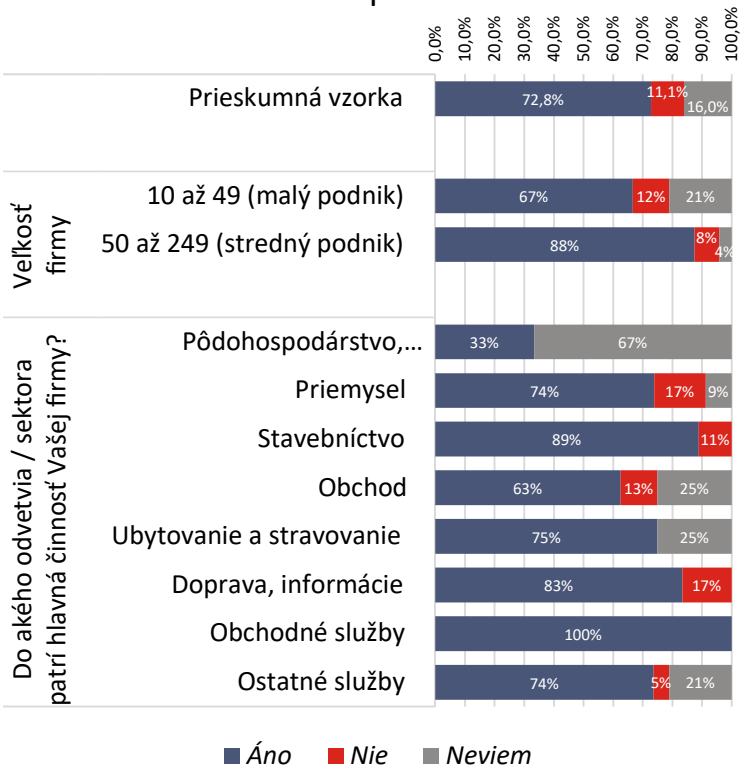
Odpovede podľa štruktúry podnikov

N= 200



Ak áno: Je táto analýza založená na štandardizovanom procese riadenia rizík?

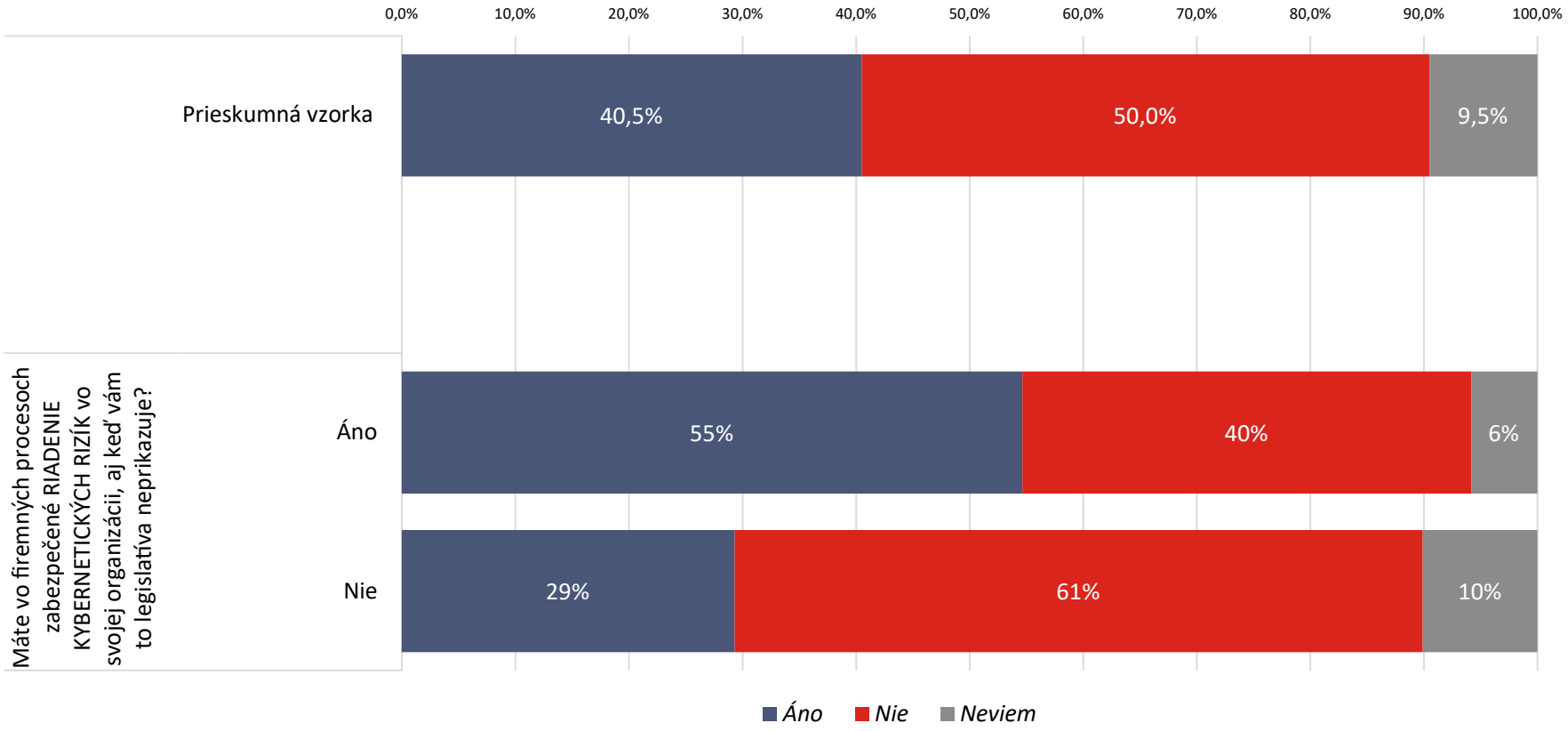
N= 81



3.2 ANALÝZA RIZÍK V OBLASTI KYBERNETICKEJ BEZPEČNOSTI

„Má vaša firma vypracovanú analýzu rizík v oblasti kybernetickej bezpečnosti?"

Odpovede podľa toho, či majú zabezpečené riadenie kybernetických rizík



PRIEBEŽNÉ ZHRNUTIE - ANALÝZA RIZÍK V OBLASTI KB

Otázka je kontrolnou (krížovou) otázkou, nadväzujúcou na otázku, či podniky majú zabezpečené riadenie kybernetických rizík, aj keď im to legislatíva neprikazuje.

Odpovede potvrdzujú pôvodné zistenie, že iba **25%** podnikov sa reálne a štandardne zaoberá riadením rizík.

Odpoveď respondenta, že analýzu rizík podnik vykonáva nepravidelne, sa dá interpretovať ako klamlivá, t.j. že podnik v skutočnosti nemá implementovaný proces riadenia rizík.

Štyri z desiatich opýtaných MSP (40,5%) majú **vypracovanú analýzu rizík** v oblasti kybernetickej bezpečnosti (oproti minulému roku nárast o 14,5 percentuálneho bodu).

- 64,2% z nich ju aj pravidelne aktualizuje.
- U 72,8% z nich je táto analýza založená na štandardizovanom procese riadenia rizík.

Analýzu rizík KB má vypracovanú takmer polovica stredných podnikov (69%) a 67% z nich ju aj pravidelne aktualizuje. U 88% z nich je táto analýza založená na štandardizovanom procese riadenia rizík.

Analýzu rizík v oblasti KB majú oproti priemeru častejšie vypracovanú nadpriemerne podniky v oblasti:

- **stavebníctva (**50%) a 89% z nich ju aj pravidelne aktualizuje. U 89% z nich je táto analýza založená na štandardizovanom procese riadenia rizík.
- **ubytovania a stravovania** (50%) a 89% z nich ju aj pravidelne aktualizuje. U 75% z nich je táto analýza založená na štandardizovanom procese riadenia rizík.
- **a priemyslu (**47%) a 61% z nich ju aj pravidelne aktualizuje. U 74% z nich je táto analýza založená na štandardizovanom procese riadenia rizík.

3.3 PLÁNY KONTINUITY ČINNOSTI ORGANIZÁCIE (BCP)

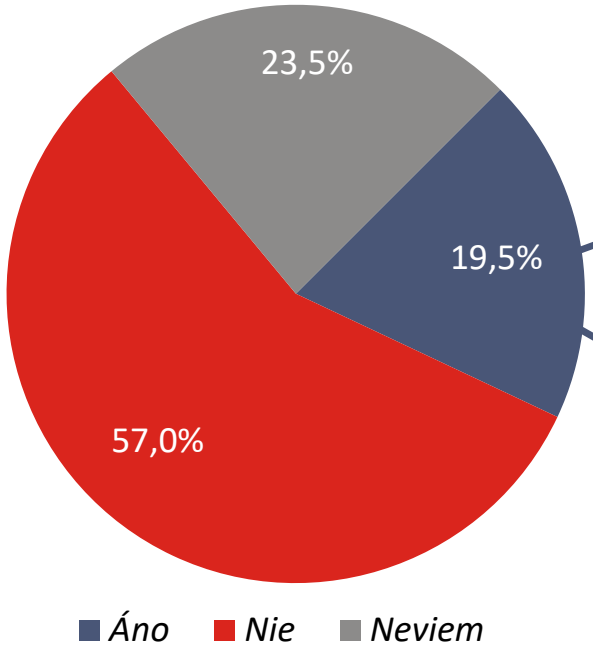
„Máte vypracované a pripravené plány kontinuity činnosti organizácie (BCP)?"

3.3 PLÁNY KONTINUITY ČINNOSTI ORGANIZÁCIE (BCP)

„Máte vypracované a pripravené plány kontinuity činnosti organizácie (BCP)?"

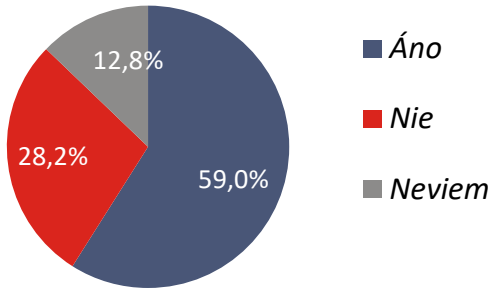
Odpovede všetkých respondentov

N= 200

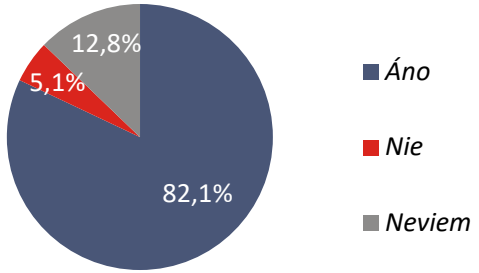


Ak áno: Vykonávate test BCM, pri ktorom overujete ich využiteľnosť, aspoň raz za rok?

N= 39



Ak áno: Sú tieto plány a testy založené na štandardizovanom procese riadenia kontinuity činnosti?

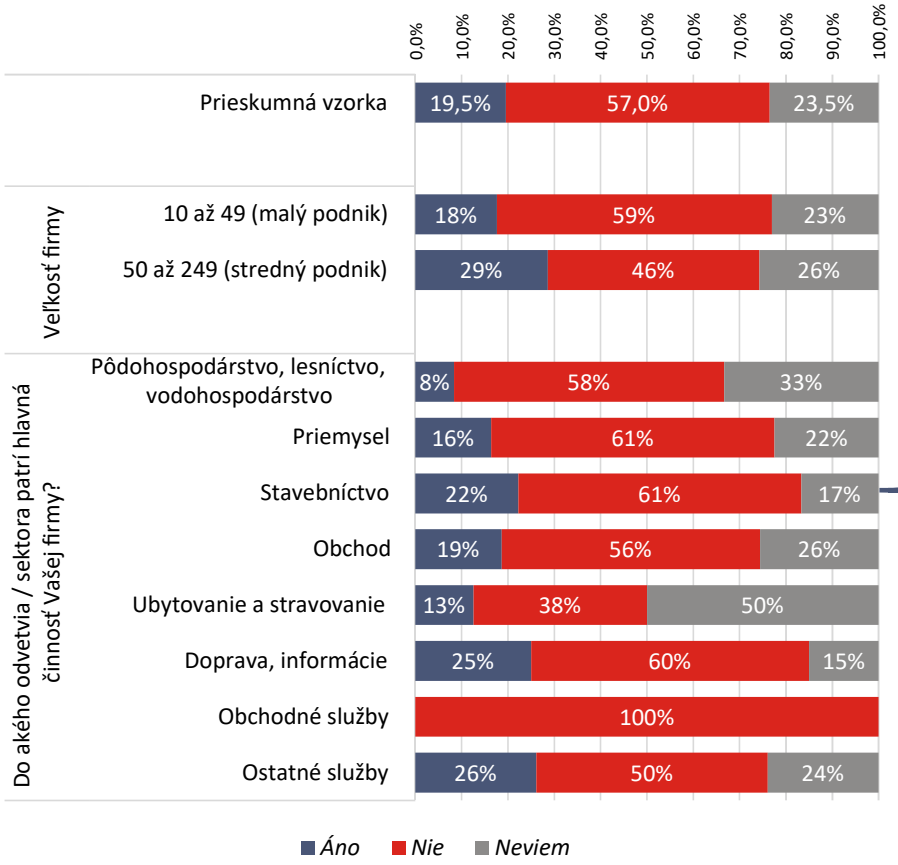


Respondent mal možnosť vybrať odpoveď z vopred preddefinovaných možností odpovedí. Možnosť len jednej odpovede.

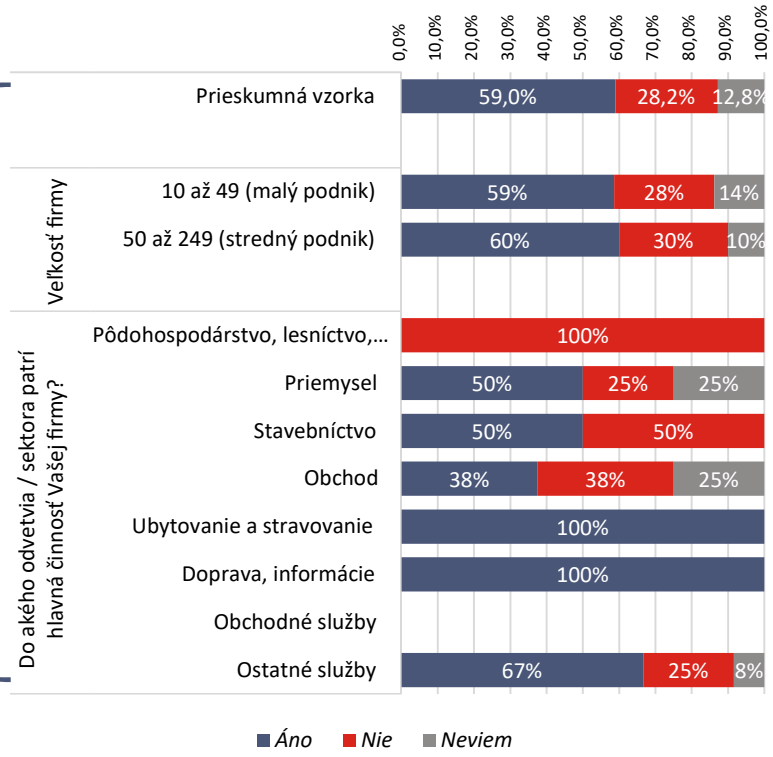
3.3 PLÁNY KONTINUITY ČINNOSTI ORGANIZÁCIE (BCP)

„Máte vypracované a pripravené plány kontinuity činnosti organizácie (BCP)?"

Odpovede podľa štruktúry podnikov



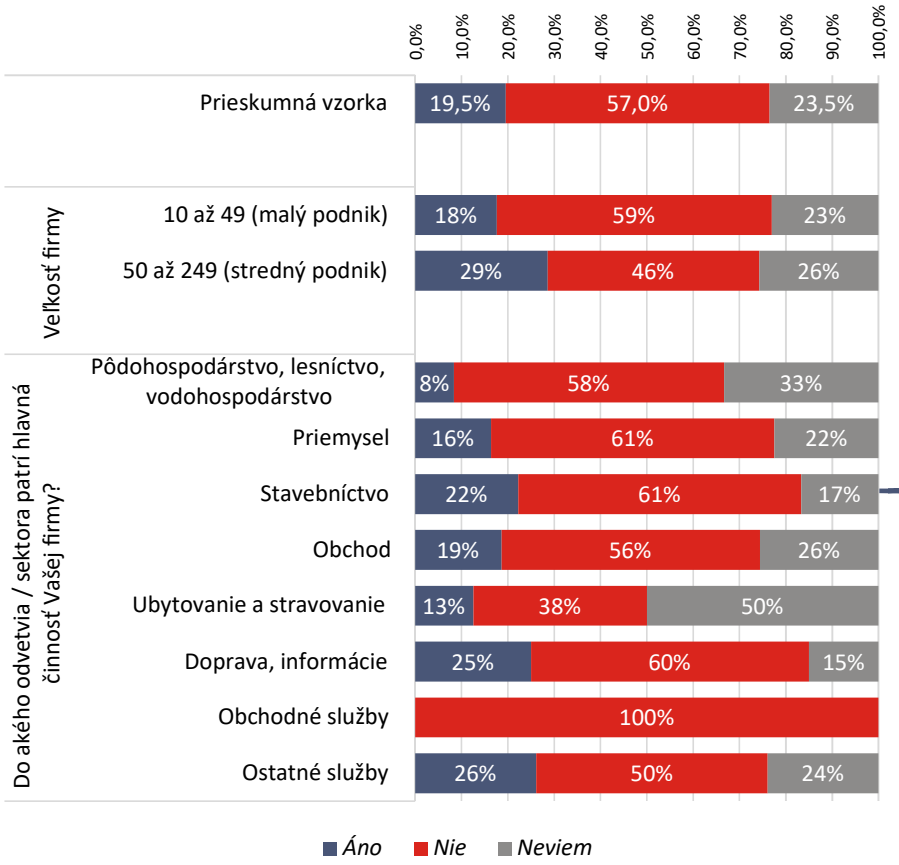
Ak áno: Vykonávate test BCM, pri ktorom overujete ich využiteľnosť, aspoň raz za rok?



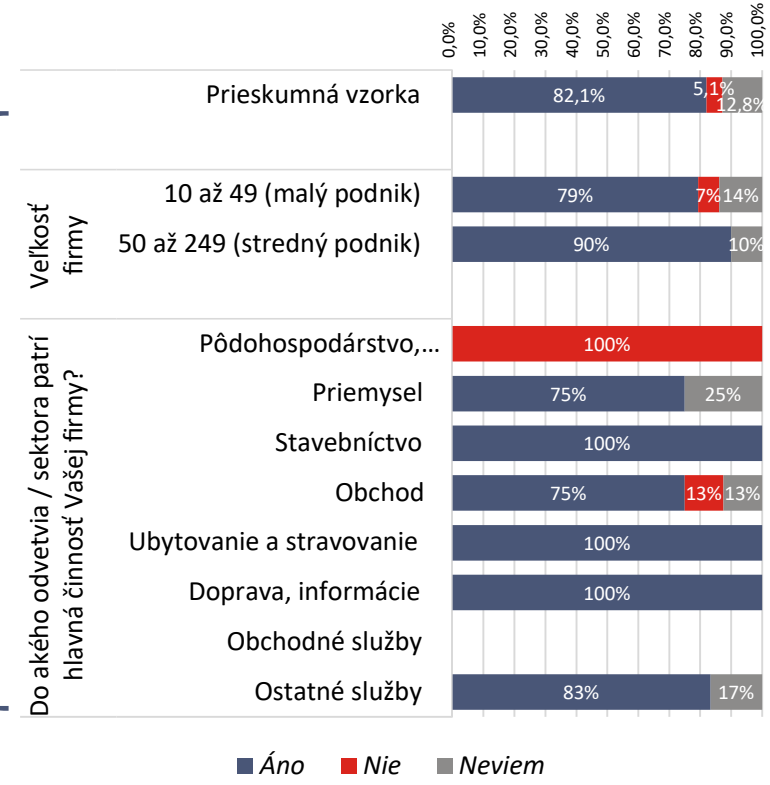
3.3 PLÁNY KONTINUITY ČINNOSTI ORGANIZÁCIE (BCP)

„Máte vypracované a pripravené plány kontinuity činnosti organizácie (BCP)?"

