DIGITALIZACE A KYBERBEZPEČNOST

Závěrečná zpráva

Červen 2023

AMSP ČR

ŠKODA Google KB

vodafone Deloitte.

PKF APOGEO merXu CZECHINVEST Drive for success

GAME CHANGERS

Ipsos

VÝZKUMNÉ POZADÍ

Asociace malých a středních podniků a živnostníků ČR sdružuje na otevřené, nepolitické platformě malé a střední podniky a živnostníky i jejich organizace z celé České republiky. Kromě návrhů legislativy se zabývá také tématy jako je export, inovace, financování či vzdělávání.

Ve spolupráci se svými partnery AMSP ČR průběžně realizuje projekty cílené na aktuální otázky ve své oblasti působení, podporované výzkumy trhu.

Hlavním cílem výzkumu bylo zjistit, jak proces digitalizace ovlivňuje malé a střední podniky a s jakými problémy se v rámci implementace digitalizace potýkají.

METODIKA

Metoda ankety	**Online dotazování, Ipsos B2B panel**
Cílová skupina	**Majitelé, jednatelé a ředitelé malých a středních firem o velikosti 4-249 zaměstnanců**
Velikost vzorku	**202 firem** **sběr proběhl 11. 5. – 30. 5. 2023**
Výzkumný nástroj	**Strukturovaný dotazník o délce cca 7 minut** **Vyznačené rozdíly v rámci podskupin jsou sig. na hladině 95 %**

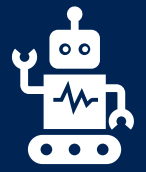
SHRNUTÍ VÝSLEDKŮ

HLAVNÍ ZÁVĚRY (1/2)

Největší motivací k digitalizaci je zvýšení efektivity či produktivity a snížení nákladů.

Třetina firem má určený plán digitální transformace. V případě podniků ze sektoru služeb je to však jen pětina.

Dle podniků může cloud computing přinést převážně zjednodušenou správu IT, úsporu nákladů a vzdálený přístup či spolupráci.



Zavedení AI může přinést úsporu nákladů, zvýšení efektivity či produktivity a lepší analýzu dat.

4 z 10 podniků udávají, že v následujících 5-10 letech umělá inteligence a cloud computing odvětví jejich společnosti nijak neovlivní, nebo neví, zdali ho ovlivní. Ostatní udávají, že bude dané odvětví změněno ve velké míře, nebo udávají konkrétní příklady změn.

HLAVNÍ ZÁVĚRY (2/2)

Pětina firem zažila během procesu digitalizace jisté neúspěchy či selhání, nejčastěji se jednalo o technický problém.

Téměř třetina firem se setkala s kyberútokem, nejčastěji se jednalo o podvodné faktury.

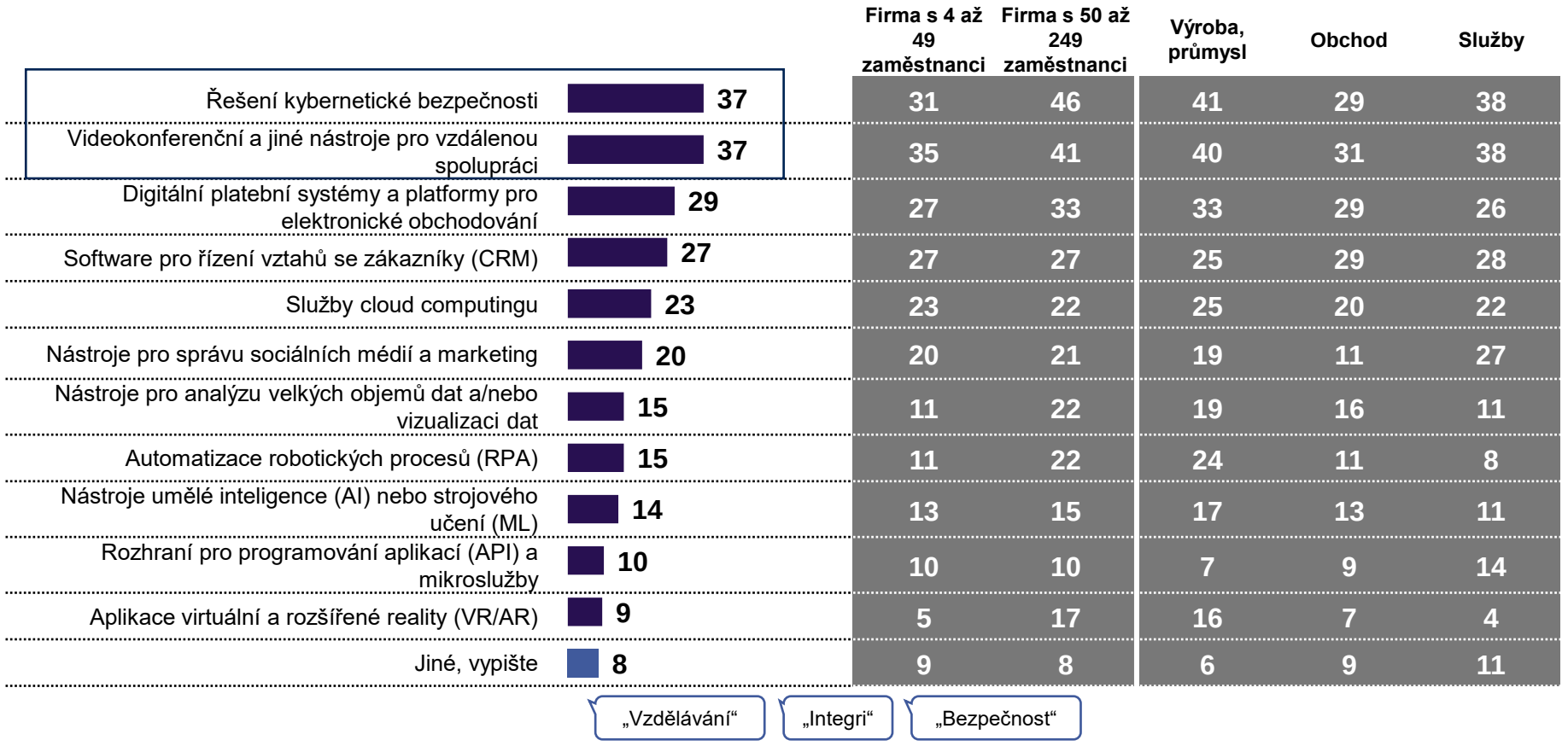
Jako největší riziko z hlediska zabezpečení vnímají firmy lidský faktor.