Odpovede podľa štruktúry podnikov



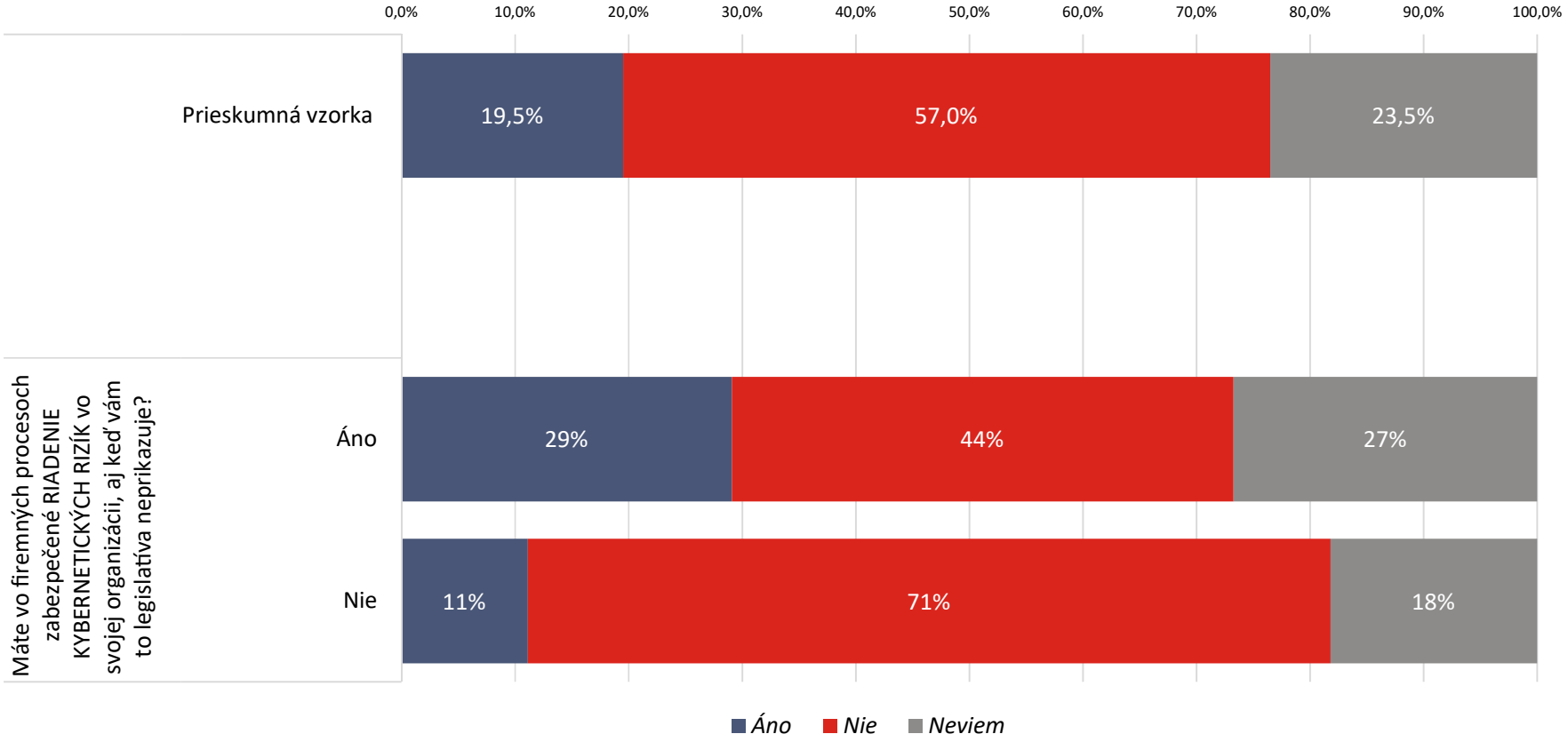
Ak áno: Sú tieto plány a testy založené na štandardizovanom procese riadenia kontinuity činnosti?



3.3 PLÁNY KONTINUITY ČINNOSTI ORGANIZÁCIE (BCP)

„Máte vypracované a pripravené plány kontinuity činnosti organizácie (BCP)?"

Odpovede podľa toho, či majú zabezpečené riadenie kybernetických rizík



PRIEBEŽNÉ ZHRNUTIE - PLÁNY KONTINUITY ČINNOSTI ORGANIZÁCIE (BCP)

Vzhľadom na nízky počet kladných odpovedí, je možné považovať odpovede za pravdivé.

19,5% z opýtaných MSP má vypracované a pripravené **plány kontinuity činnosti organizácie (BCP).** Oproti minulému roku došlo k nárastu o 8,5 percentuálneho bodu.

57% opýtaných MSP **plány BCP nemá.**

23,5% sa nevedelo/nechcelo vyjadriť.

Z tých MSP, ktoré majú vypracované a pripravené BCP:

- 59% z nich vykonáva test BCM aspoň raz za rok (oproti minulému roku nárast o 4,5 percentuálneho bodu)
- U 82,1% z nich sú tieto testy založené na štandardizovanom procese riadenia kontinuity činnosti.

Plány kontinuity činnosti organizácie (BCP) má pripravené 29% stredných podnikov. 60% z nich vykonáva test BCM aspoň raz za rok. U 90% z nich sú tieto testy založené na štandardizovanom procese riadenia kontinuity činnosti.

Plány kontinuity činnosti organizácie (BCP) majú pripravené nadpriemerne podniky v oblasti:

- **Ostatných služieb** (26%): 67% z nich vykonáva test BCM aspoň raz za rok a u 83% z nich sú tieto testy založené na štandardizovanom procese riadenia kontinuity činnosti.
- **Dopravy a informácií** (25%): 100% z nich vykonáva test BCM aspoň raz za rok a u 100% z nich sú tieto testy založené na štandardizovanom procese riadenia kontinuity činnosti.
- **a stavebníctva (**22%): 50% z nich vykonáva test BCM aspoň raz za rok a u 100% z nich sú tieto testy založené na štandardizovanom procese riadenia kontinuity činnosti.

Predchádzajúca odpoveď respondentov, že riadenie rizík vykonáva podnik pravidelne, sa dá interpretovať ako klamlivá, pretože pokiaľ by podnik v skutočnosti mal implementovaný proces riadenia rizík, nebolo by možné očakávať takú nízku mieru implementácie procesov BCM.

3.4 ROZPOČET NA KYBERNETICKÚ BEZPEČNOSŤ

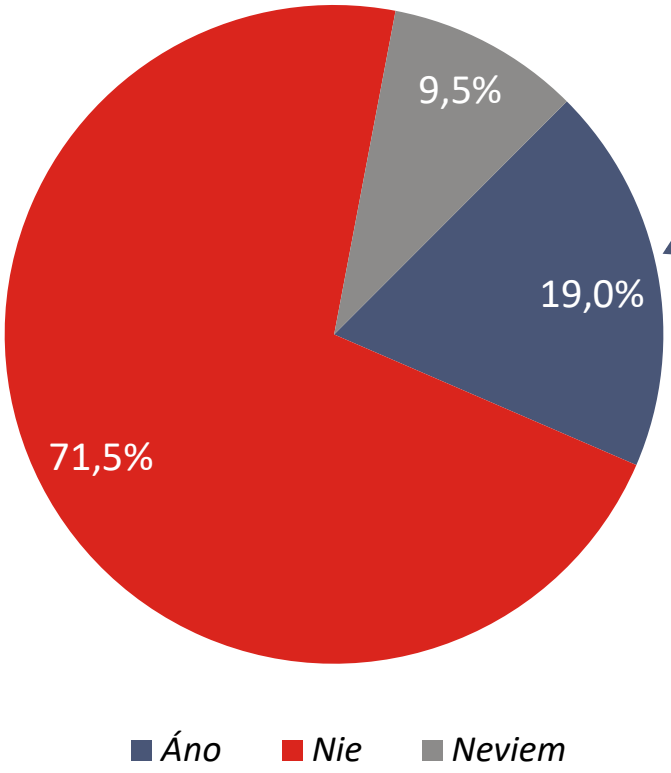
„Je rozpočet na kybernetickú bezpečnosť súčasťou rozpočtu firmy ako samostatná časť?“

3.4 ROZPOČET NA KYBERNETICKÚ BEZPEČNOSŤ

„Je rozpočet na kybernetickú bezpečnosť súčasťou rozpočtu firmy ako samostatná časť?"

Odpovede všetkých respondentov

N= 200

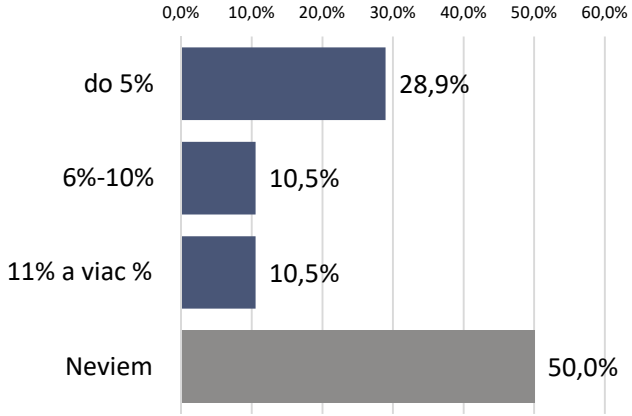


Respondent mal možnosť vybrať odpoveď z vopred preddefinovaných možností odpovedí. Možnosť len jednej odpovede.

Takmer pätina SME podnikov (19%) má v rozpočte aj rozpočet na kybernetickú bezpečnosť ako samostatnú časť.

Ak áno: Koľko percent rozpočtu organizácie tvoria náklady na kybernetickú bezpečnosť?

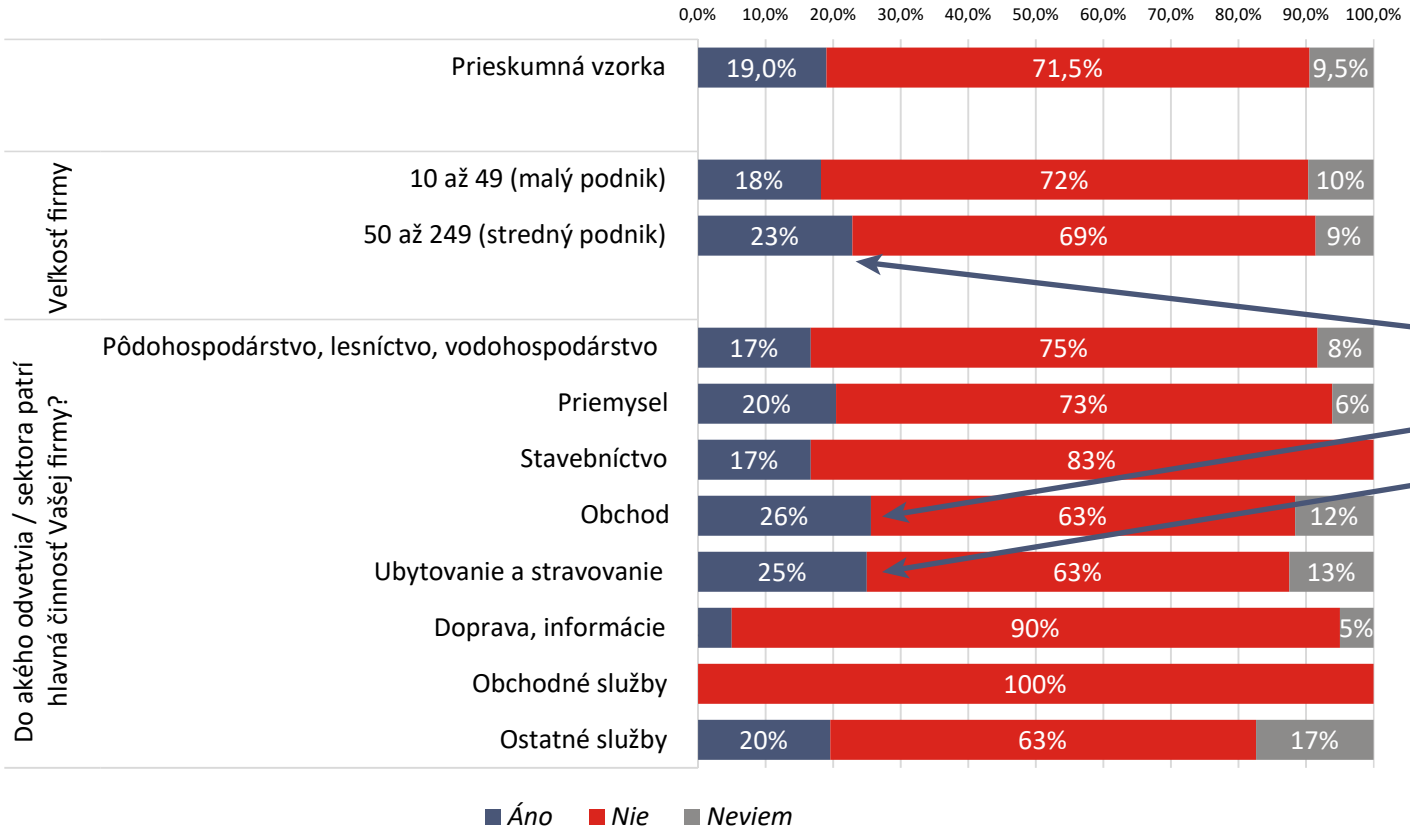
N= 38



3.4 ROZPOČET NA KYBERNETICKÚ BEZPEČNOSŤ

„Je rozpočet na kybernetickú bezpečnosť súčasťou rozpočtu firmy ako samostatná časť?"

Odpovede podľa štruktúry podnikov



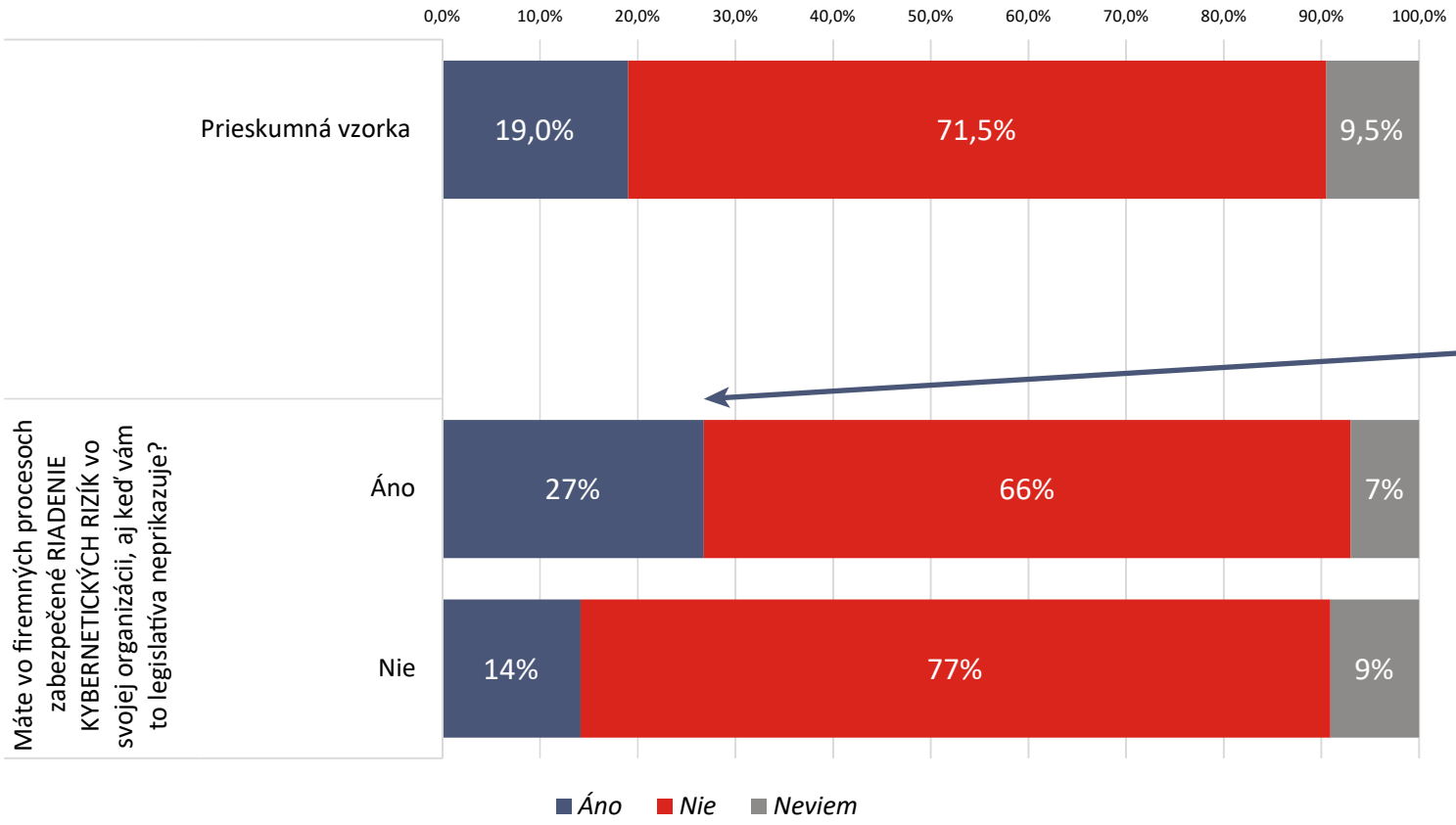
Ide častejšie o stredné podniky – samostatnú časť rozpočtu na KB má 23% z nich.

Z hľadiska sektorov samostatnú časť rozpočtu na KB majú nadpriemerne firmy z oblasti Obchodu a Ubytovania/stravovania.

3.4 ROZPOČET NA KYBERNETICKÚ BEZPEČNOSŤ

„Je rozpočet na kybernetickú bezpečnosť súčasťou rozpočtu firmy ako samostatná časť?"

Odpovede podľa toho, či majú zabezpečené riadenie kybernetických rizík



Samostatnú časť rozpočtu na KB má 27% tých podnikov, ktoré deklarovali, že majú vo firemných procesoch zabezpečené RKR.

PRIEBEŽNÉ ZHRNUTIE - ROZPOČET NA KYBERNETICKÚ BEZPEČNOSŤ

Takmer pätina MSP (19%) má v rozpočte aj **rozpočet na kybernetickú bezpečnosť** ako samostatnú časť. Oproti minulému roku došlo k nárastu o 8,5 percentuálneho bodu.

71,5% opýtaných MSP **nemá samostatnú časť rozpočtu** na kybernetickú bezpečnosť. Z kontextu odpovedí však vyplýva, že pojem **„rozpočet na kybernetickú bezpečnosť"** si firmy pravdepodobne spájajú s rozpočtom na prevádzku IT.

9,5% sa nevedelo/nechcelo vyjadriť.

Z tých MSP, ktoré majú v rozpočte aj rozpočet na KB ako samostatnú časť, náklady na KB zväčša tvoria do 5% celkového rozpočtu (u 28,9% tých podnikov, ktoré majú na KB samostatnú časť rozpočtu).

V porovnaní s priemerným výsledkom, samostatnú časť rozpočtu na KB majú nadpriemerne stredné podniky (23% oproti priemeru 19%).

Samostatnú časť rozpočtu majú nadpriemerne podniky zo sektorov:

- **Obchodu** (26%)
- **Ubytovania a stravovania** (25%)

Pozitívnym zistením z prieskumu je, že firmy vnímajú potrebu financovania kybernetickej bezpečnosti a že u firiem ktoré uplatňujú procesy riadenia rizík je vyšší počet tých, ktoré rozpočet na kybernetickú bezpečnosť vyčleňujú .

3.5 OSOBITNÝ ROZPOČET NA BCM

„Má vaša firma osobitne určený rozpočet na BCM (výnimočné situácie)?"

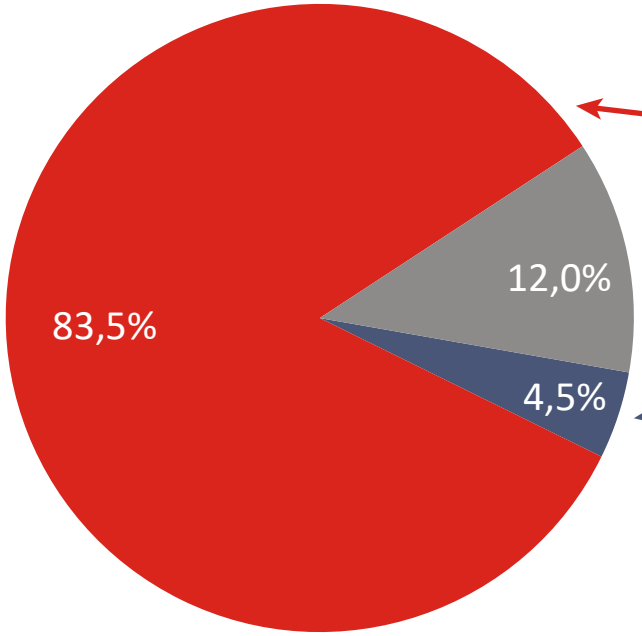
3.5 OSOBITNÝ ROZPOČET NA BCM

„Má vaša firma osobitne určený rozpočet na BCM (výnimočné situácie)?"

Odpovede všetkých respondentov

N= 200

Respondent mal možnosť vybrať odpoveď z vopred preddefinovaných možností odpovedí. Možnosť len jednej odpovede.



83,5% SME podnikov nemá osobitne určený rozpočet na BCM (výnimočné situácie).

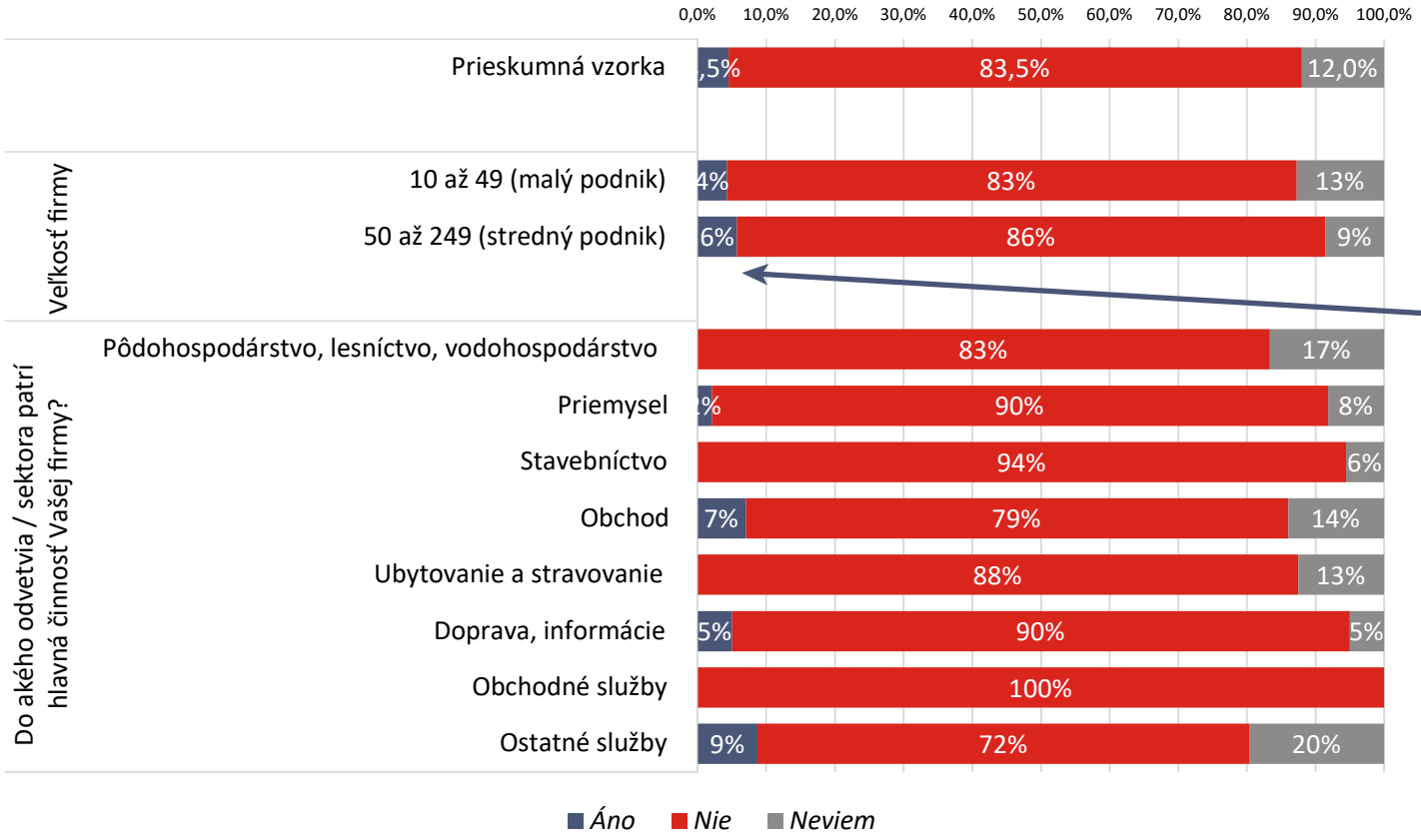
Len 4,5% opytovaných SME firiem takýto rozpočet má .

Áno *Nie* *Neviem*

3.5 OSOBITNÝ ROZPOČET NA BCM

„Má vaša firma osobitne určený rozpočet na BCM (výnimočné situácie)?"

Odpovede podľa štruktúry podnikov



Mierne nadpriemerne osobitný rozpočet na výnimočné situácie majú stredné firmy (6%), nadpriemerne aj obchodné podniky (7%) a firmy z oblasti ostatných služieb (9%).

Rozpočet na BCM vôbec nemajú, resp. nevedia, či majú, podniky zo sektorov pôdohospodárstvo, stavebníctvo, ubytovanie a stravovanie a obchodné služby.

PRIEBEŽNÉ ZHRNUTIE - OSOBITNÝ ROZPOČET NA BCM

Zistenie poukazuje na skutočnosť, že napriek negatívnym skúsenostiam z udalostí prerušenia kontinuity a napriek negatívnym skúsenostiam z incidentov sa firmy nepoučili a rozpočet na BCM netvoria (t.j. nepočítajú s možným výskytom výnimočných situácií).

Len 4,5% opýtaných MSP má osobitne určený rozpočet na BCM (výnimočné situácie). Oproti minulému roku došlo k poklesu o 3 percentuálne body, zvýšil sa však podiel tých, ktorí nevedia, či má firma takýto rozpočet.

83,5% MSP **nemá osobitne určený rozpočet na BCM.**

12% sa nevedelo/nechcelo vyjadriť.

V porovnaní s priemerným výsledkom osobitne určený rozpočet na BCM majú mierne nadpriemerne stredné podniky (6% oproti priemeru 4,5%).

Osobitne určený rozpočet na BCM majú častejšie podniky zo sektorov:

- **Obchod** (7%)
- **Ostatných služieb** (9%)

3.6 POSKYTOVANIE SLUŽIEB / PRODUKTOV INÉMU PREVÁDZKOVATEĽOVI ZS

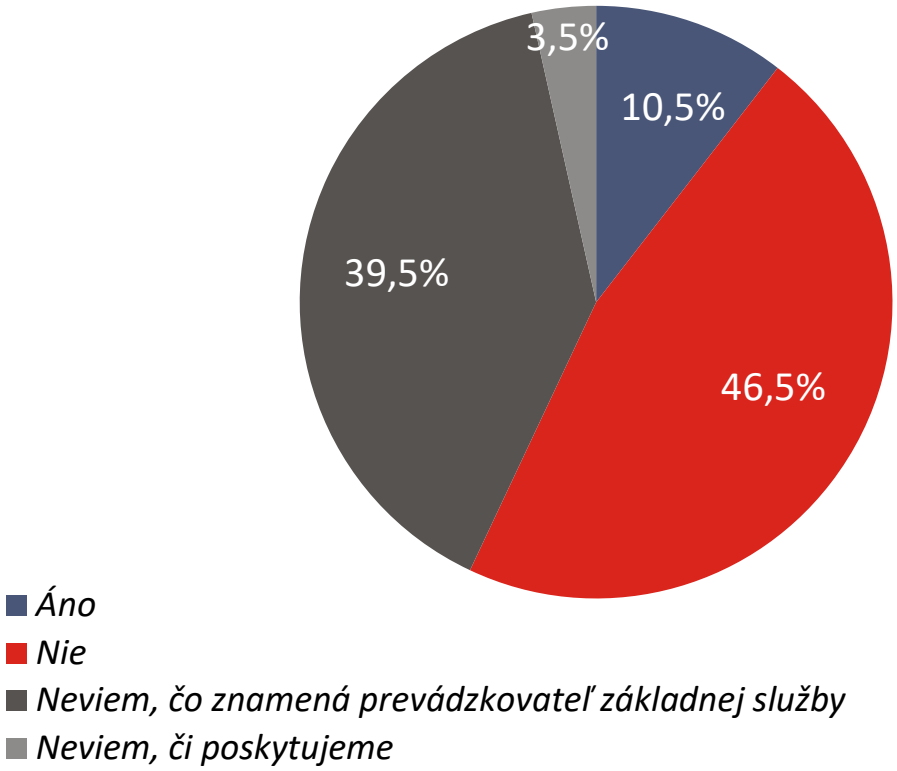
„Poskytujete služby alebo produkty pre iného prevádzkovateľa tzv. základnej služby?“

3.6 POSKYTOVANIE SLUŽIEB / PRODUKTOV INÉMU PREVÁDZKOVATEĽOVI ZS

„Poskytujete služby alebo produkty pre iného prevádzkovateľa tzv. základnej služby?"

Odpovede všetkých respondentov

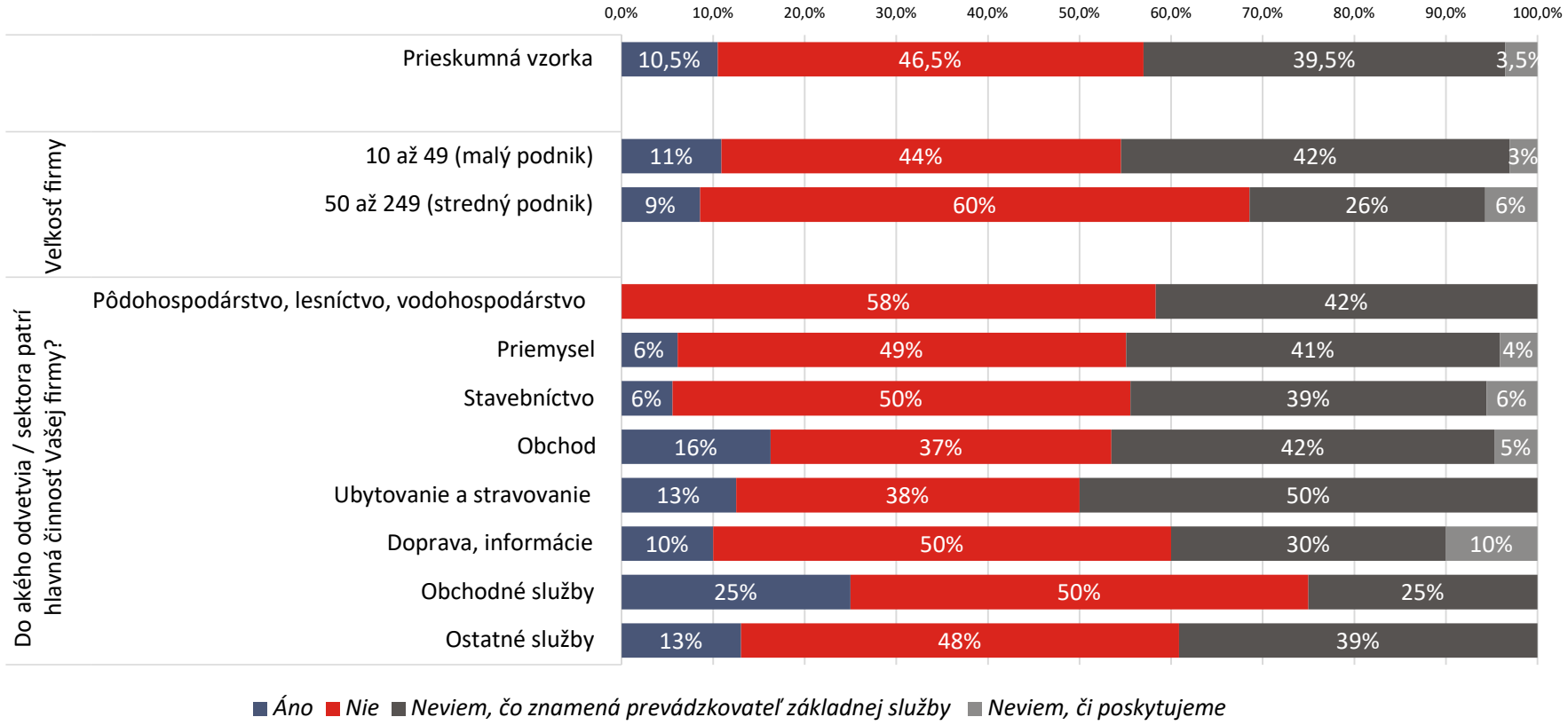
N= 200



3.6 POSKYTOVANIE SLUŽIEB / PRODUKTOV INÉMU PREVÁDZKOVATEĽOVI ZS

„Poskytujete služby alebo produkty pre iného prevádzkovateľa tzv. základnej služby?"

Odpovede podľa štruktúry podnikov



PRIEBEŽNÉ ZHRNUTIE - POSKYTOVANIE SLUŽIEB / PRODUKTOV INÉMU PREVÁDZKOVATEĽOVI ZS

Z prieskumu boli vylúčené podniky, ktoré sú poskytovateľmi základnej služby.

Približne každý desiaty opýtaný MSP (mimo poskytovateľov základnej služby) svoju podnikateľskú činnosť realizuje **pre iného poskytovateľa základnej služby** (10,5%).

46,5% **opýtaných MSP** (mimo poskytovateľov základnej služby) neposkytuje produkty alebo služby **pre iného poskytovateľa základnej služby.**

Z prieskumnej vzorky MSP 3,5% nevedelo uviesť, či poskytujú produkty, alebo službypre iného poskytovateľa základnej služby a 39,5% opýtaných nevedelo, čo to poskytovateľ základnej služby je.

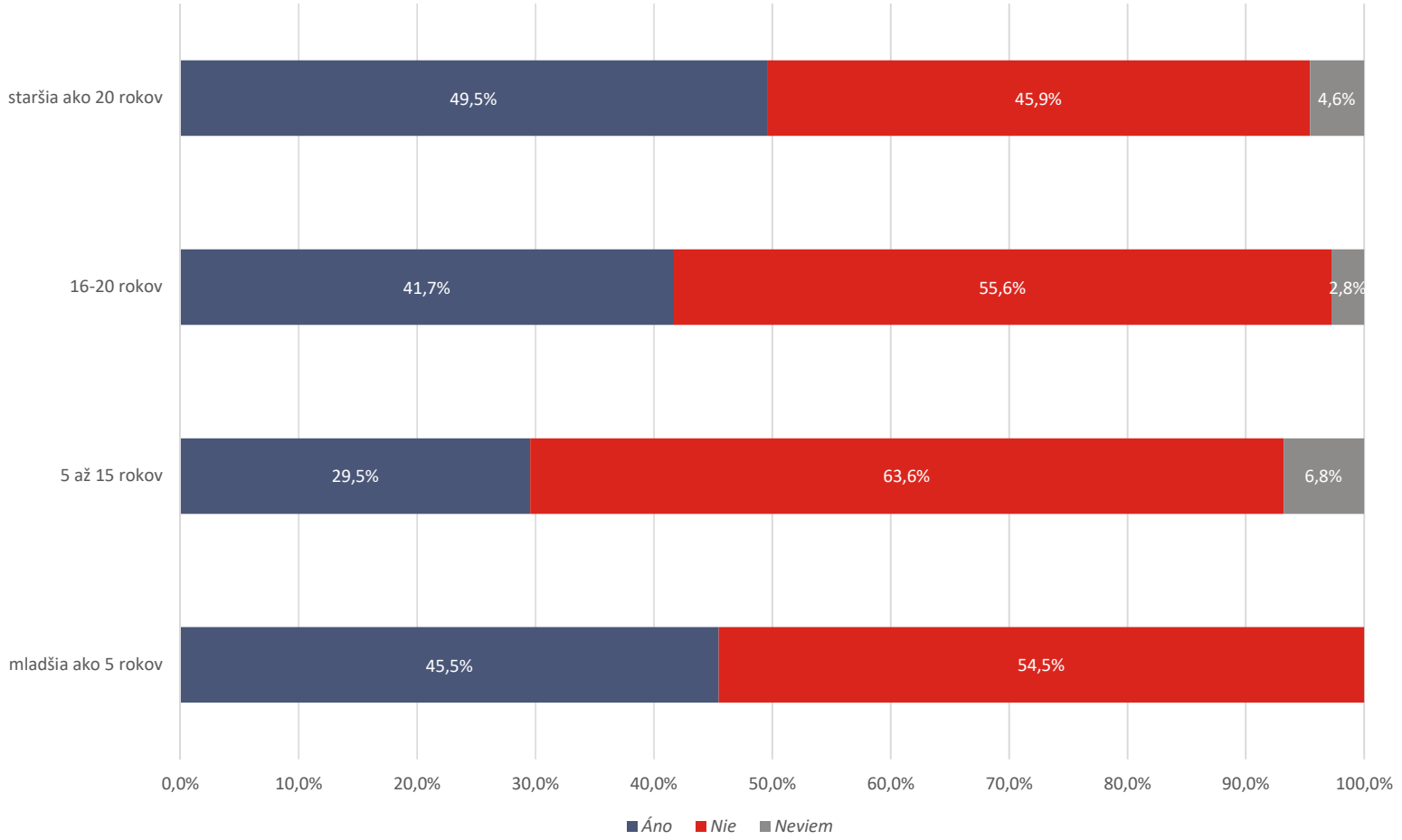
Z odpovedí vyplýva, že takmer polovica podnikov si neuvedomuje kritičnosť služieb svojich odberateľov, ktorým sami poskytujú svoje dodávateľské služby. Podniky teda nepoznajú svoju bezpečnostnú rolu v dodávateľsko-odberateľskom reťazci (supply chain).

4. TRIEDENIE CEZ VEK FIRIEM A CEZ POSKYTOVANIE ZÁKLADNEJ SLUŽBY

4.1 POROVNANIE PODĽA VEKU FIRMY

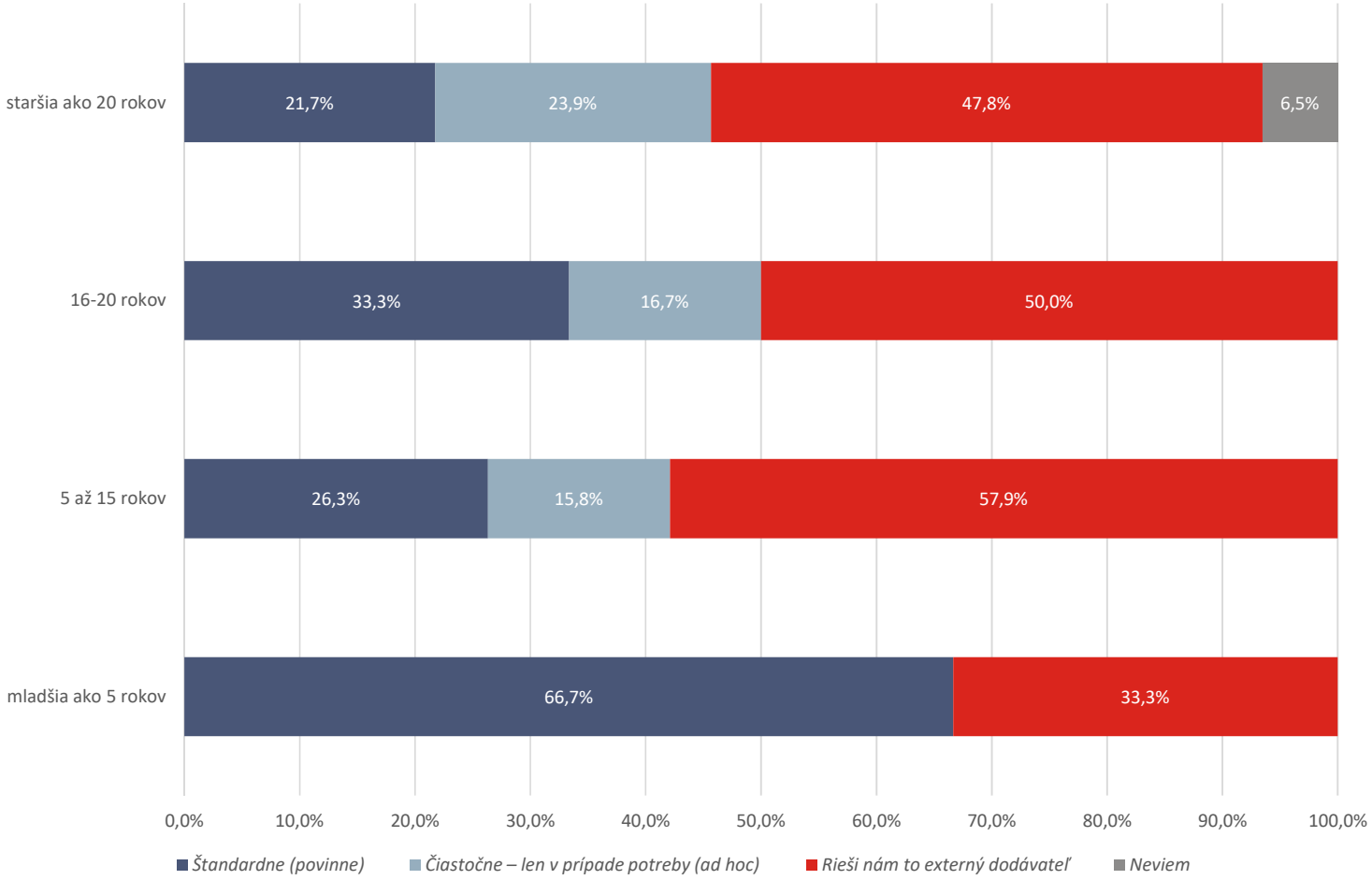
4.1 POROVNANIE PODĽA VEKU FIRMY

Je alebo nie je vaša firma ohrozená kybernetickými útokmi?