Vnímanými lídry v bezpečnosti internetového online bankovnictví jsou Česká spořitelna, ČSOB a Komerční banka.

VÝSLEDKY V DETAILU

SPOLEČNOSTI NEJČASTĚJI PŘIJALY NEBO ZAVÁDÍ TECHNOLOGIE ŘEŠÍCÍ KYBERNETICKOU BEZPEČNOST A NÁSTROJE PRO VZDÁLENOU SPOLUPRÁCI.

Digitální technologie, které společnosti přijaly či zavádí (v %)



	Firma s 4 až 49 zaměstnanci	Firma s 50 až 249 zaměstnanci	Výroba, průmysl	Obchod	Služby
Řešení kybernetické bezpečnosti	31	46	41	29	38
Videokonferenční a jiné nástroje pro vzdálenou spolupráci	35	41	40	31	38
Digitální platební systémy a platformy pro elektronické obchodování	27	33	33	29	26
Software pro řízení vztahů se zákazníky (CRM)	27	27	25	29	28
Služby cloud computingu	23	22	25	20	22
Nástroje pro správu sociálních médií a marketing	20	21	19	11	27
Nástroje pro analýzu velkých objemů dat a/nebo vizualizaci dat	11	22	19	16	11
Automatizace robotických procesů (RPA)	11	22	24	11	8
Nástroje umělé inteligence (AI) nebo strojového učení (ML)	13	15	17	13	11
Rozhraní pro programování aplikací (API) a mikroslužby	10	10	7	9	14
Aplikace virtuální a rozšířené reality (VR/AR)	5	17	16	7	4
Jiné, vypište	9	8	6	9	11

„Vzdělávání“ „Integri“ „Bezpečnost“

Komentář AMSP ČR:

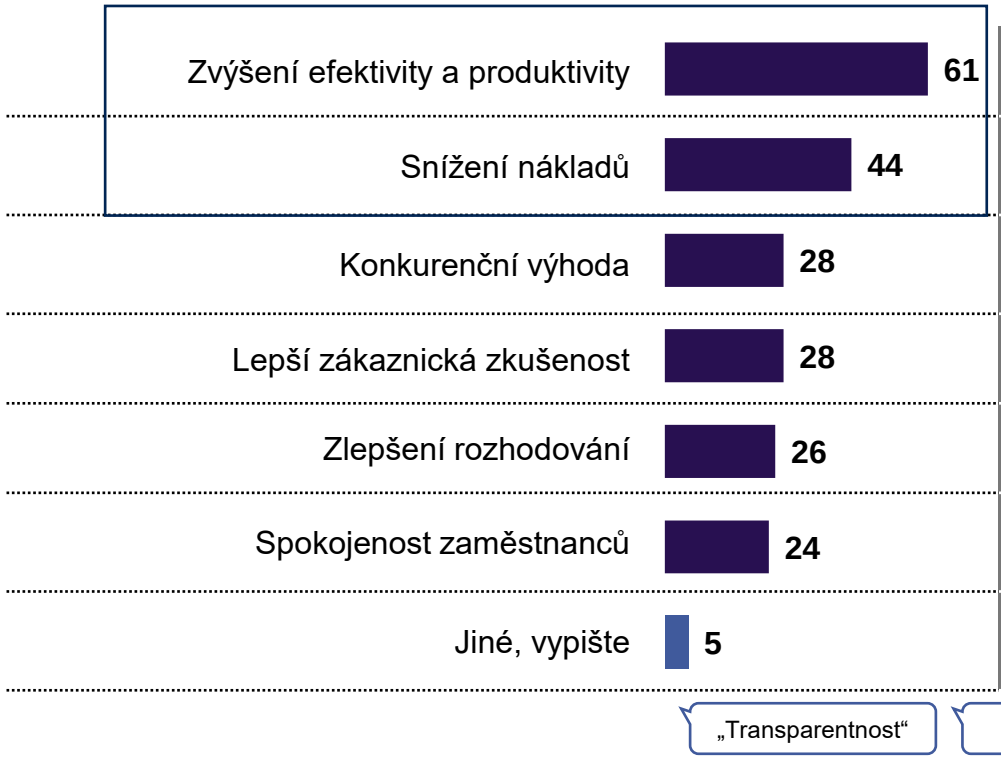
Jakkoli je oblast kyberbezpečnosti v porovnání s velkými firmami zatím slabší, **MSP nejsou v této oblasti žádnými outsidery**. **Řešení kybernetické bezpečnosti** je u MSP na prvních příčkách digitálních řešení, jak ukazuje náš průzkum. Stejnou pozici zastávají i nástroje **pro vzdálenou spolupráci** (37 %) – to jsou oblasti, kterým MSP přikládají důležitost.