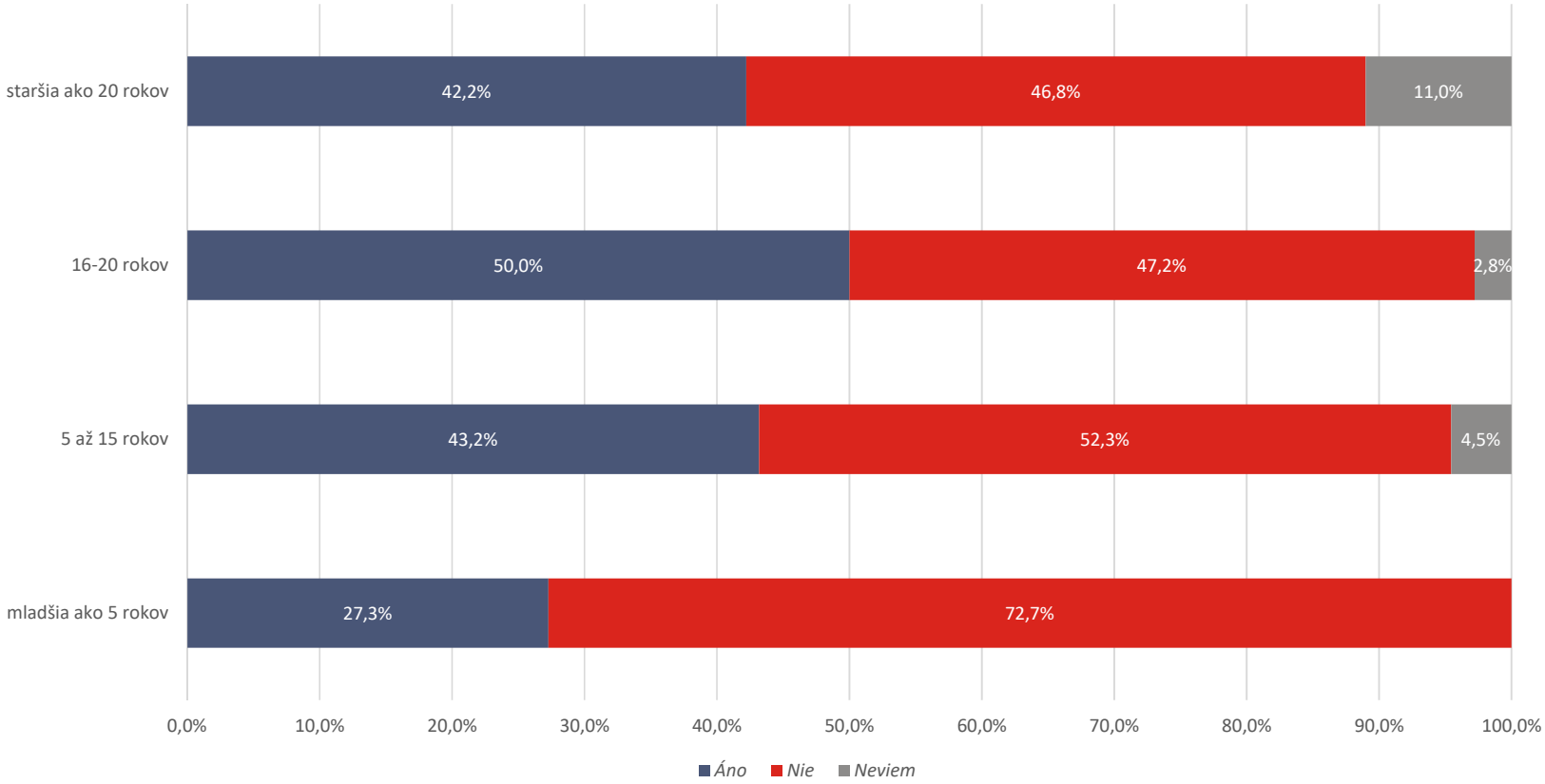
4.1 POROVNANIE PODĽA VEKU FIRMY

Akým spôsobom máte zabezpečené riadenie kybernetických rizík?



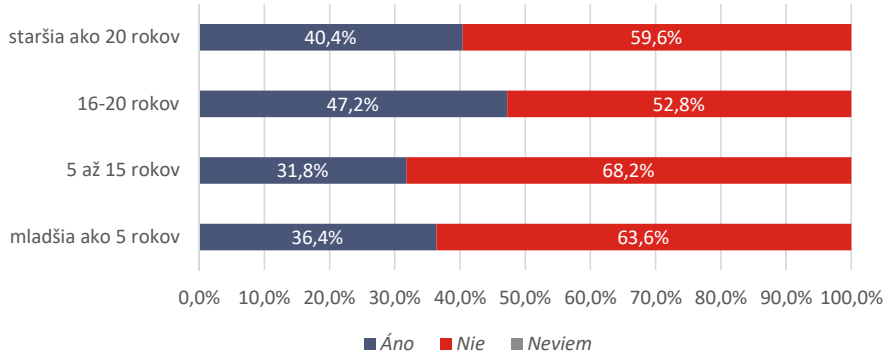
4.1 POROVNANIE PODĽA VEKU FIRMY

Máte vo firemných procesoch zabezpečené RIADENIE KYBERNETICKÝCH RIZÍK vo svojej organizácii, aj keď vám to legislatíva neprikazuje?

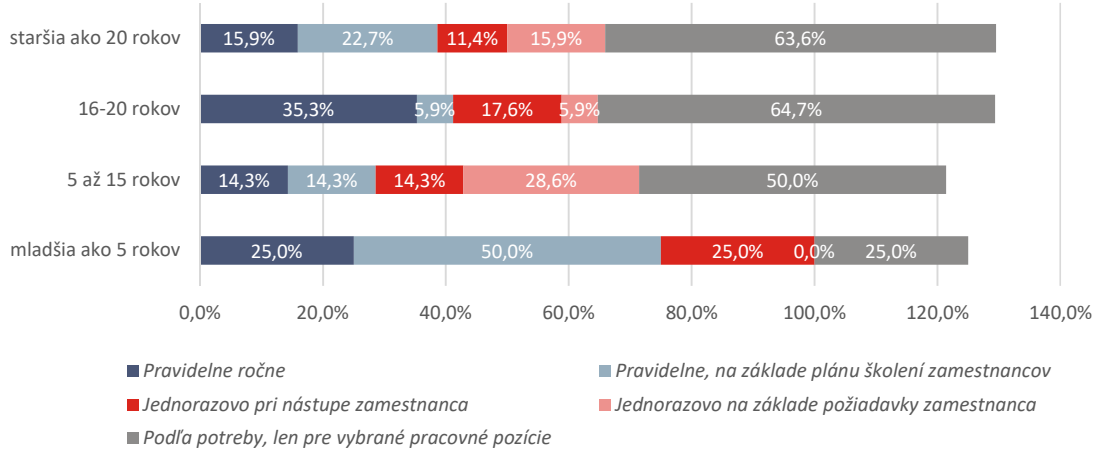


4.1 POROVNANIE PODĽA VEKU FIRMY

Poskytujete svojim zamestnancom možnosti školenia na zvyšovanie ich znalostí a schopností v oblasti kybernetickej bezpečnosti?

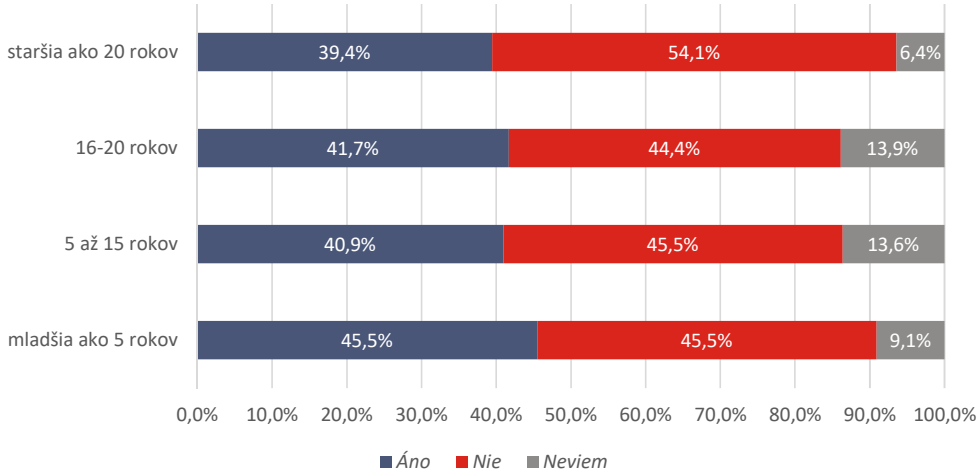


Poskytujete svojim zamestnancom možnosti školenia na zvyšovanie ich znalostí a schopností v oblasti kybernetickej bezpečnosti? Ak áno, ako často?

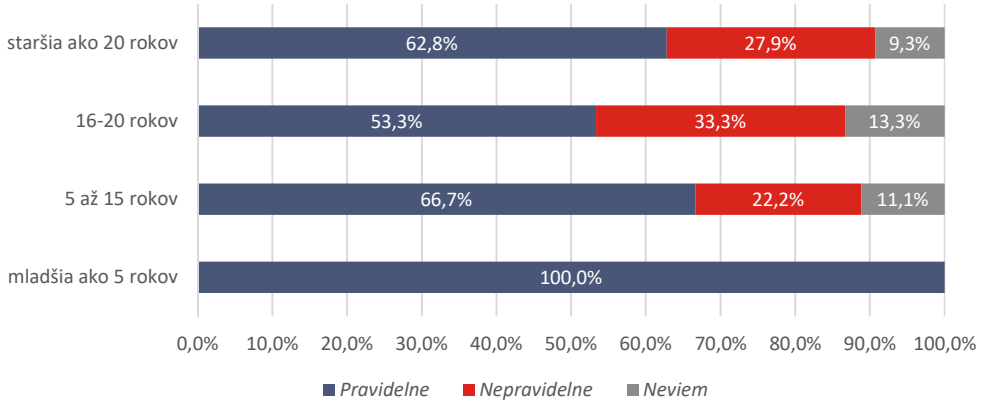


4.1 POROVNANIE PODĽA VEKU FIRMY

Má vaša firma vypracovanú analýzu rizík?

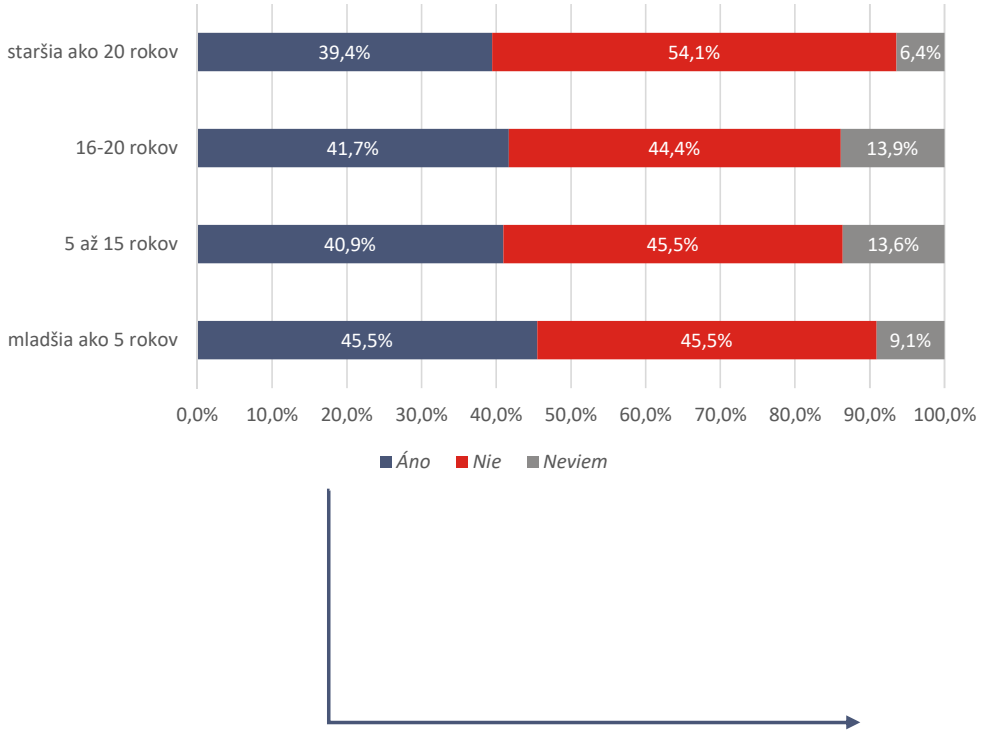


Má vaša firma vypracovanú analýzu rizík, Ak áno, ako často analýzu rizík aktualizujete?

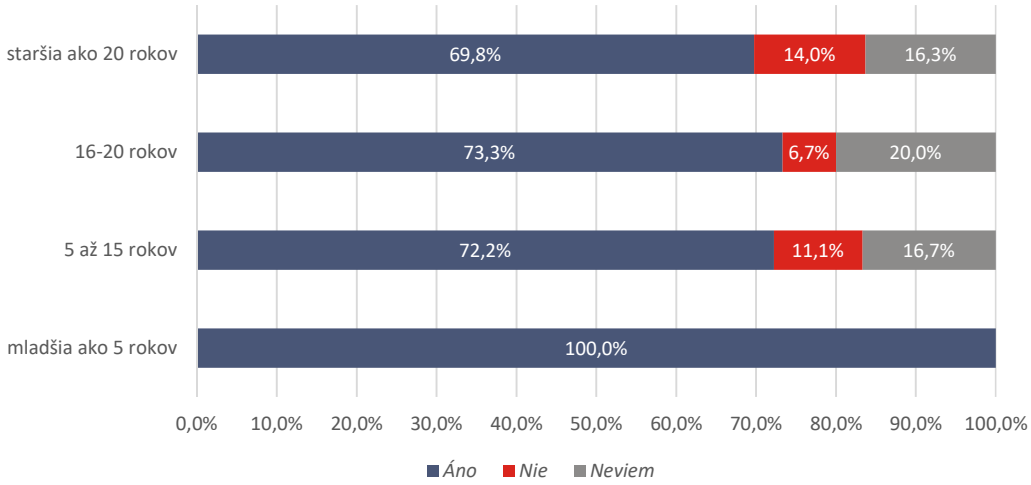


4.1 POROVNANIE PODĽA VEKU FIRMY

Má vaša firma vypracovanú analýzu rizík?

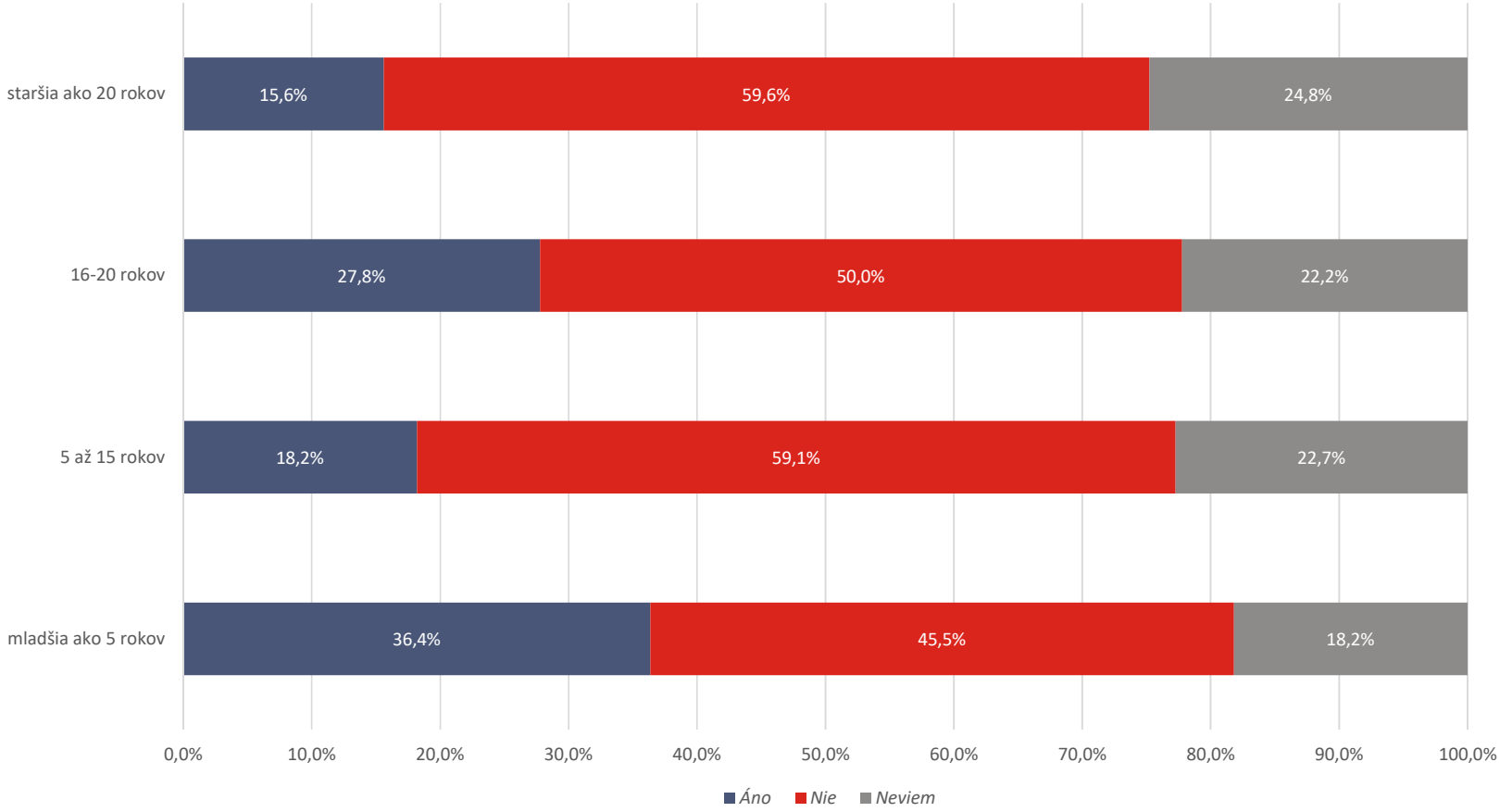


Je táto analýza založená na štandardizovanom procese riadenia rizík?



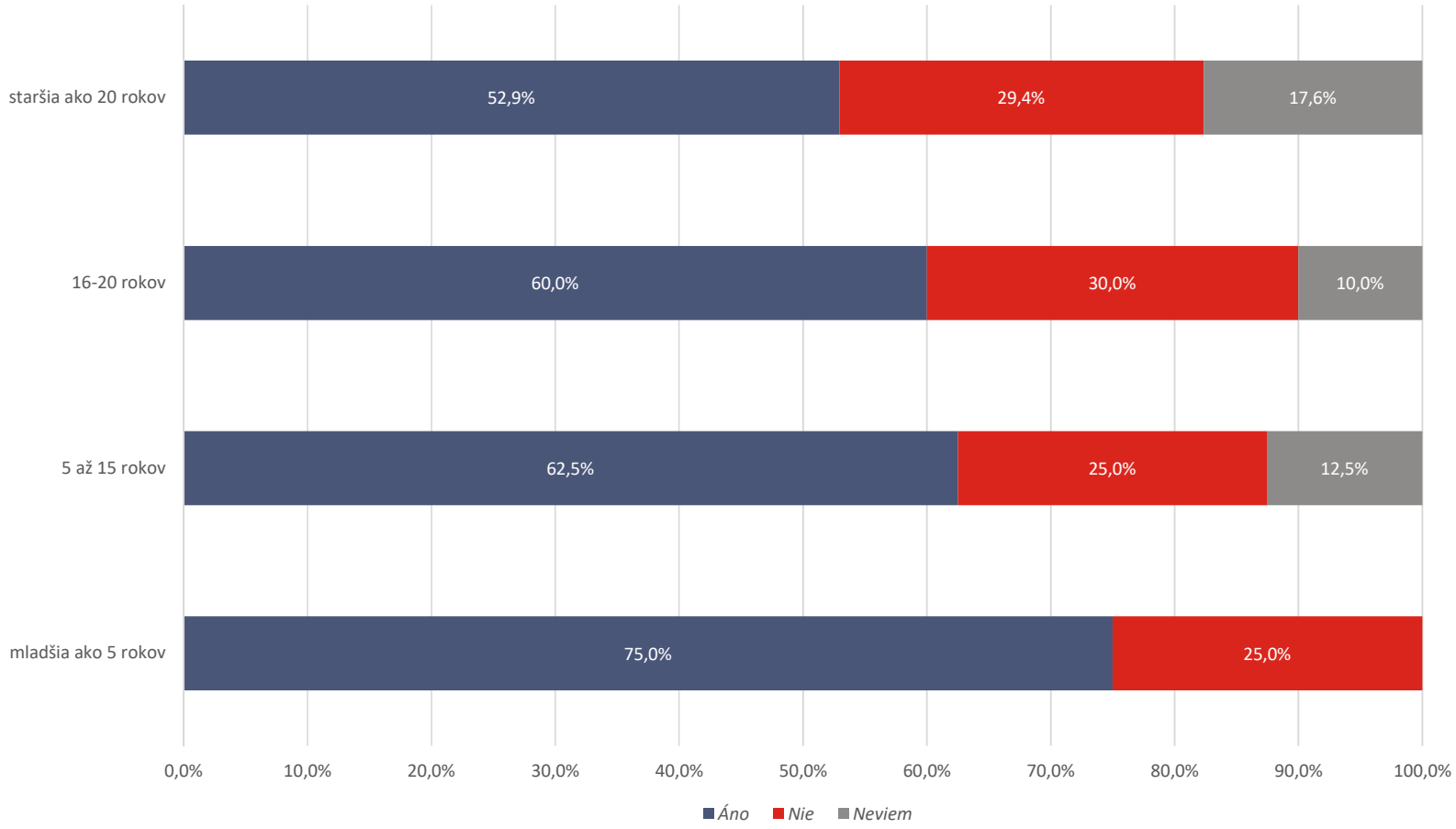
4.1 POROVNANIE PODĽA VEKU FIRMY

Máte vypracované a pripravené plány kontinuity činnosti organizácie (BCP)?



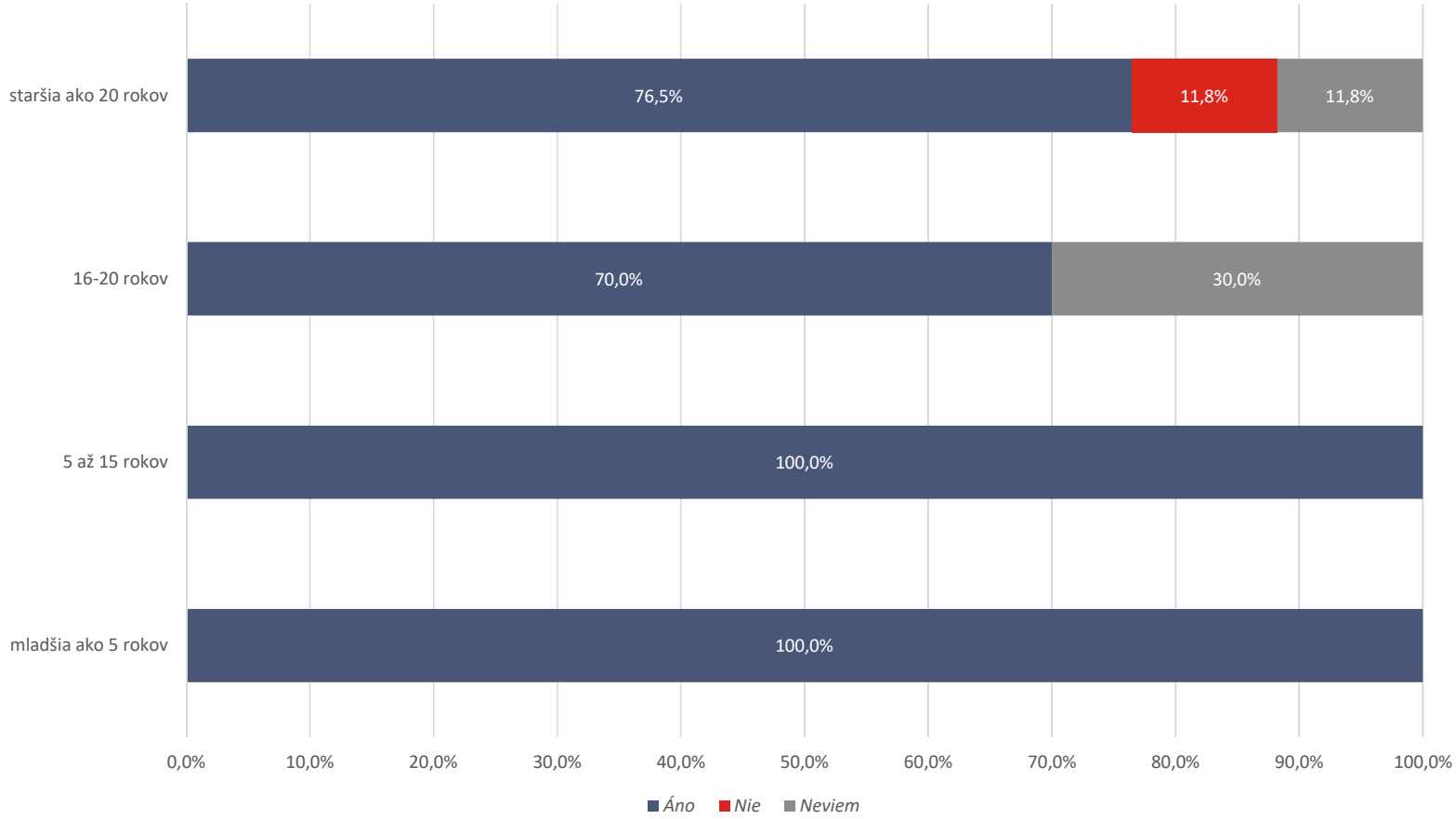
4.1 POROVNANIE PODĽA VEKU FIRMY

Vykonávate test BCP, pri ktorom overujete ich využiteľnosť, aspoň raz za rok?



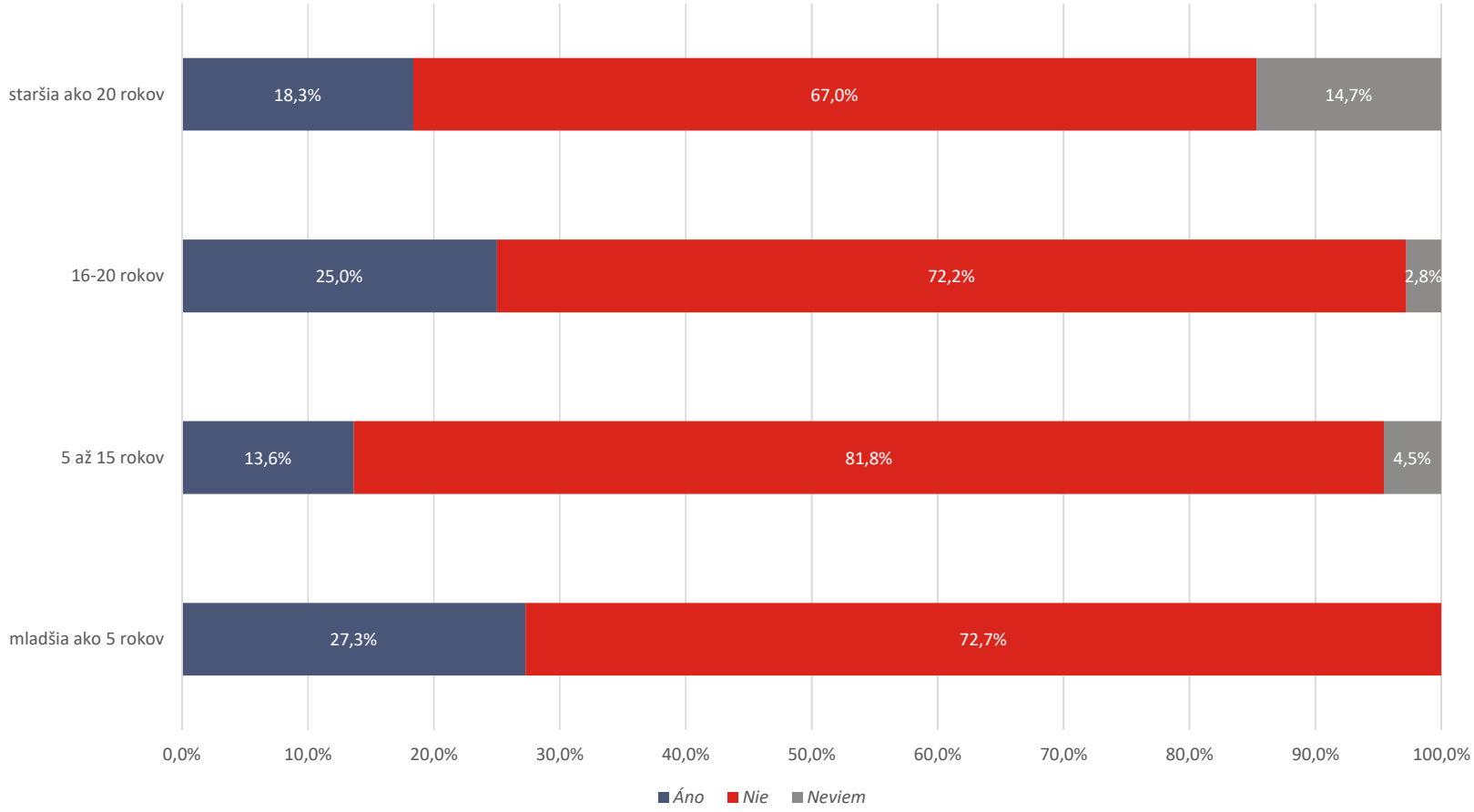
4.1 POROVNANIE PODĽA VEKU FIRMY

Sú tieto plány a testy založené na štandardizovanom procese riadenia kontinuity činností?



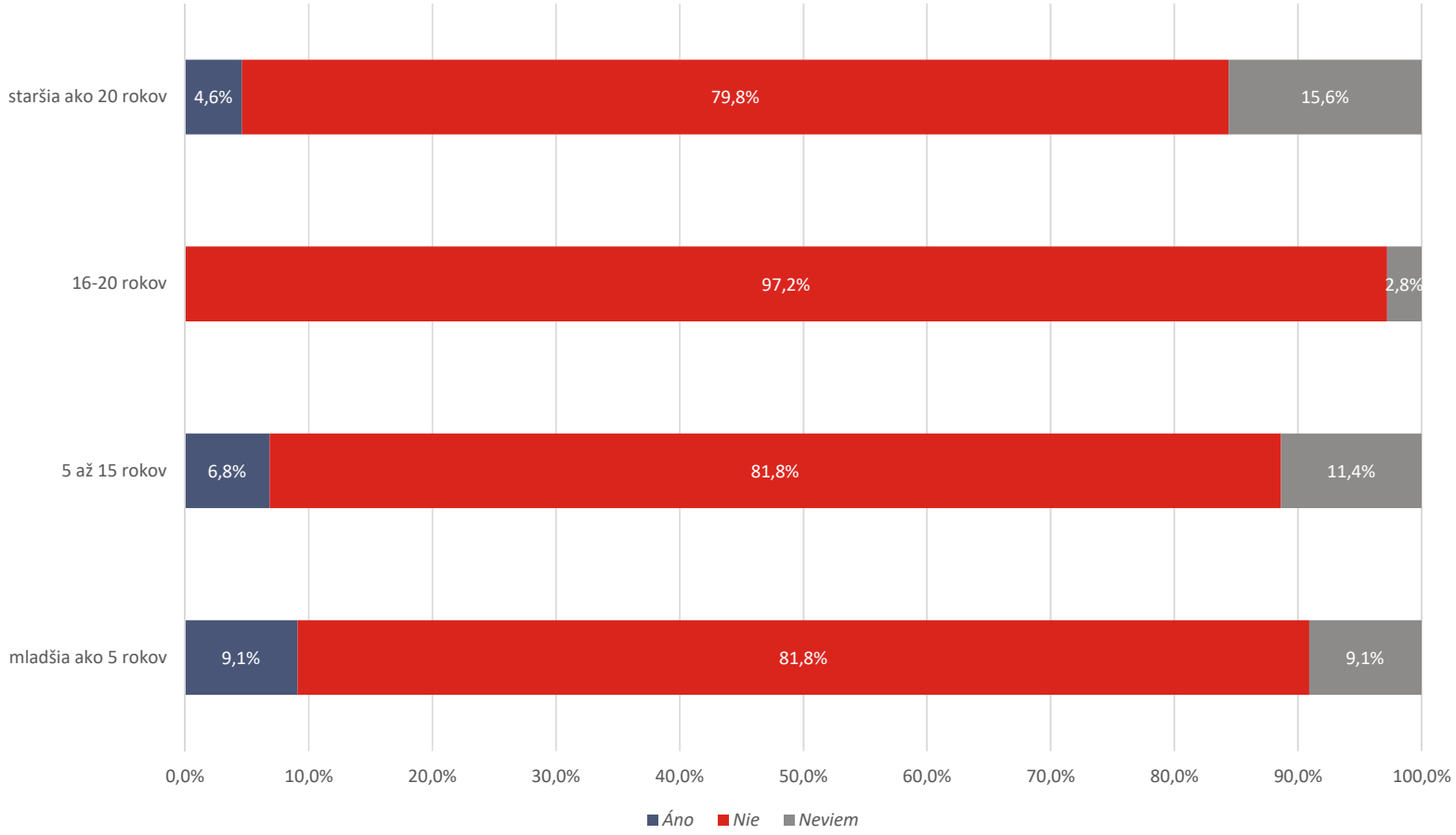
4.1 POROVNANIE PODĽA VEKU FIRMY

Je rozpočet na kybernetickú bezpečnosť súčasťou rozpočtu firmy ako samostatná časť?



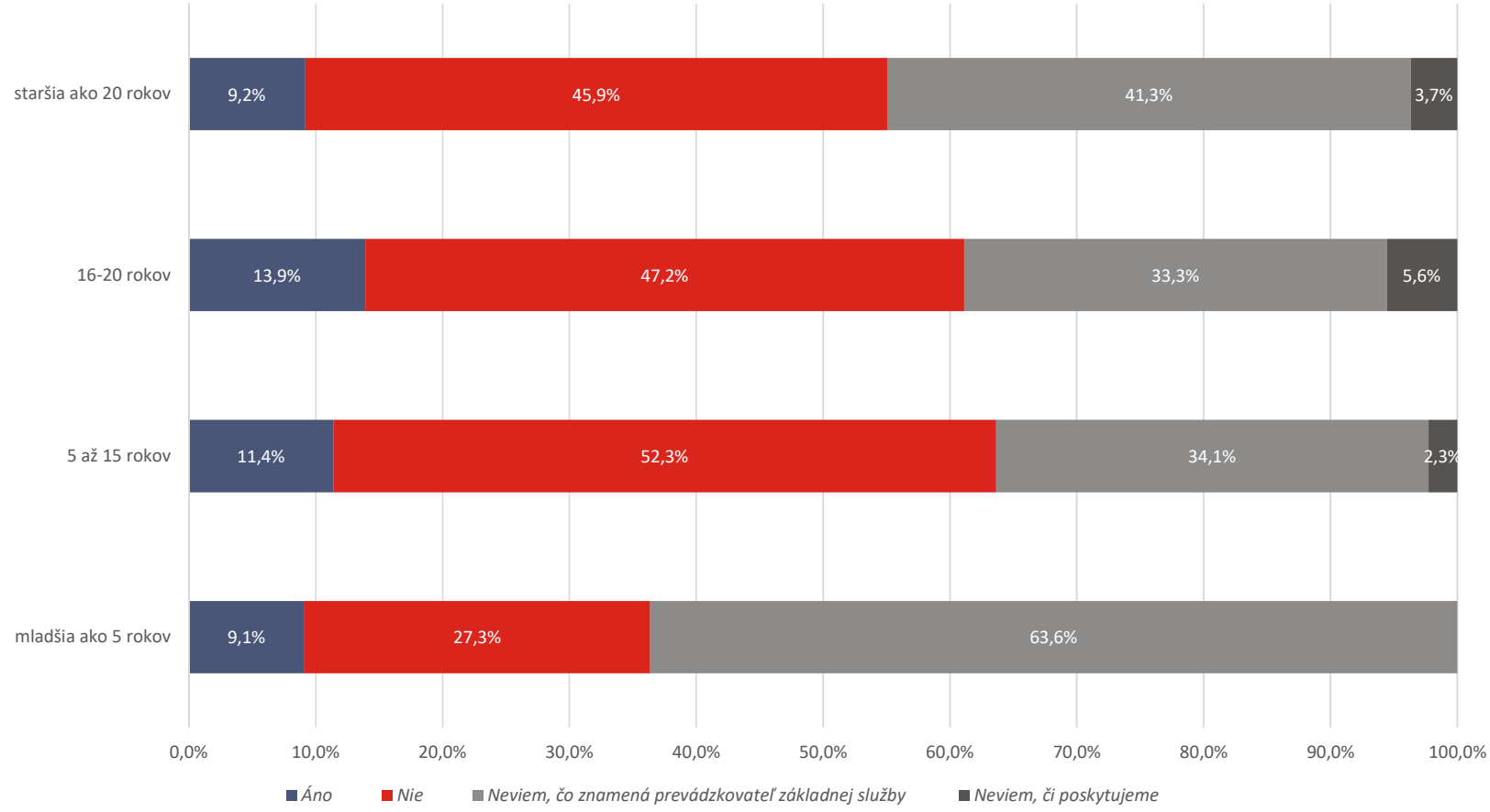
4.1 POROVNANIE PODĽA VEKU FIRMY

Má vaša firma osobitne určený rozpočet na BCM?



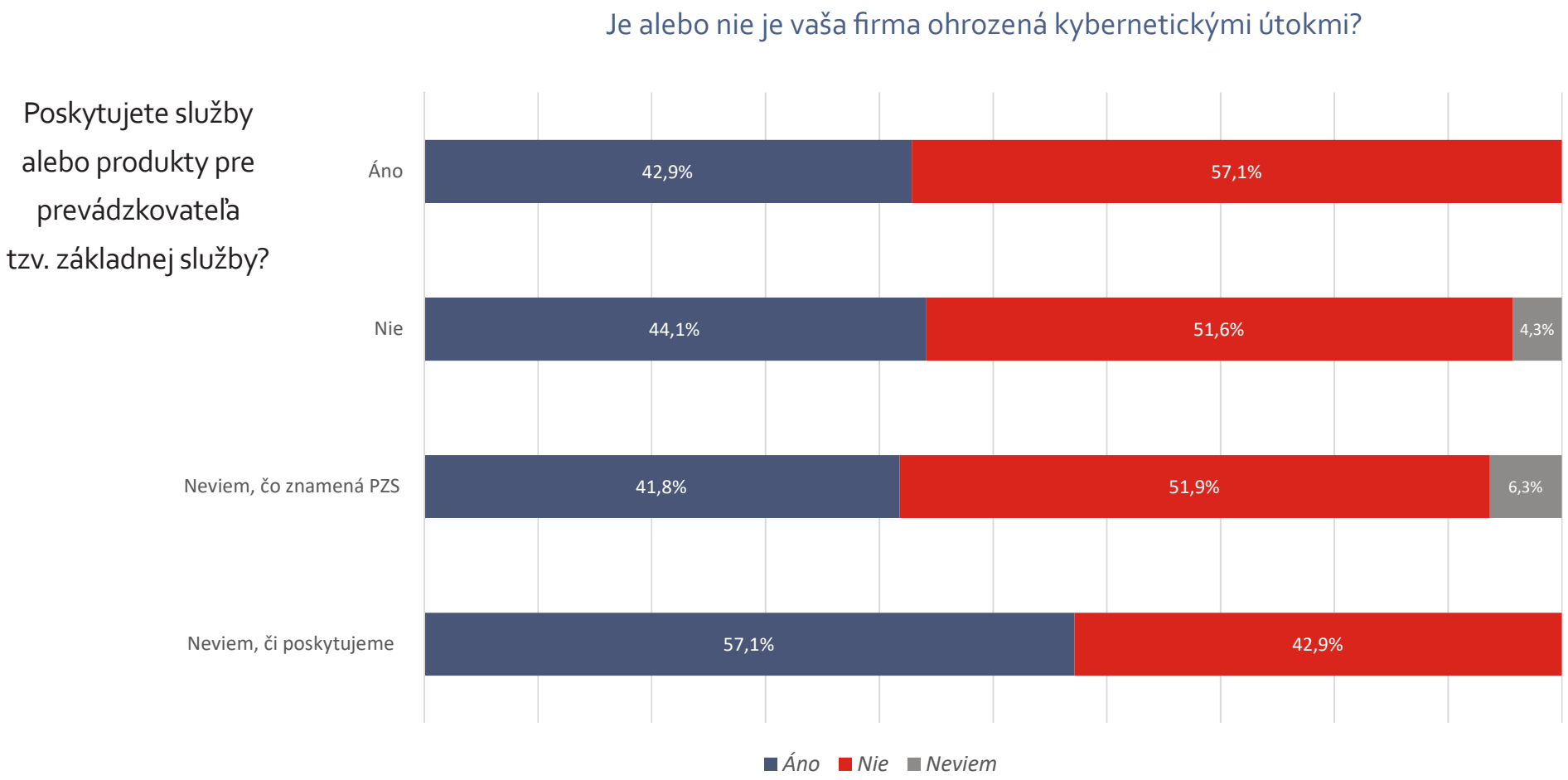
4.1 POROVNANIE PODĽA VEKU FIRMY

Poskytujete služby alebo produkty pre prevádzkovateľa tzv. základnej služby?