S odstupem jsou následovány nástroji pro ELEKTRONICKÉ OBCHODOVÁNÍ a ŘÍZENÍ VZTAHŮ SE ZÁKAZNÍKY. Poměrně významné je i zastoupení CLOUDU.

D1. Které z následujících digitálních technologií vaše společnost přijala nebo v současné době zavádí? (Vyberte všechny možnosti, které se na vás vztahují)
N=202/124/78/83/45/74

NEJVĚTŠÍ MOTIVACÍ PRO DIGITALIZACI JE ZVÝŠENÍ EFEKTIVITY A PRODUKTIVITY. S O NĚCO MENŠÍ ČETNOSTÍ TAKÉ SNÍŽENÍ NÁKLADŮ.

Hlavní motivace k digitalizaci (v %)



	Firma s 4 až 49 zaměstnanci	Firma s 50 až 249 zaměstnanci	Výroba, průmysl	Obchod	Služby
Zvýšení efektivity a produktivity	62	60	49	67	72
Snížení nákladů	42	46	43	40	46
Konkurenční výhoda	24	33	29	36	22
Lepší zákaznická zkušenost	24	33	30	29	24
Zlepšení rozhodování	21	33	34	18	22
Spokojenost zaměstnanců	26	22	22	27	26
Jiné, vypište	7	3	7	4	4

„Transparentnost“ „Bezpečnost“

Komentář AMSP ČR:

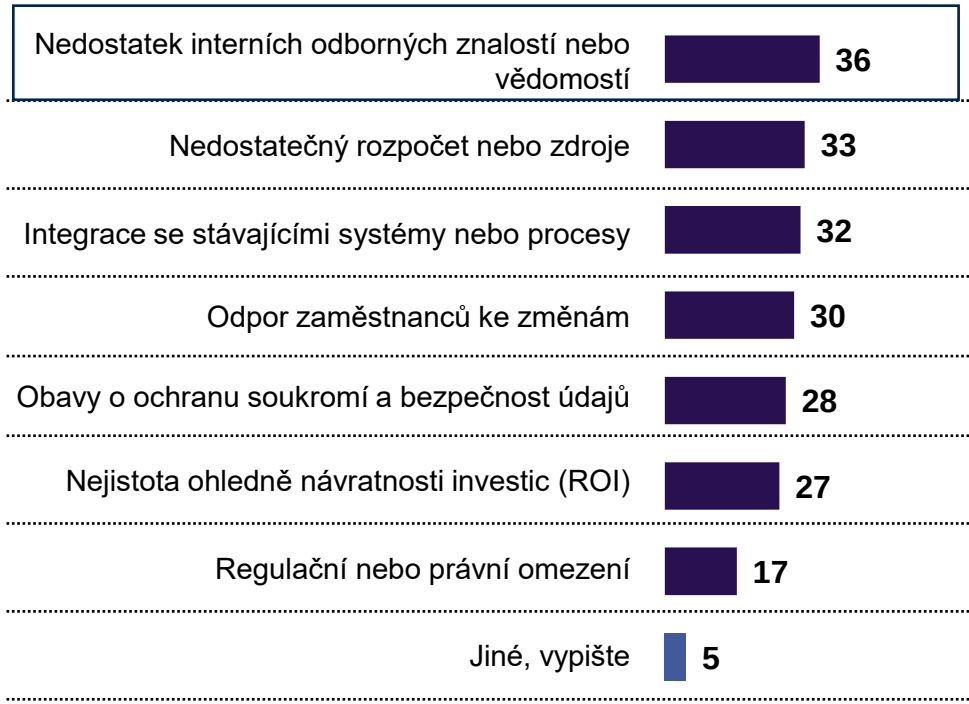
MSP jsou tradičně nejlepšími hospodáři – nejsou to korporáty, a už vůbec ne stát. MSP nekompromisně zvažují, **co vynaložený náklad přinese, jakou získají přidanou hodnotu.** Ukázalo se nám to již v průzkumu na téma Automatizace-Robotizace, a nejinak je tomu i v případě DIGITALIZACE.

MSP striktně sledují efektivitu vynaložených zdrojů, je tedy logické, že **největším motorem digitalizace v MSP je zvyšování produktivity (61 %) a snižování nákladů (44 %).** Výrazným výsledkem bylo až 72 % důrazu na efektivitu v případě SLUŽBOVÉHO SEKTORU.

D2. Jaká je hlavní motivace digitalizace vaší společnosti?
N=202/124/78/83/45/74

NEJČASTĚJŠÍ VÝZVOU PŘI DIGITALIZACI JE NEDOSTATEK INTERNÍCH ODBORNÝCH ZNALOSTÍ ČI VĚDOMOSTÍ.

Výzvy, kterým firmy čelí během procesu digitalizace (v %)



	Firma s 4 až 49 zaměstnanci	Firma s 50 až 249 zaměstnanci	Výroba, průmysl	Obchod	Služby
Nedostatek interních odborných znalostí nebo vědomostí	32	42	39	38	32
Nedostatečný rozpočet nebo zdroje	29	38	29	29	39
Integrace se stávajícími systémy nebo procesy	29	36	29	42	28
Odpor zaměstnanců ke změnám	27	35	31	29	30
Obavy o ochranu soukromí a bezpečnost údajů	30	26	33	24	26
Nejistota ohledně návratnosti investic (ROI)	21	36	35	27	18
Regulační nebo právní omezení	13	23	18	11	19
Jiné, vypište	6	3	6	4	4

Komentář AMSP ČR:

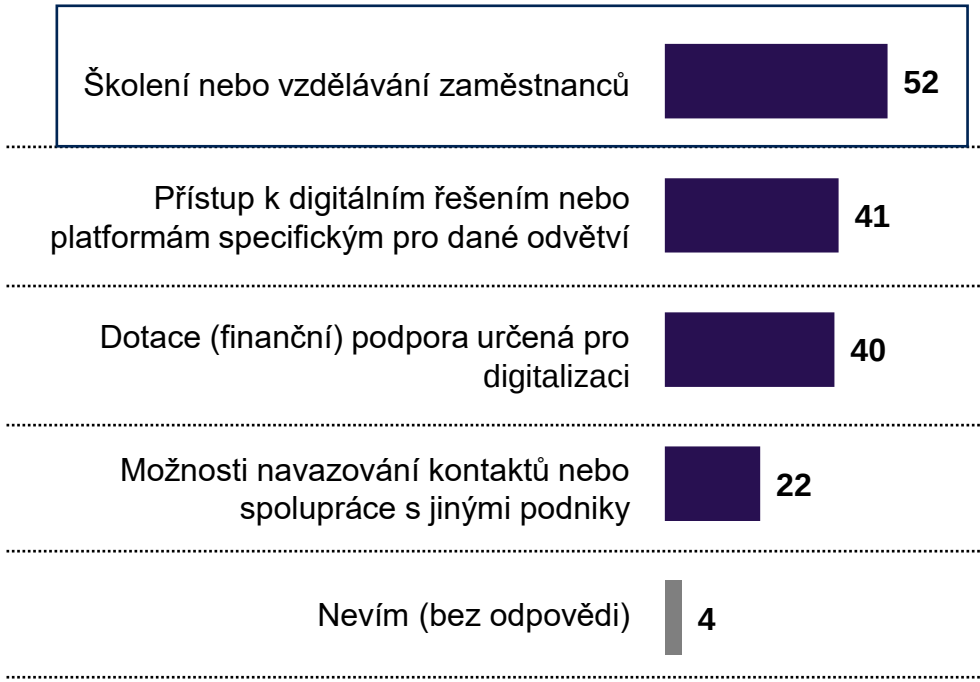
Nejčastěji zmiňovanou bariérou či výzvou pro MSP je při digitalizaci **nedostatek interních odborných znalostí či vědomostí**. To není zvláště překvapivé: MSP logicky zpravidla nemají specializované útvary na různé podpůrné odbornosti jako například HR, daňové služby, ale rovněž digitalizační procesy. Problémem je někdy ale i outsourcing – specialistů je buď na trhu nedostatek, nebo si je obsadí velké firmy, mnohdy i díky vládním incentivám, čímž si podkopáváme rozvoj sektoru MSP.

Častým problémem jsou však i **nedostatečné zdroje** na rozsáhlejší digitalizaci, začíná se projevovat současný **propad ekonomiky**, zvláště v sektoru B2B, který rozhodně inflační a vstupový tlak nepromítl do cen.

D3. Jakým výzvám čelila vaše společnost během procesu digitalizace?
N=202/124/78/83/45/74

NEJVÍCE NÁPOMOCNÉ V PROCESU DIGITALIZACE JE ŠKOLENÍ NEBO VZDĚLÁVÁNÍ ZAMĚSTNANCŮ, UVÁDÍ TO VÍCE NEŽ POLOVINA FIREM.

Podpora či zdroje nejvíce nápomocné v procesu digitalizace (v %)



	Firma s 4 až 49 zaměstnanci	Firma s 50 až 249 zaměstnanci	Výroba, průmysl	Obchod	Služby
Školení nebo vzdělávání zaměstnanců	54	49	52	44	57
Přístup k digitálním řešením nebo platformám specifickým pro dané odvětví	34	51	42	31	45
Dotace (finanční) podpora určená pro digitalizaci	41	37	39	38	42
Možnosti navazování kontaktů nebo spolupráce s jinými podniky	19	28	31	24	11
Nevím (bez odpovědi)	6	1	4	7	3

Komentář AMSP ČR:

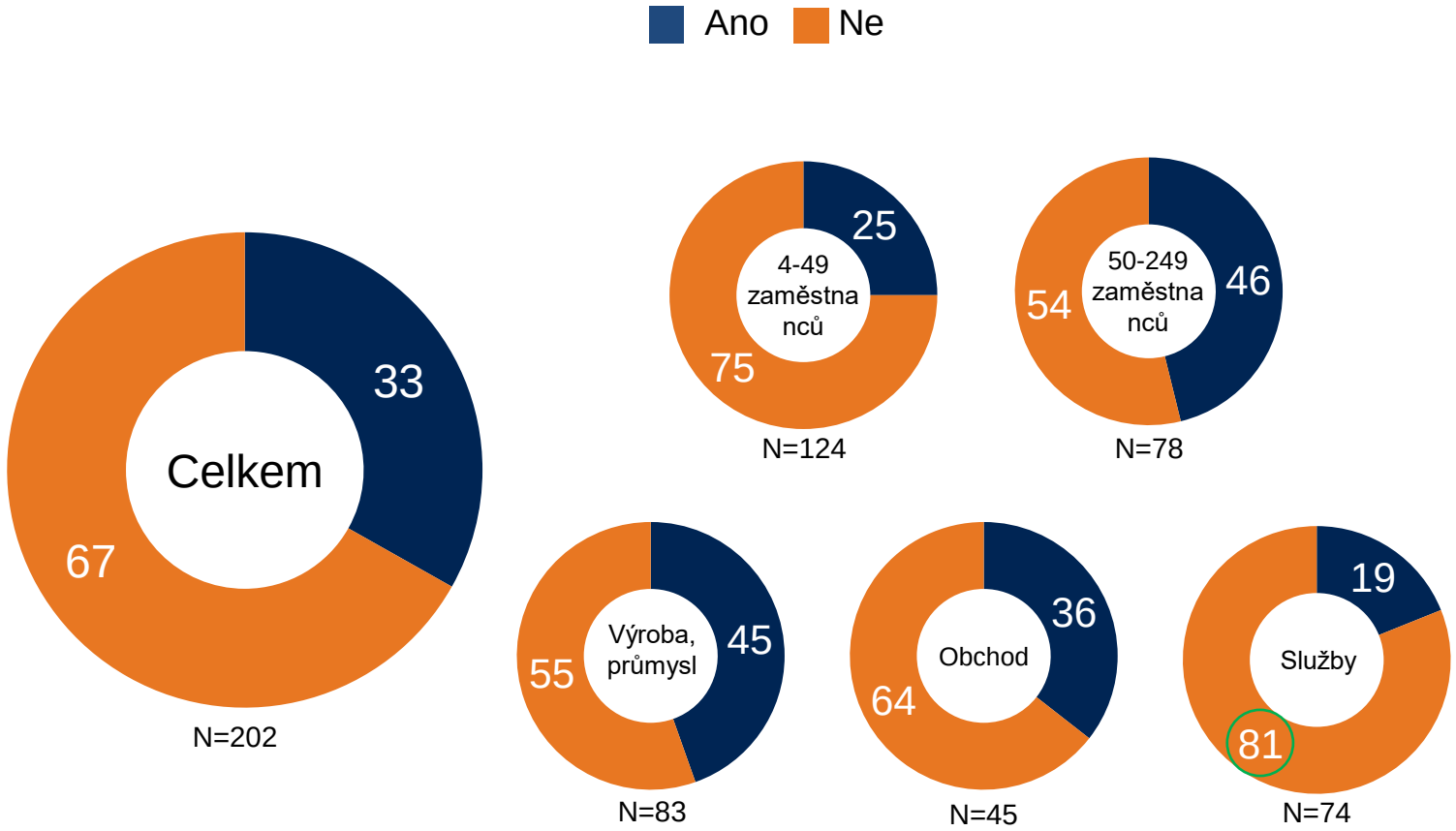
V návaznosti na předchozí komentář ohledně potíží s outsourcingem některých služeb (např. digitalizačních) se firmy snaží vzdělat vlastní lidské zdroje v potřebných oblastech, proto se zde v průzkumu projevuje silně důraz na školení a vzdělávání zaměstnanců.

Za nápomocné firmy stále považují i dotační podporu.

D4. Jaká podpora nebo zdroje by podle vás vaší společnosti nejvíce pomohly v procesu digitalizace?
N=202/124/78/83/45/74

TŘETINA FIREM MÁ URČENÝ PLÁN DIGITÁLNÍ TRANSFORMACE. FIRMY ZE SEKTORU SLUŽEB MAJÍ TENTO PLÁN MÉNĚ ČASTO.

Má Vaše společnost určený nějaký plán digitální transformace? (v %)



Komentář AMSP ČR:

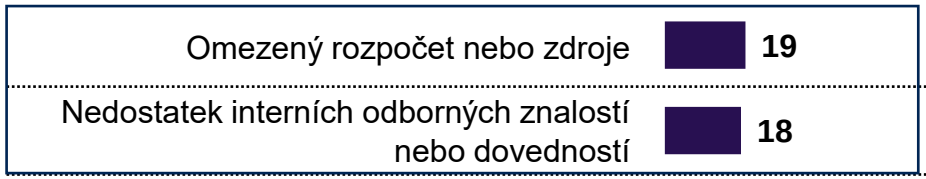
Dvě třetiny českých firem nemají plán digitální transformace. V sektoru služeb pak až 80 % podniků tento plán nemá. Z průzkumu vyplývá, že nejvíce s tímto plánem digitalizace pracují výrobní firmy. Je to asi přirozené. Výroba je ze zkoumaných sektorů asi nejkomplexnější obor a digitální nástroje tyto firmy mohou zavádět v mnoha stupních předvýrobního, výrobního, prodejního a servisního procesu.

D5. Má vaše společnost určený nějaký plán digitální transformace?

Statisticky signifikantní

FIRMY PŘI ZAVÁDĚNÍ AI NEBO AUTOMATIZACE SE NEJČASTĚJI POTÝKAJÍ S OMEZENÝM ROZPOČTEM ČI ZDROJI A NEDOSTATKEM INTERNÍCH ZNALOSTÍ.

Výzvy, kterým firmy čelí při zavádění technologií AI nebo automatizace (v %)



	Firma s 4 až 49 zaměstnanci	Firma s 50 až 249 zaměstnanci	Výroba, průmysl	Obchod	Služby
Omezený rozpočet nebo zdroje	19	19	22	16	18
Nedostatek interních odborných znalostí nebo dovedností	19	15	14	22	19
Obavy o soukromí a bezpečnost dat	18	12	12	22	15
Integrace se stávajícími systémy nebo procesy	12	19	17	16	12
Nejistota ohledně návratnosti investic (ROI)	10	9	8	9	11
Etické nebo právní aspekty	4	10	8	7	4
Jiné, vypište	4	1	4	4	1
Není pro mé podnikání relevantní	15	14	14	4	20