4.2 POROVNANIE PODĽA DODÁVANIA SLUŽIEB POSKYTOVATEĽOM ZS

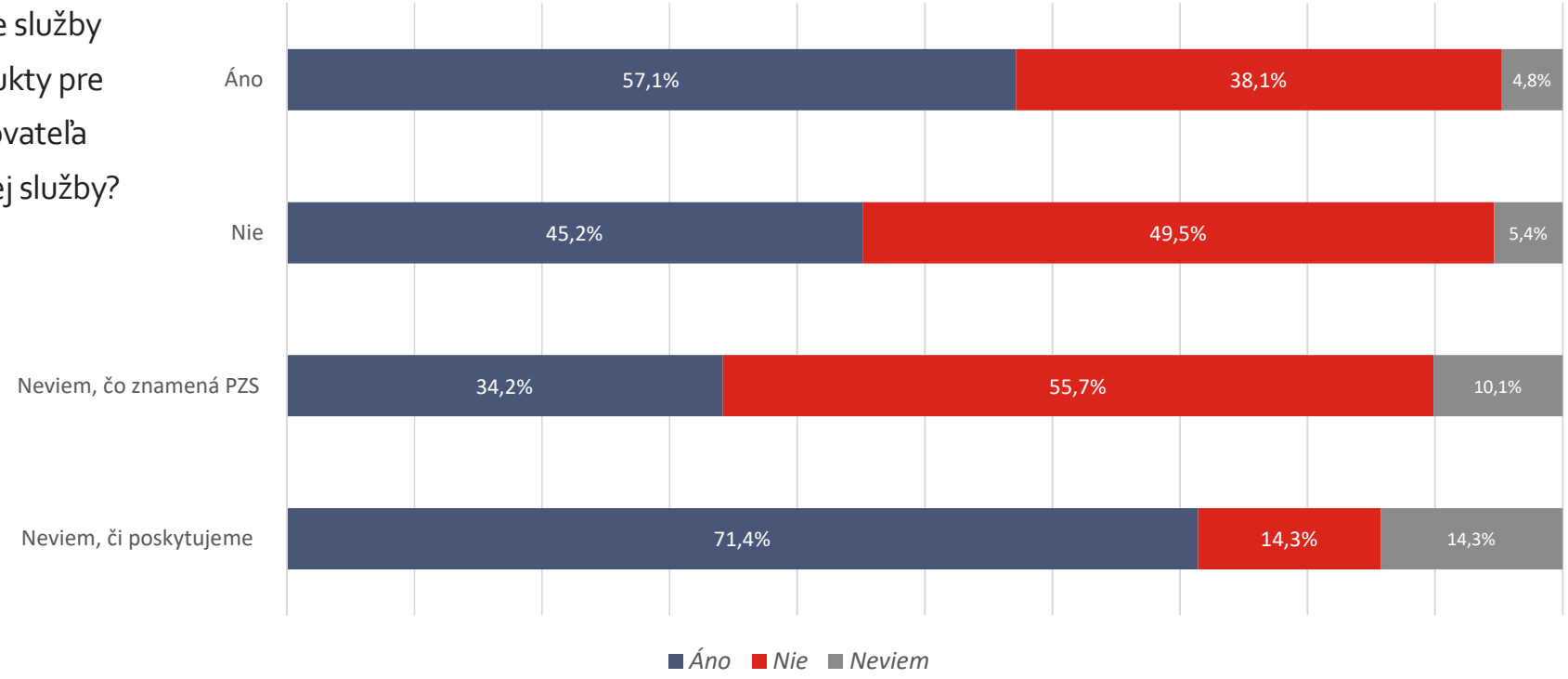
4.2 POROVNANIE PODĽA DODÁVANIA SLUŽIEB POSKYTOVATEĽOM ZS



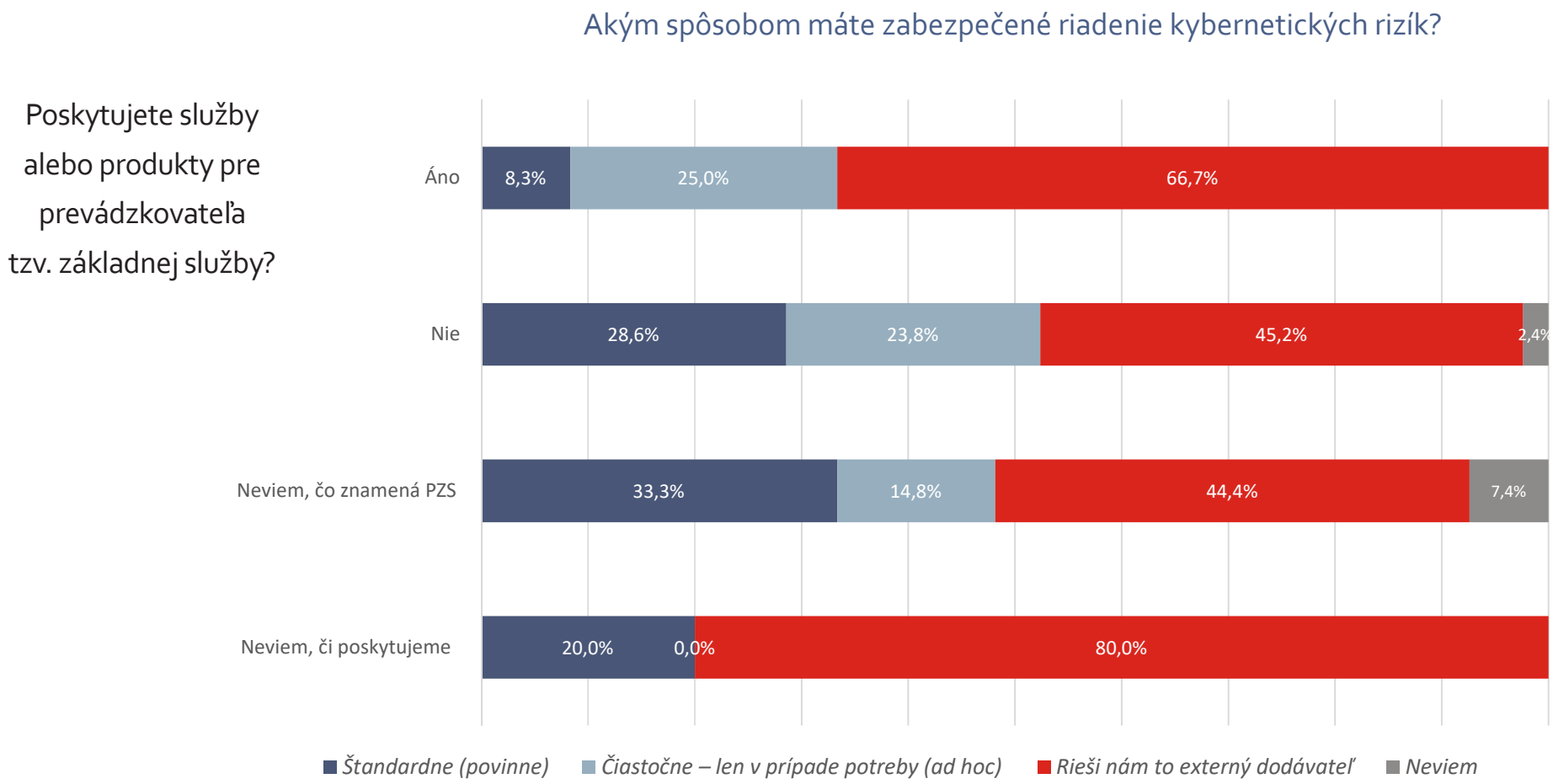
4.2 POROVNANIE PODĽA DODÁVANIA SLUŽIEB POSKYTOVATEĽOM ZS

Máte vo firemných procesoch zabezpečené RIADENIE KYBERNETICKÝCH RIZÍK vo svojej organizácii, aj keď vám to legislatíva neprikazuje?

Poskytujete služby alebo produkty pre prevádzkovateľa tzv. základnej služby?

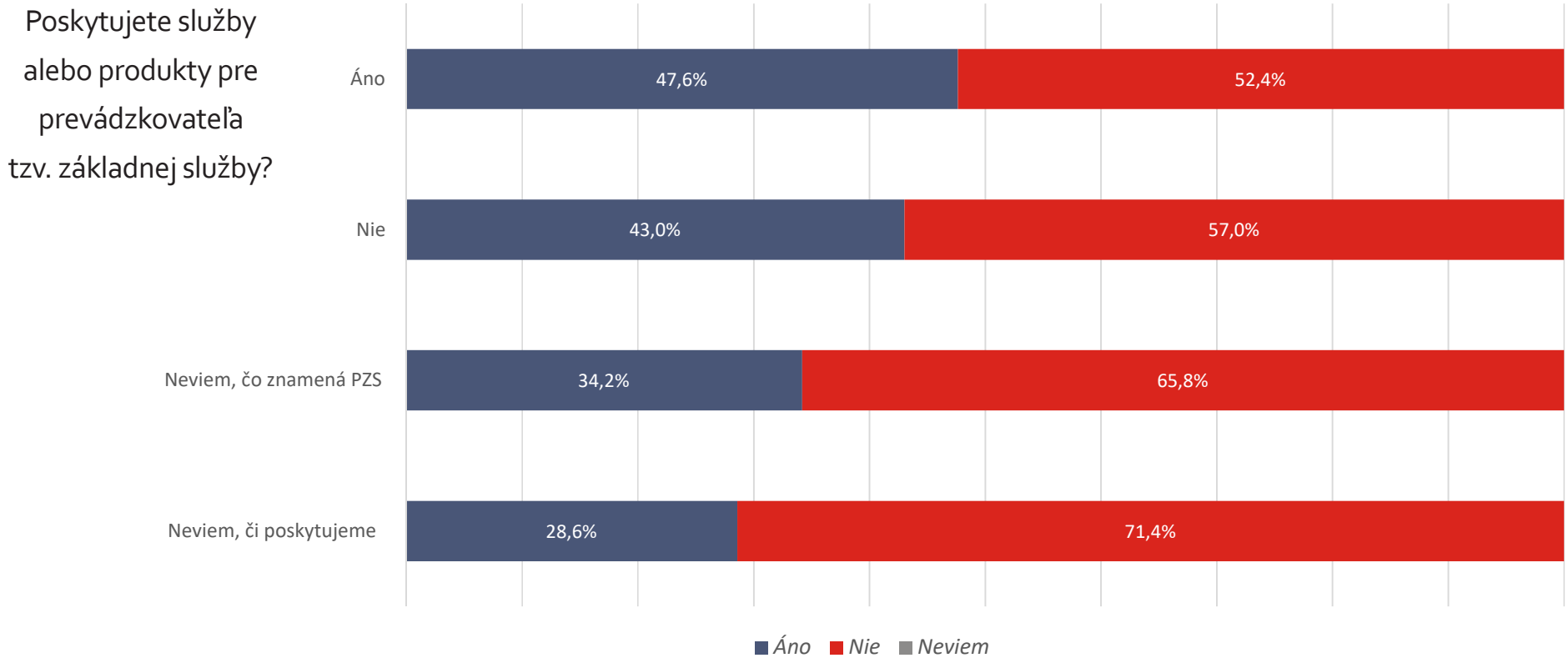


4.2 POROVNANIE PODĽA DODÁVANIA SLUŽIEB POSKYTOVATEĽOM ZS

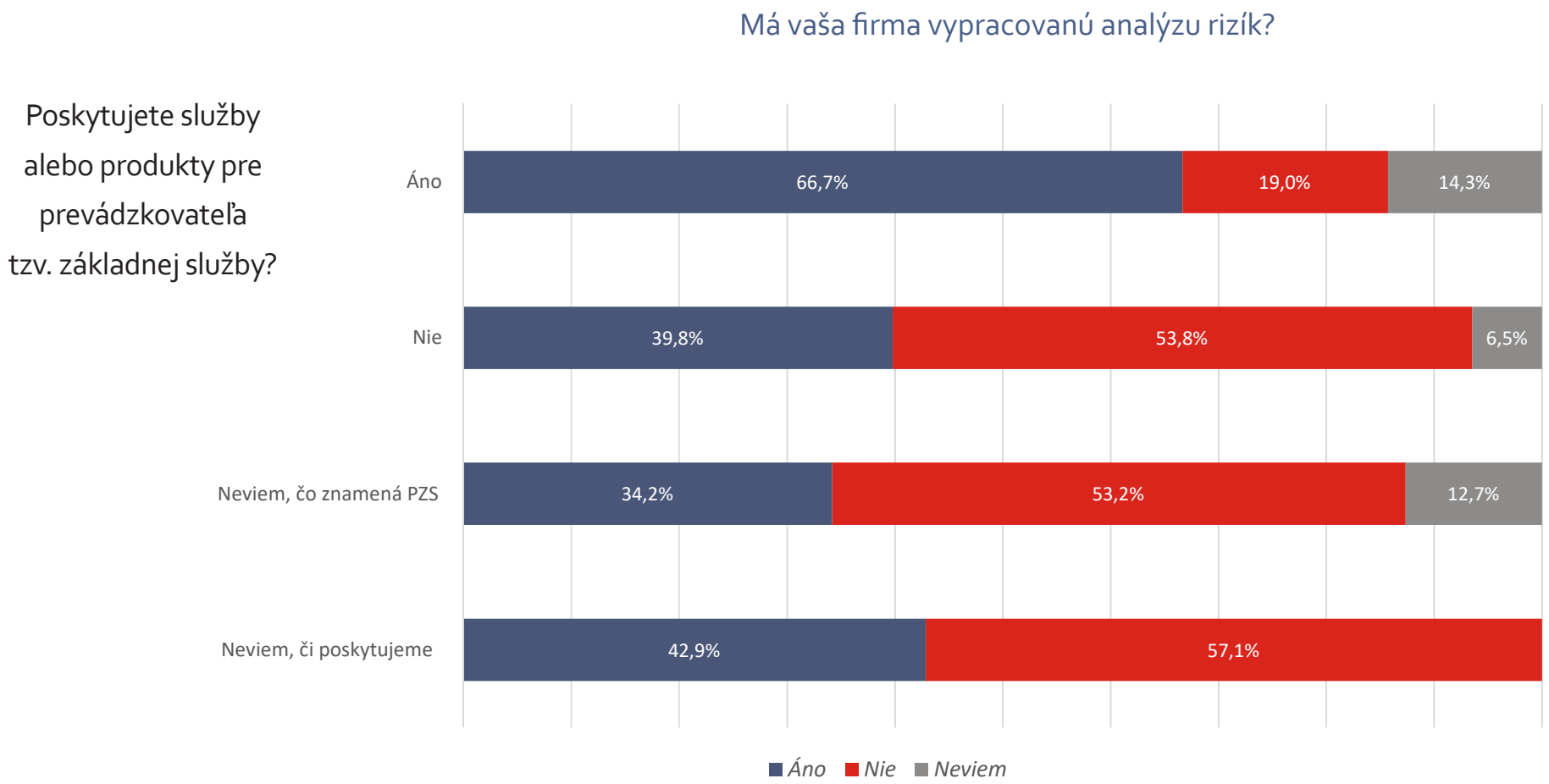


4.2 POROVNANIE PODĽA DODÁVANIA SLUŽIEB POSKYTOVATEĽOM ZS

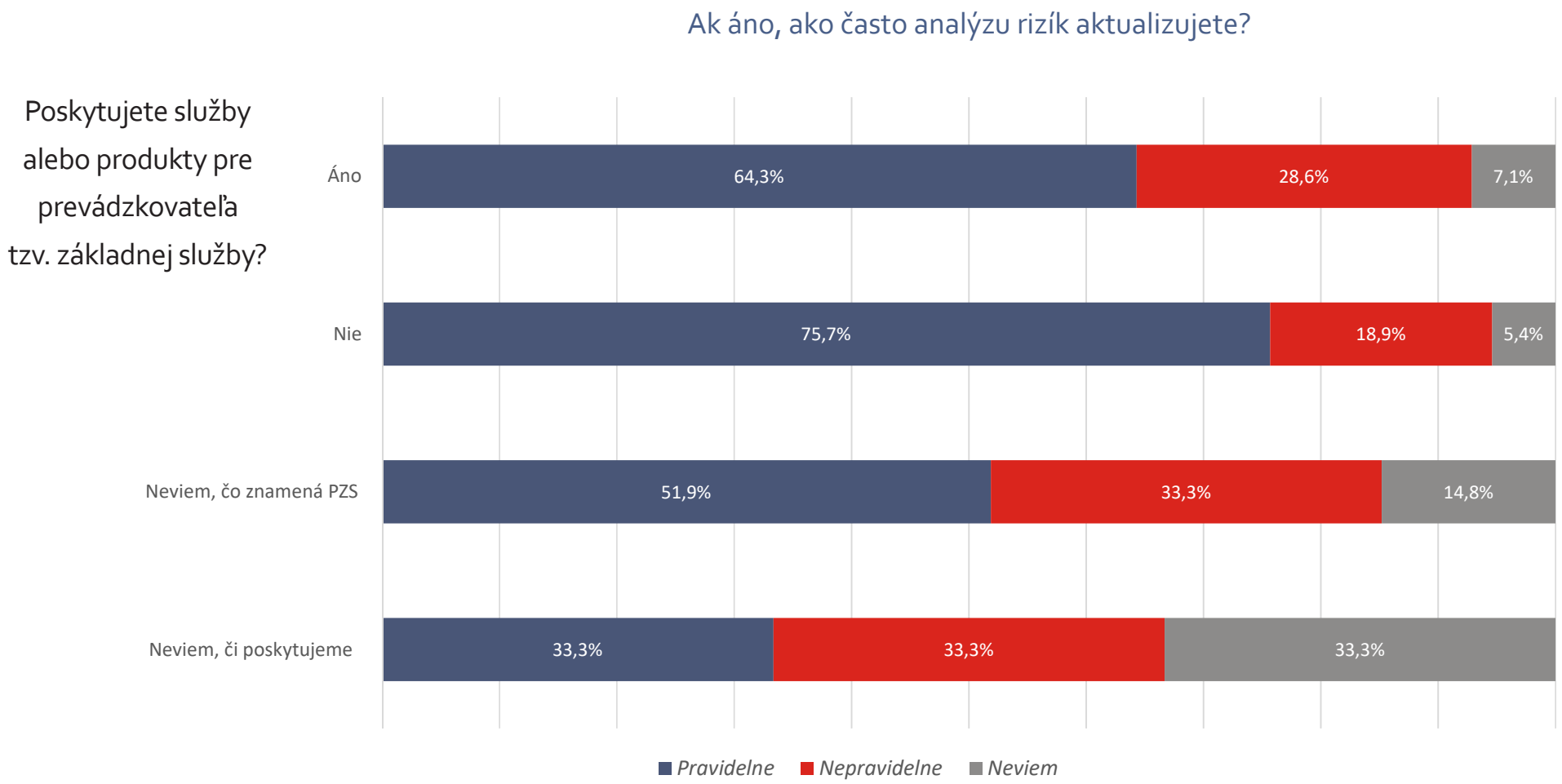
Poskytujete svojim zamestnancom možnosti školenia na zvyšovanie ich znalostí a schopností v oblasti kybernetickej bezpečnosti?