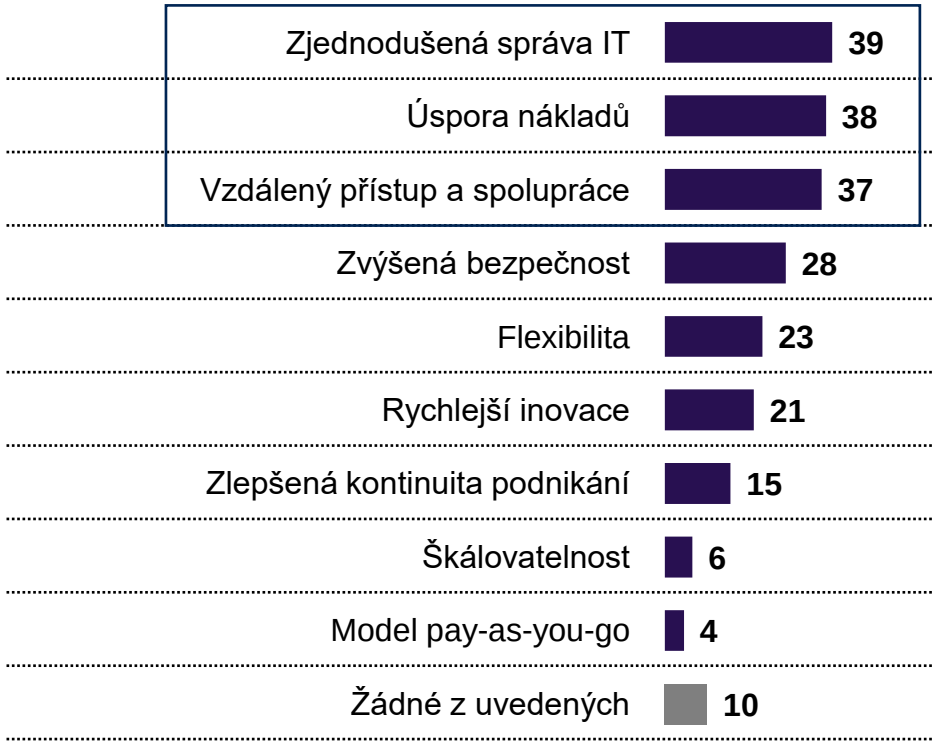
Komentář AMSP ČR:

Opakovaně se v průzkumech ukazuje **nedostatek zdrojů – zejména z oblasti specializovaných znalostí**. Pro MSP je typické outsourcovat například zavádění nových technologií (AI nebo automatizace), přičemž si pak již zpravidla dokáží „vychovat“ interní obsluhu. Při zavádění se ale potýkají s tím, že **dodavatelé těchto služeb dávají přednost větším zakázkám korporátů**, a tak **technologický či digitální rozvoj v MSP není možné realizovat tempem, na které již velká část MSP je dávno připravená**.

D6. Jakým výzvám nebo překážkám čelí vaše společnost při zavádění technologií AI nebo automatizace?
N=202/124/78/83/45/74

CLOUD COMPUTING MŮŽE DLE FIREM PŘINÉST ZJEDNODUŠENOU SPRÁVU IT, ÚSPORU NÁKLADŮ A TAKÉ VZDÁLENÝ PŘÍSTUP ČI SPOLUPRÁCI.

Výhody, které může přinést cloud computing (v %)



	Firma s 4 až 49 zaměstnanci	Firma s 50 až 249 zaměstnanci	Výroba, průmysl	Obchod	Služby
Zjednodušená správa IT	40	38	41	44	34
Úspora nákladů	35	42	37	31	42
Vzdálený přístup a spolupráce	38	35	36	29	42
Zvýšená bezpečnost	24	35	28	22	32
Flexibilita	18	31	20	29	22
Rychlejší inovace	20	22	20	27	18
Zlepšená kontinuita podnikání	15	17	24	11	8
Škálovatelnost	6	8	12	4	1
Model pay-as-you-go	4	5	5	4	4
Žádné z uvedených	11	8	10	11	9

Komentář AMSP ČR:

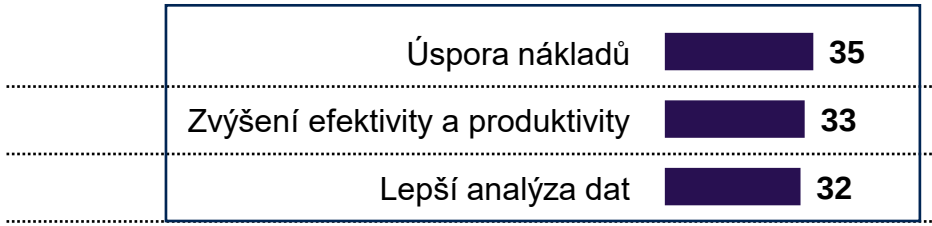
Co se týká CLOUDOVÝCH ŘEŠENÍ, část firem má zato, že může přinést zjednodušení správy IT, případně uspořit náklady, a rovněž umožnit vzdálený přístup.

Naopak jen asi čtvrtina firem (28 %) považuje CLOUD ZA BEZPEČNÝ. I to může být důvod, proč určitá část firem spoléhá spíše na vlastní serverové řešení a ke cloudu neinklinuje.

D7. Jaké výhody si myslíte, že cloud computing může přinést vaší organizaci?
N=202/124/78/83/45/74

FIRMY UDÁVAJÍ, ŽE AI MŮŽE PŘINÉST PRIMÁRNĚ ÚSPORU NÁKLADŮ, ZVÝŠENÍ EFEKTIVITY ČI PRODUKTIVITY A TAKÉ LEPŠÍ ANALÝZU DAT.