4.2 POROVNANIE PODĽA DODÁVANIA SLUŽIEB POSKYTOVATEĽOM ZS



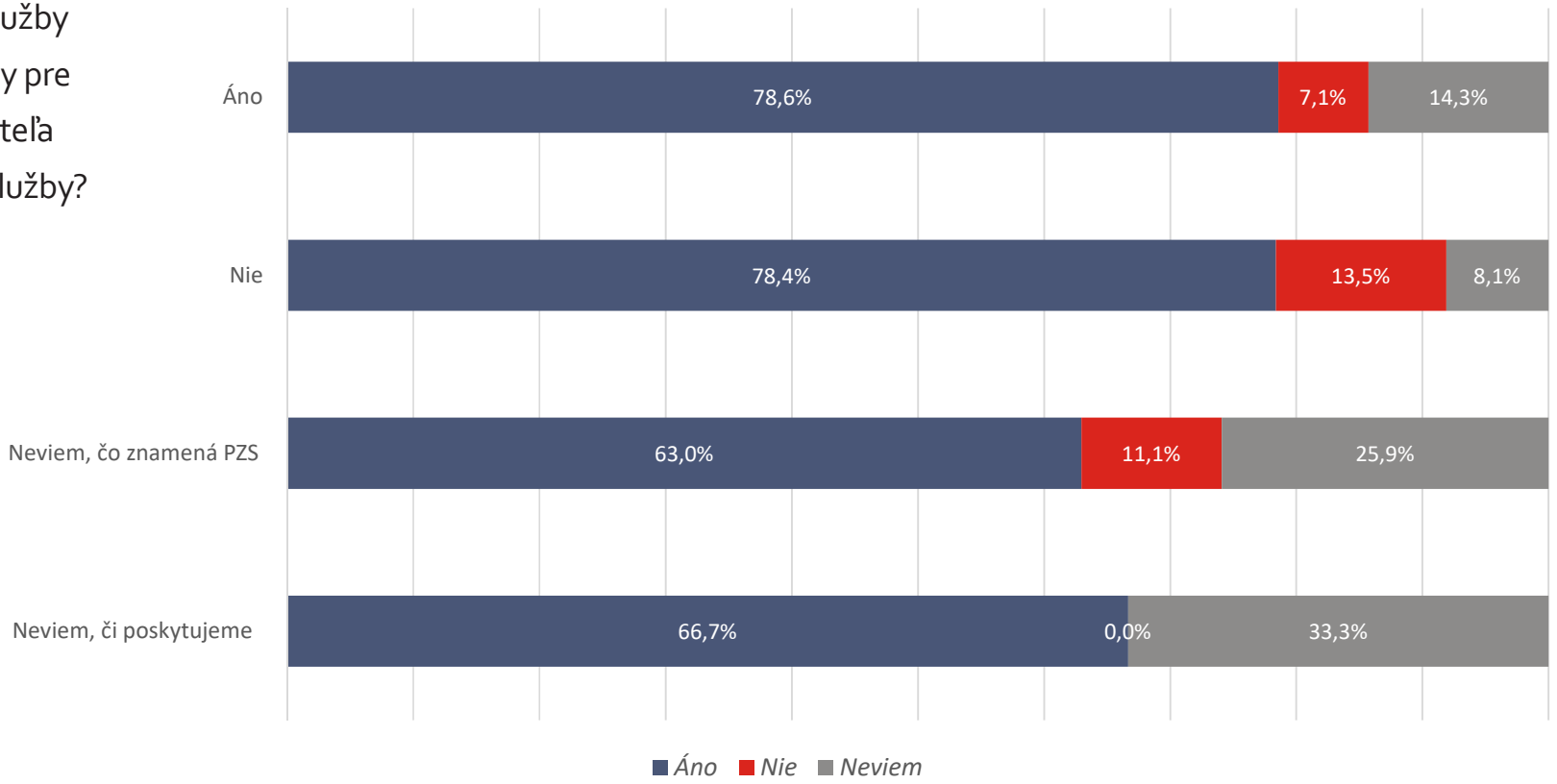
4.2 POROVNANIE PODĽA DODÁVANIA SLUŽIEB POSKYTOVATEĽOM ZS



4.2 POROVNANIE PODĽA DODÁVANIA SLUŽIEB POSKYTOVATEĽOM ZS

Je táto analýza založená na štandardizovanom procese riadenia rizík?

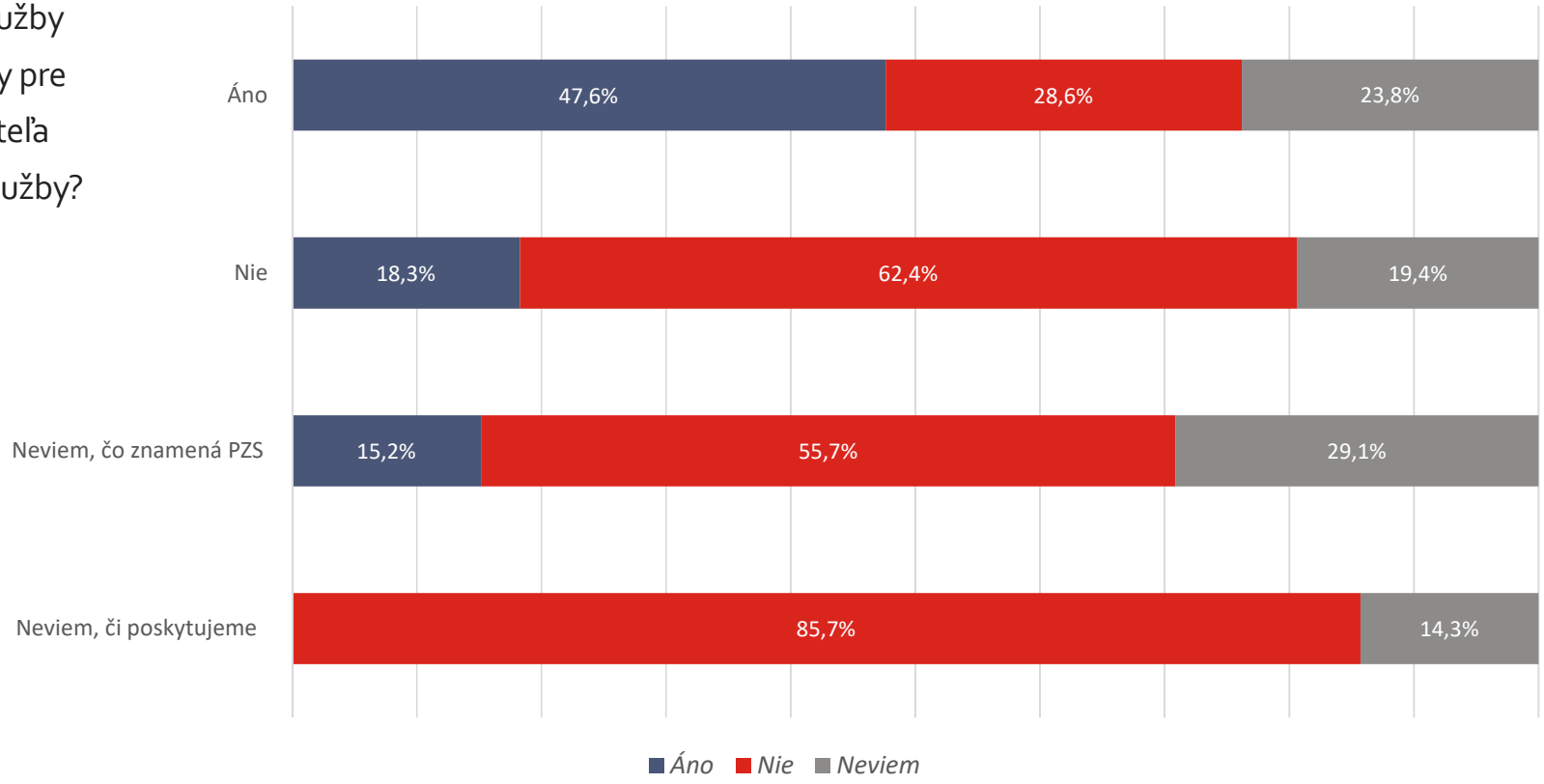
Poskytujete služby alebo produkty pre prevádzkovateľa tzv. základnej služby?



4.2 POROVNANIE PODĽA DODÁVANIA SLUŽIEB POSKYTOVATEĽOM ZS

Máte vypracované a pripravené plány kontinuity činnosti organizácie (BCP)?

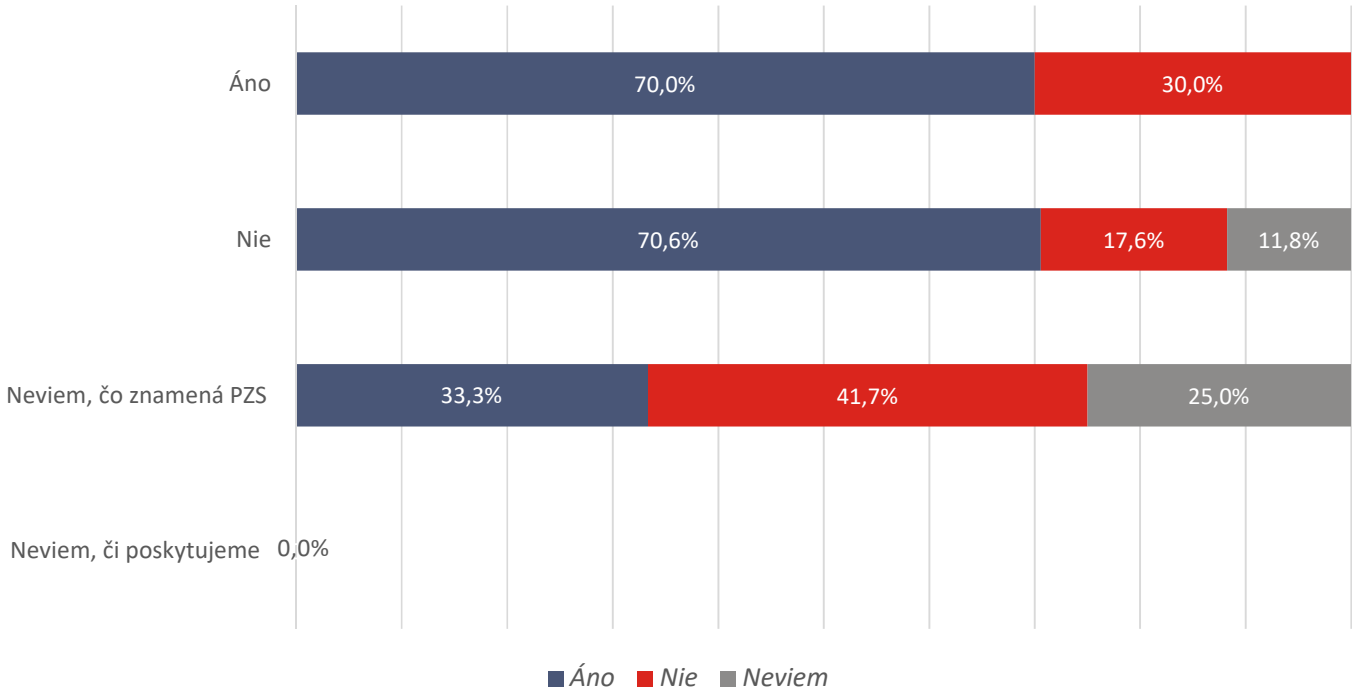
Poskytujete služby alebo produkty pre prevádzkovateľa tzv. základnej služby?



4.2 POROVNANIE PODĽA DODÁVANIA SLUŽIEB POSKYTOVATEĽOM ZS

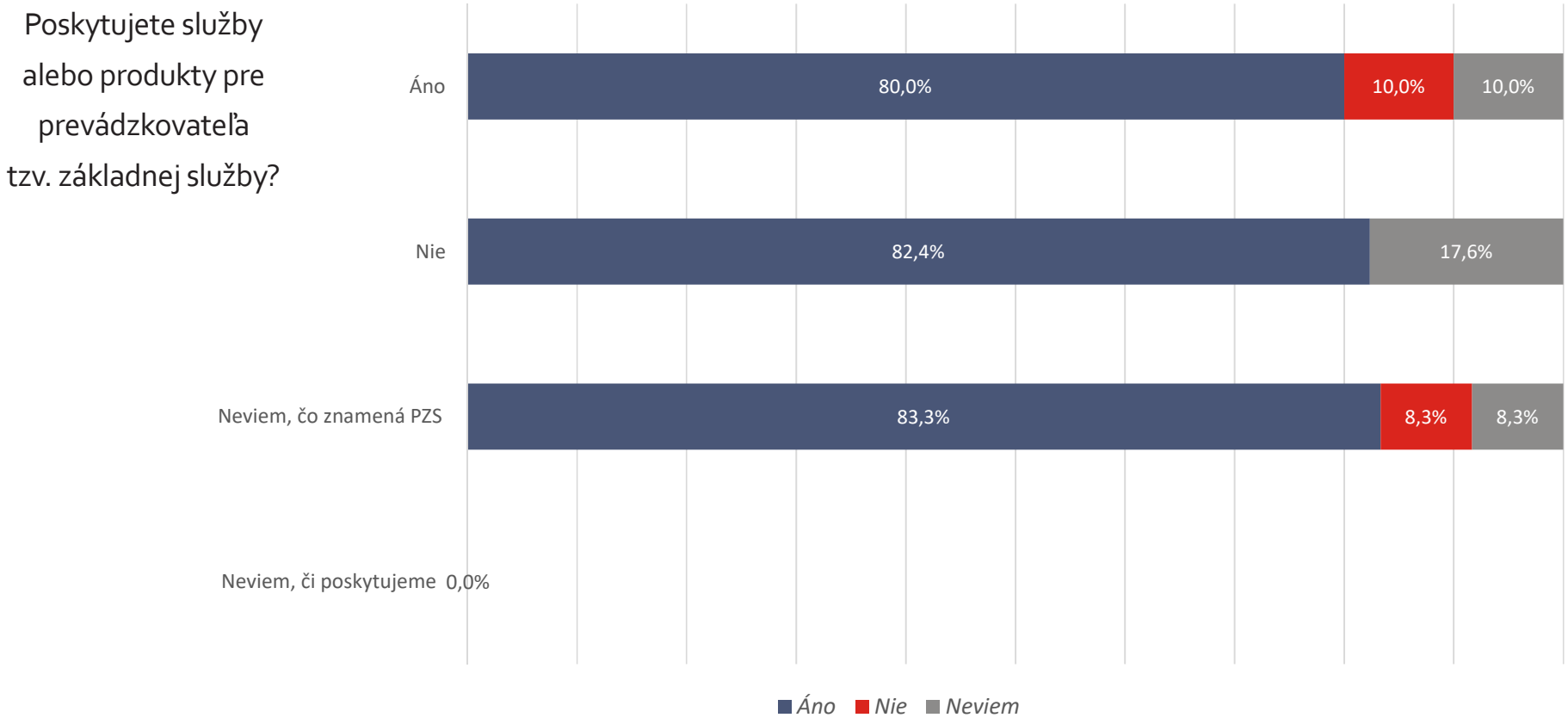
Vykonávate test BCP, pri ktorom overujete ich využiteľnosť, aspoň raz za rok?

Poskytujete služby alebo produkty pre prevádzkovateľa tzv. základnej služby?



4.2 POROVNANIE PODĽA DODÁVANIA SLUŽIEB POSKYTOVATEĽOM ZS

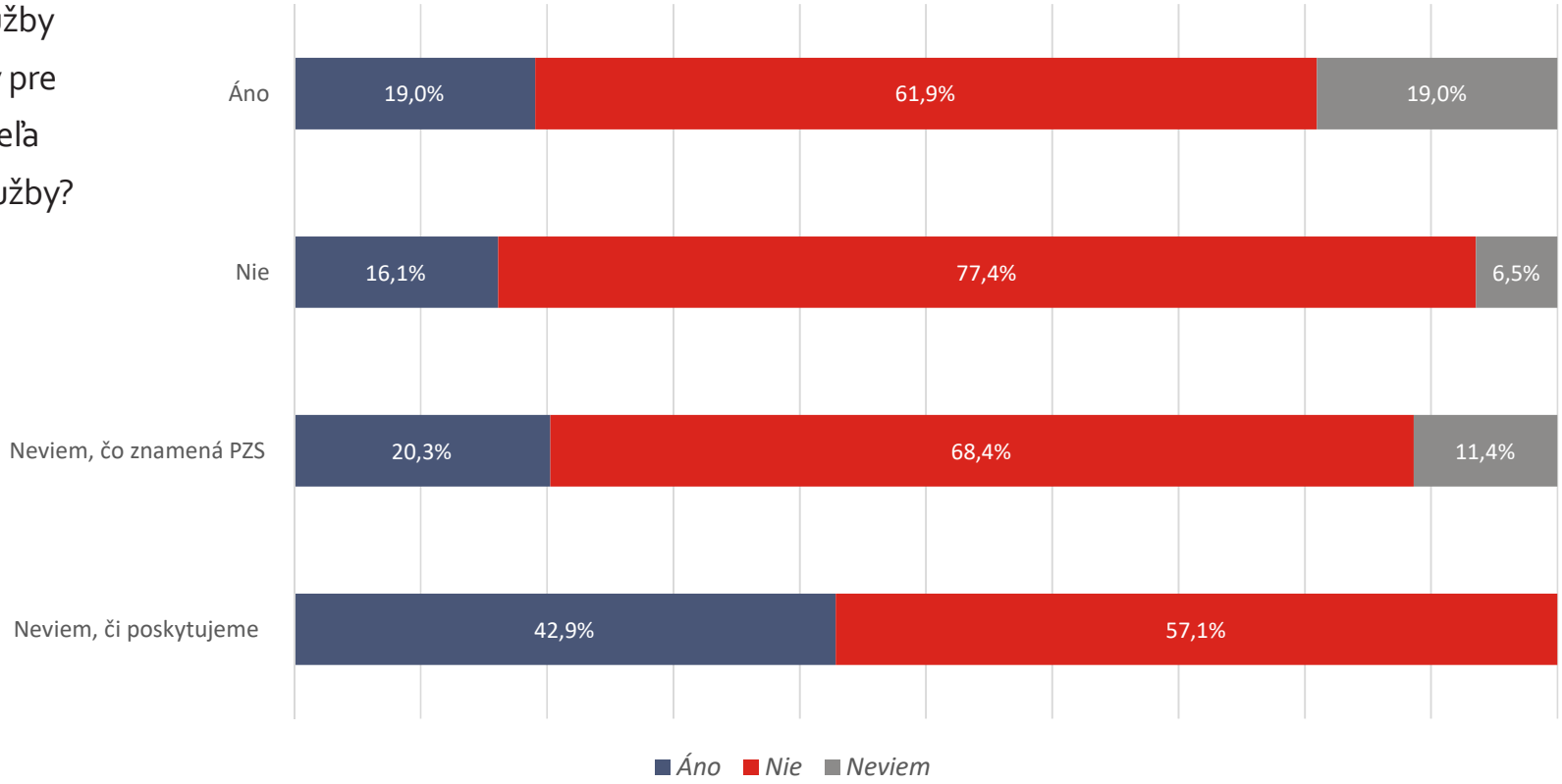
Sú tieto plány a testy založené na štandardizovanom procese riadenia kontinuity činností?



4.2 POROVNANIE PODĽA DODÁVANIA SLUŽIEB POSKYTOVATEĽOM ZS

Je rozpočet na kybernetickú bezpečnosť súčasťou rozpočtu firmy ako samostatná časť?

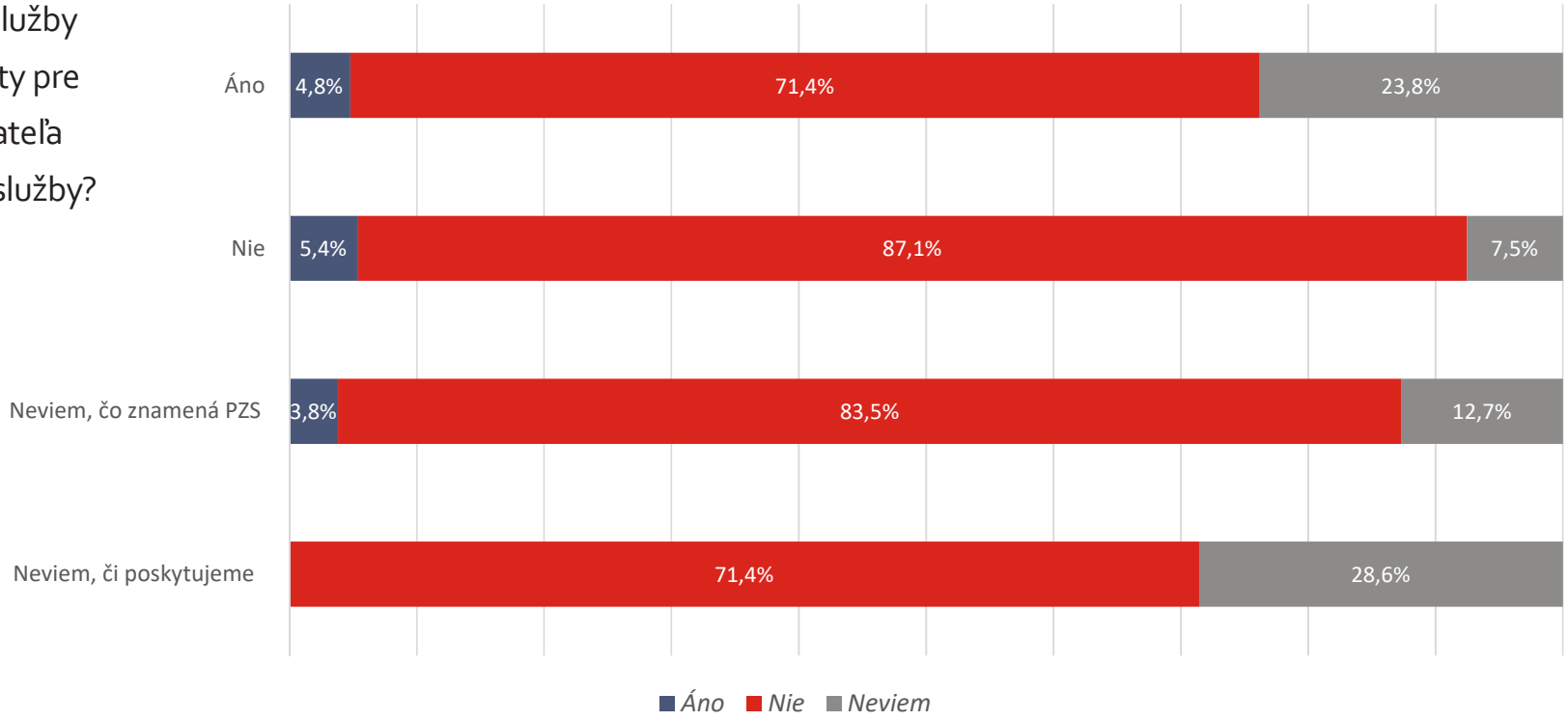
Poskytujete služby alebo produkty pre prevádzkovateľa tzv. základnej služby?