Výhody, které může přinést umělá inteligence (AI) (v %)



	Firma s 4 až 49 zaměstnanci	Firma s 50 až 249 zaměstnanci	Výroba, průmysl	Obchod	Služby
Úspora nákladů	35	35	33	33	38
Zvýšení efektivity a produktivity	31	36	34	33	31
Lepší analýza dat	28	37	27	36	35
Lepší rozhodování	23	32	34	20	22
Inovace produktů a služeb	25	15	18	18	27
Konkurenční výhoda	23	19	20	20	23
Zefektivnění obchodních procesů	18	19	17	22	18
Lepší zákaznická zkušenost	16	19	20	18	14
Lepší spolupráce zaměstnanců	14	17	18	18	9
Efektivnější řízení rizik	13	17	16	18	11
Žádné z uvedených	15	9	12	13	14

Komentář AMSP ČR:

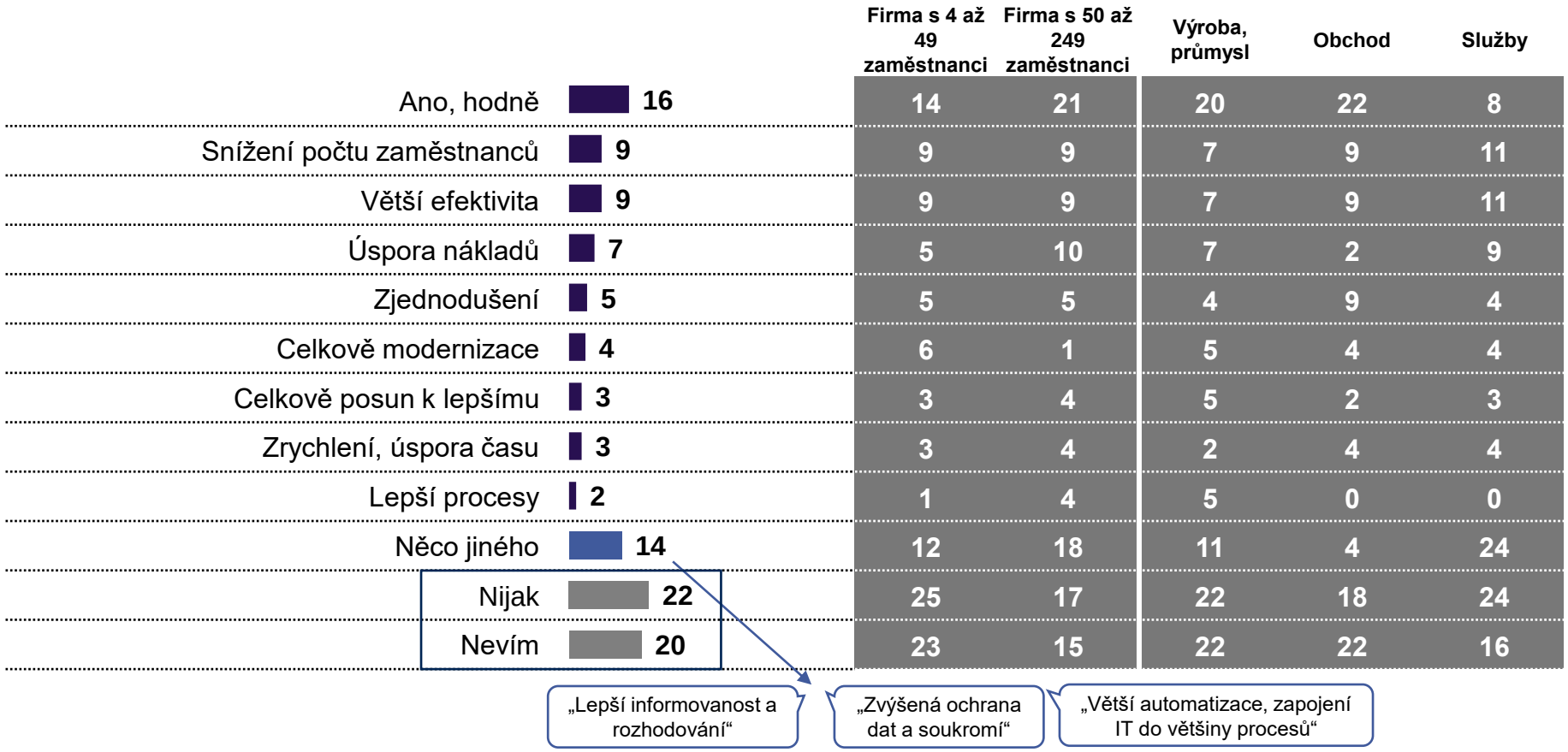
Třetina firem napříč velikostním spektrem považuje AI za zdroj úspory nákladů, zvýšení efektivity a produktivity, případně se domnívá, že jim může dopomoci k lepší analýze získaných dat.

Zajímavé je, že užitečnost AI z hlediska datové analýzy považuje za přínos jen 27 % výrobních firem.

D8. Jaké výhody může podle vás umělá inteligence (AI) přinést vaší organizaci?
N=202/124/78/83/45/74

6 Z 10 FIREM OČEKÁVÁ VLIV AI A CLOUD COMPUTINGU NA JEJICH ODVĚTVÍ. OSTATNÍ UDÁVAJÍ, ŽE JE TYTO TECHNOLOGIE NEOVLIVNÍ, NEBO NEVÍ.

Jak ovlivní AI a cloud computing společnosti v příštích 5-10 letech? (v %)



	Firma s 4 až 49 zaměstnanci	Firma s 50 až 249 zaměstnanci	Výroba, průmysl	Obchod	Služby
Ano, hodně	14	21	20	22	8
Snížení počtu zaměstnanců	9	9	7	9	11
Větší efektivita	9	9	7	9	11
Úspora nákladů	5	10	7	2	9
Zjednodušení	5	5	4	9	4
Celkově modernizace	6	1	5	4	4
Celkově posun k lepšímu	3	4	5	2	3
Zrychlení, úspora času	3	4	2	4	4
Lepší procesy	1	4	5	0	0
Něco jiného	12	18	11	4	24
Nijak	25	17	22	18	24
Nevím	23	15	22	22	16

„Lepší informovanost a rozhodování“

„Zvýšená ochrana dat a soukromí“

„Větší automatizace, zapojení IT do většiny procesů“

Komentář AMSP ČR:

Jen 16 % firem ze sektoru MSP očekává větší vliv AI a CLOUD computingu na jejich odvětví, naopak více než pětina firem žádný výraznější vliv neočekává.