4.2 POROVNANIE PODĽA DODÁVANIA SLUŽIEB POSKYTOVATEĽOM ZS

Má vaša firma osobitne určený rozpočet na BCM
(výnimočné situácie v súvislosti s kybernetickou bezpečnosťou)?

Poskytujete služby alebo produkty pre prevádzkovateľa tzv. základnej služby?



METODIKA PRIESKUMU

METODIKA PRIESKUMU

Prieskum bol vypracovaný podľa medzinárodných štandardov kvality WAPOR, ESOMAR a štandardov Slovenskej Asociácie Výskumných Agentúr (SAVA), ktorých je agentúra AKO členom.

Agentúra AKO pôsobí na trhu 31 rokov.

METODIKA PRIESKUMU

Parametre prieskumu	malé a stredné podniky
metóda:	CATI (telefonicky prostredníctvom profesionálneho call centra)
veľkosť vzorky:	200
počet otázok:	2 skríningové + 4 štatistické + 13 meritórnych
termín zberu dát:	24. 4. - 2. 5. 2022
zloženie výskumnej vzorky:	reprezentatívne v kvótnych znakoch veľkosť podniku (podľa počtu zamestnancov) a sektor hlavnej činnosti
báza pre výber:	Štatistický úrad SR
anketovanie:	školení tele-anketári
kontrola:	skript, príposluch, spätná náhodná kontrola
štatistické spracovanie:	SPSS, Excel

UPOZORNENIE: *Pri druhostupňových triedeniach boli výsledky zaokrúhľované na celé čísla, a preto sa v ich súčte môže prejaviť odchýlka spôsobená zaokrúhľovaním.*

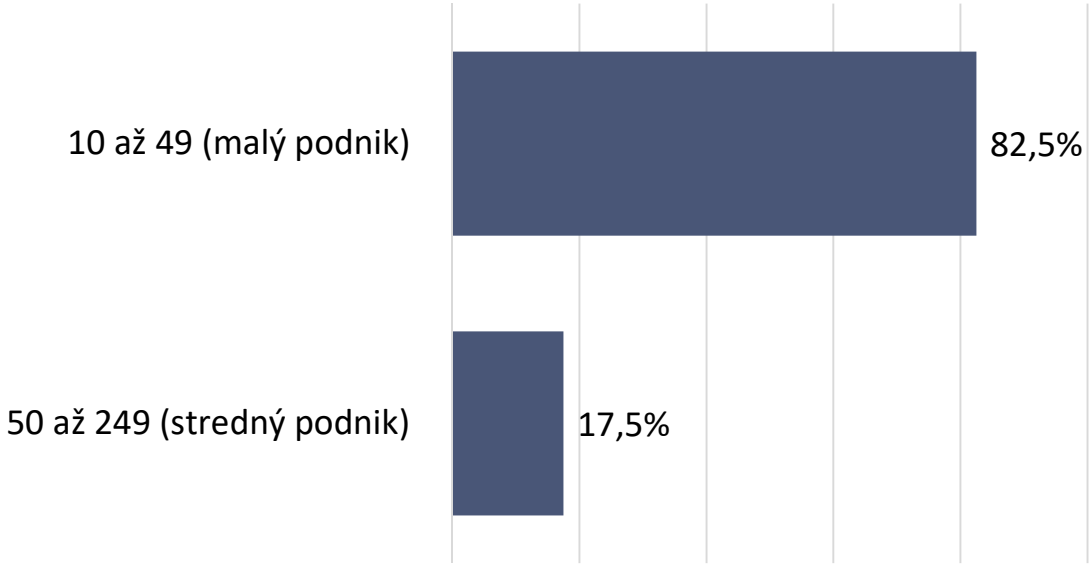
ŠTRUKTÚRA VZORKY MSP

ŠTRUKTÚRA VZORKY – MSP

„Koľko zamestnancov má vaša firma?"

Odpovede všetkých respondentov

N= 200



Zloženie prieskumnej vzorky je reprezentatívne z hľadiska veľkosti podniku a sektora, v ktorom podnik pôsobí.

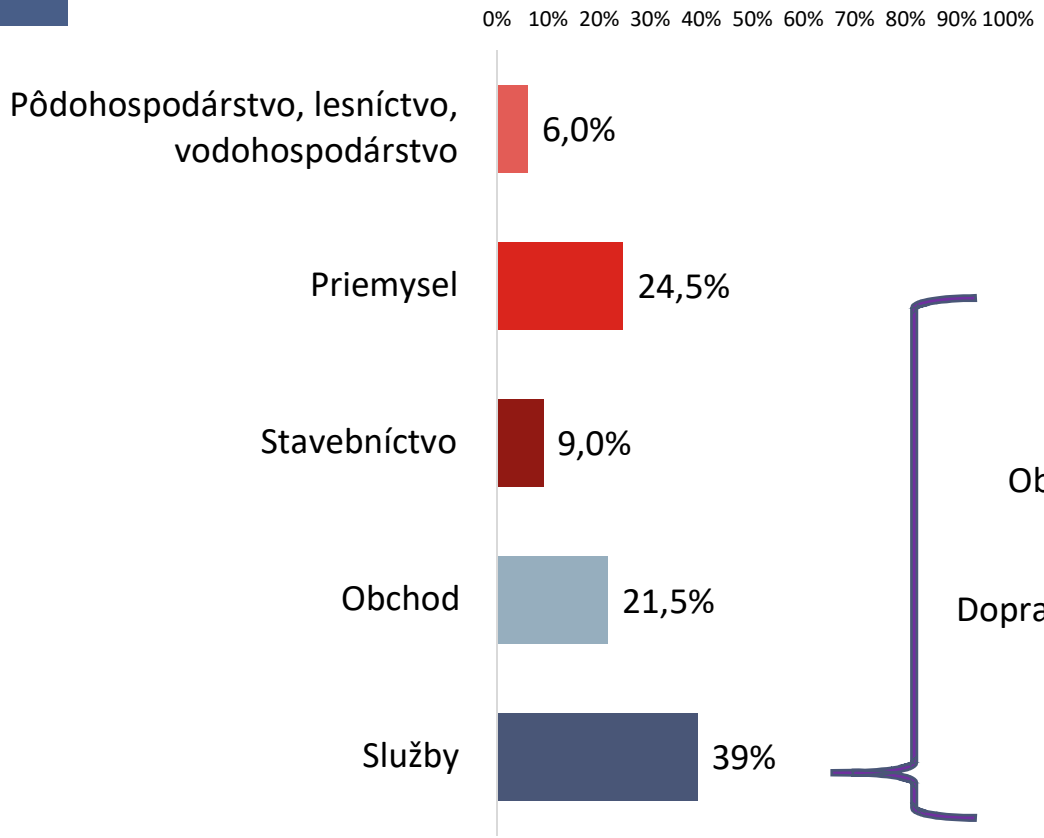
ŠTRUKTÚRA VZORKY - MSP

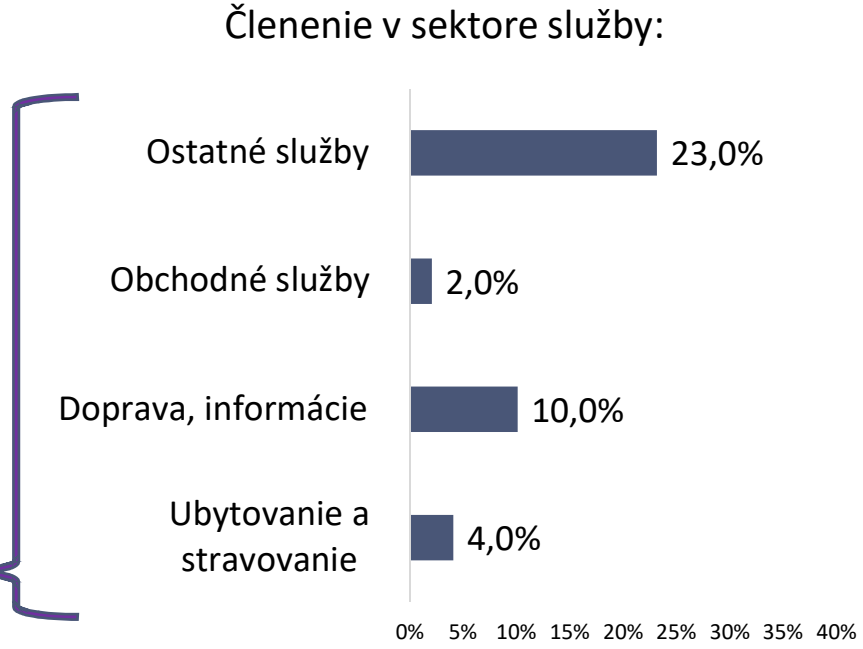
„Do akého odvetvia / sektora patrí hlavná činnosť Vašej firmy?"

Odpovede všetkých respondentov

N= 200

Zloženie prieskumnej vzorky je reprezentatívne z hľadiska veľkosti podniku a sektora, v ktorom podnik pôsobí.



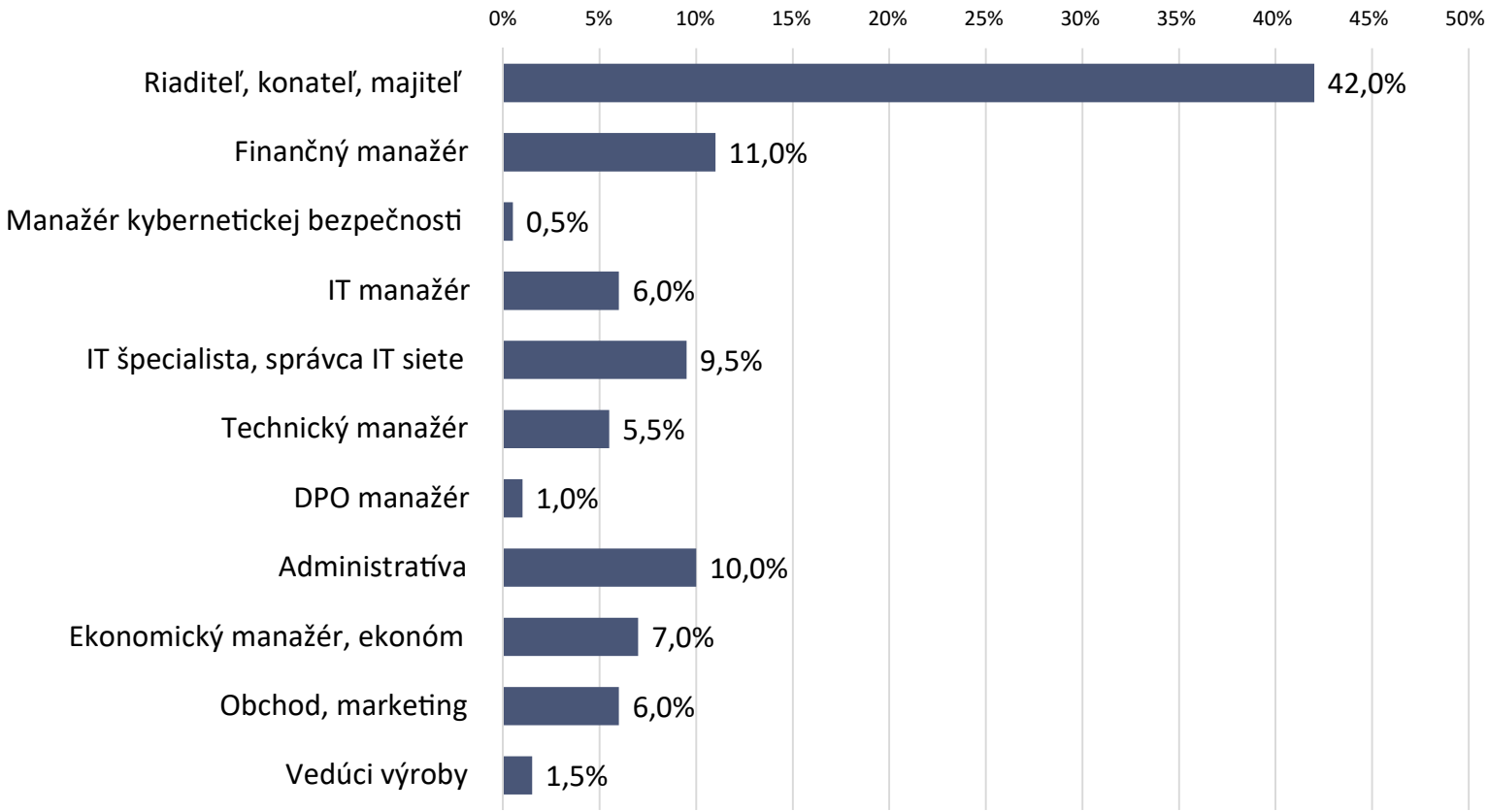


ŠTRUKTÚRA VZORKY – MSP

„Na akej pozícii vo firme pracujete?"

Odpovede všetkých respondentov

N= 200

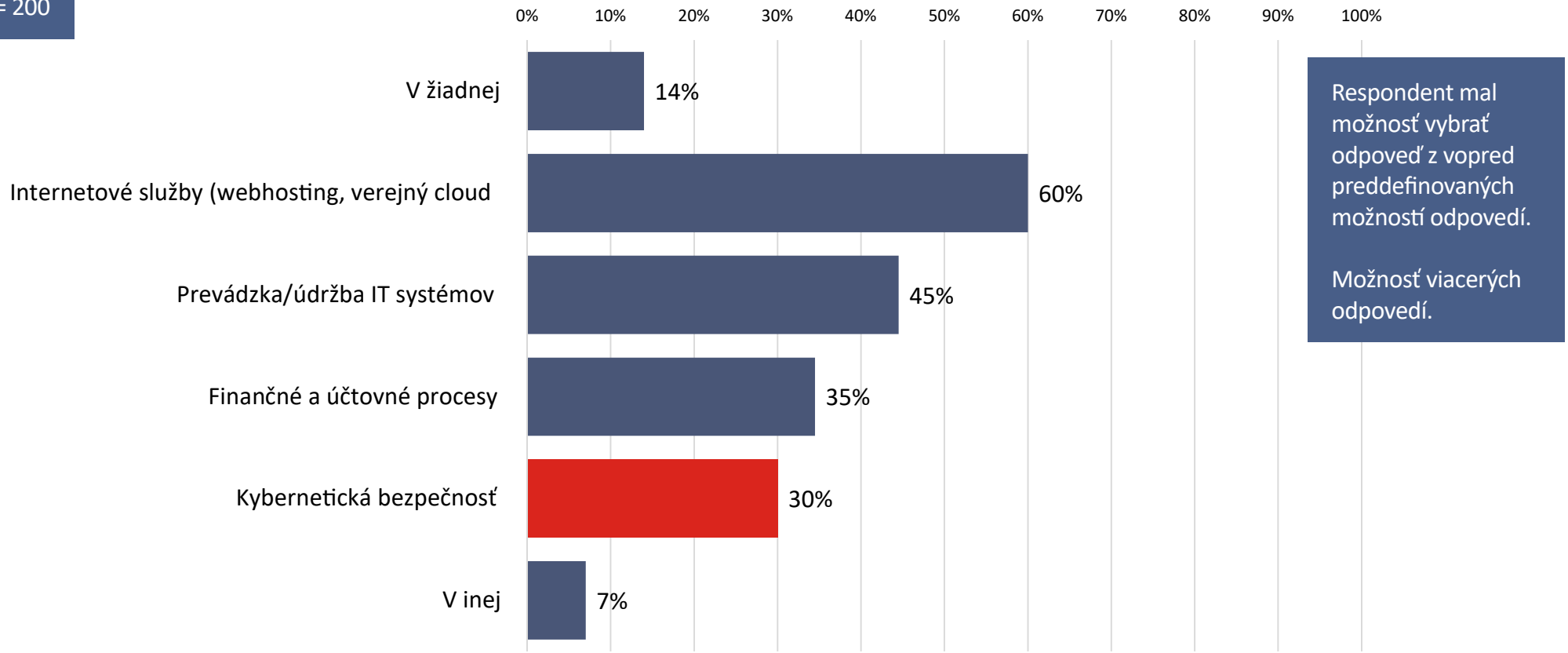


ŠTRUKTÚRA VZORKY - MSP

„V ktorej z týchto oblastí využíva vaša firma externé zdroje/procesy (outsourcing)?"

Odpovede všetkých respondentov

N= 200



ZHRNUTIE

ZHRNUTIE

Hoci každá časť prieskumu obsahuje priebežné štatistické vyhodnotenie, vrátane interpretácie významu číselných údajov, považujeme za užitočné na tomto mieste uviesť manažérske zhrnutie podstatných, alebo zaujímavých zistení.

Negatívne zistenia:

- U respondentov identifikujeme výraznú neznalosť odbornej terminológie
- Odpovede typu „neviem", „nijako" a „iné" sú typickými únikovými odpoveďami, keďže pre respondenta predstavujú istotu správnej odpovede
- Definícia priorít a smerovania pre oblasť kybernetickej bezpečnosti nie je u MSP pragmatická a preventívna (t.j. nie je odvodená od strategických cieľov podniku, z procesov riadenia rizík, alebo od zistení auditu)
- Štatutári MSP sú náchylnejší spoliehať sa na odporúčania dodávateľov, ako na úsudok odborných zamestnancov
- Nedávny boom povinností, súvisiacich s implementáciou požiadaviek na ochranu osobných údajov ovplyvnil vnímanie štatutárov v zmysle presvedčenia, že majú zároveň splnené aj povinnosti v kontexte kybernetickej bezpečnosti
- Všeobecné nariadenie EÚ o ochrane údajov (GDPR) negatívne ovplyvnilo presvedčenie štatutárov, že opatreniami aj v kybernetickej bezpečnosti sú najmä organizačné opatrenia
- Respondenti nejednoznačne rozlišujú pojem „incident" - podniky usudzujú, že prevládajú útoky „z externého prostredia", t.j. vonkajšej strany sieťového perimetra
- Zamestnanci kladú pasívny odpor bezpečnostným opatreniam, pretože pri ich používaní sú bezprostredne konfrontovaní s nedostatkom vlastných digitálnych zručností
- Len štyri z desiatich SME podnikov deklarujú, že poskytujú zamestnancom školenia na zvyšovanie ich znalostí a zručností v oblasti kybernetickej bezpečnosti; takmer 2/3 respondentov si však myslí, že školenia v kybernetickej bezpečnosti potrebujú len špecialisti

ZHRNUTIE

- Takmer tri štvrtiny opýtaných MSP nevedeli uviesť, podľa ktorej technickej alebo právnej normy postupujú pri implementácii bezpečnostných opatrení v kybernetickej bezpečnosti
- Hoci mnohé podniky majú zavedenú nejakú formu riadenia rizík, iba 25% podnikov sa zaoberá riadením rizík štandardným, konsolidovaným spôsobom
- Aktualizované a otestované plány kontinuity činnosti (BCP) má iba 29% MSP
- 71,5% MSP nemá samostatnú časť rozpočtu na kybernetickú bezpečnosť
- Z kontextu odpovedí o rozpočte na kybernetickú bezpečnosť vyplýva, že tento pojem si firmy pravdepodobne spájajú s rozpočtom na prevádzku IT
- Približne každý desiaty opýtaný MSP (mimo poskytovateľov základnej služby) svoju podnikateľskú činnosť realizuje pre iného poskytovateľa základnej služby, avšak podniky nepoznajú svoju bezpečnostnú rolu v dodávateľsko-odberateľskom reťazci (supply chain)

Pozitívne zistenia:

- Výsledky prieskumu sú reprezentatívne z hľadiska veľkosti podniku a sektora, v ktorom podnik primárne pôsobí
- V porovnaní s priemerným výsledkom, z hľadiska sektorov uvádzajú ohrozenie kybernetickými útokmi najmä podniky zo sektoru priemyslu, obchodu, obchodných služieb a ostatných služieb
- Odporúčania dodávateľov majú pozitívny vplyv na zvyšovanie celkovej úrovne kybernetickej bezpečnosti
- Z výsledkov prieskumu vyplýva, že 43% MSP má vo firemných procesoch zavedené riadenie kybernetických rizík, aj keď im to legislatíva neprikazuje
- Medzi najviac nedostatkové znalosti zamestnancov sú takmer polovice opýtaných MSP správne považované najmä digitálne zručnosti

Spolufinancovaný Európskou úniou

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberajú žiadnu zodpovednosť.

ISBN 978-80-69011-14-4

Verzia V.1