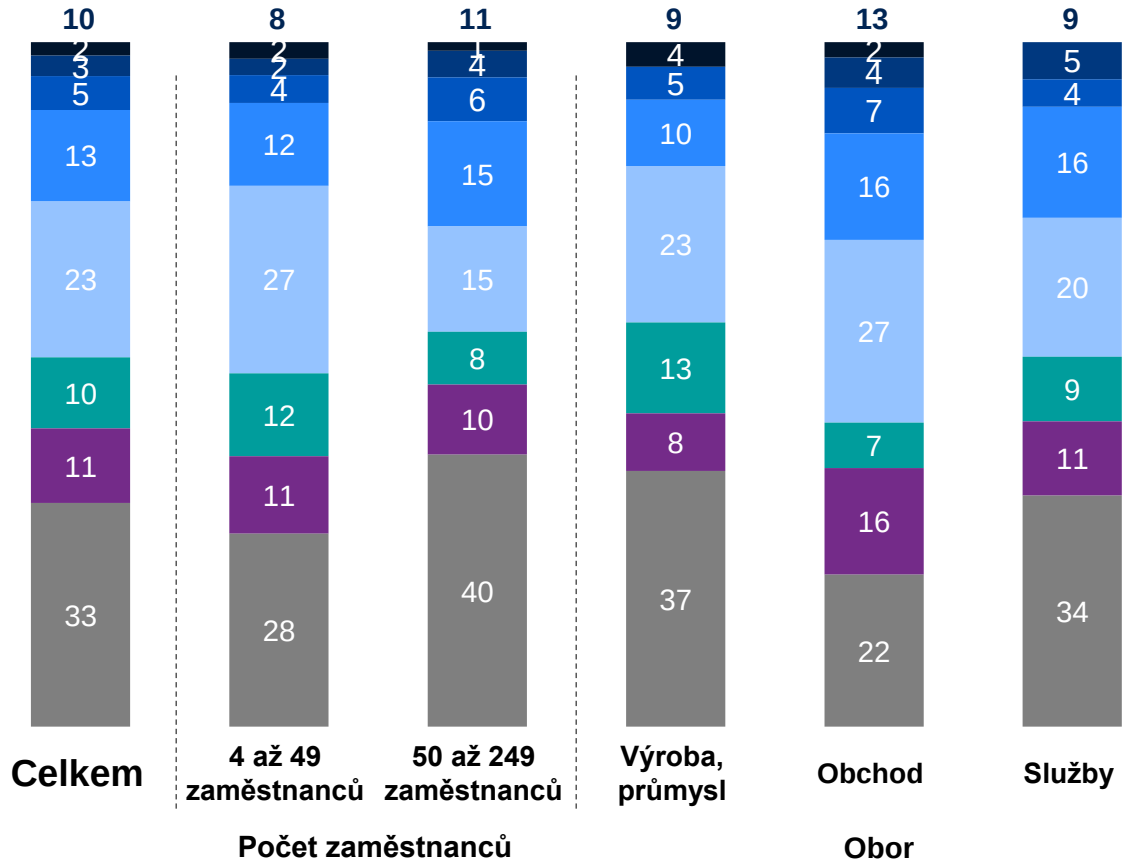
Větší efektivitu a snížení potřeby zaměstnávání lidí si slibuje pouhých 9 % firem.

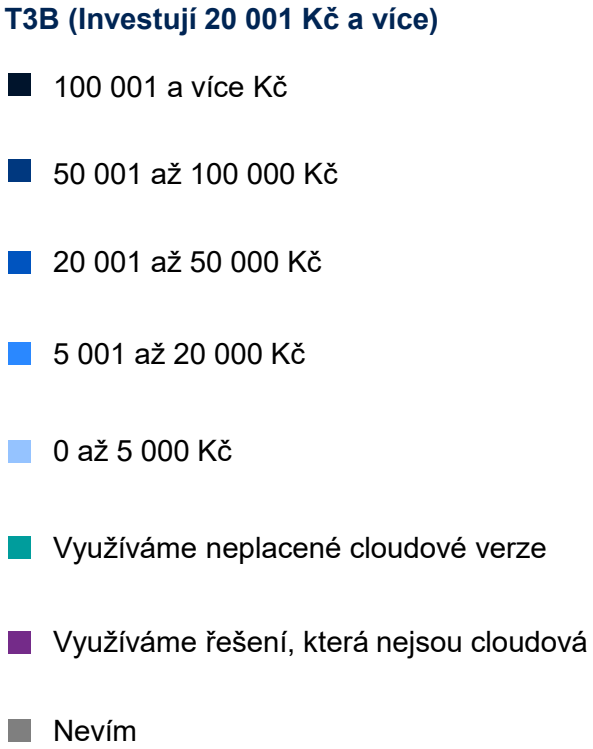
Vliv na tyto výsledky mohou mít zatím nepříliš jasné obrysy dopadů AI do většiny běžných podnikatelských oborů, respektive tato perspektiva může být vnímána jako relativně vzdálená.

D9. Jak podle vás ovlivní technologie umělé inteligence a cloud computingu odvětví vaší společnosti v příštích 5-10 letech?
N=202/124/78/83/45/74

POUZE 1 Z 10 FIREM INVESTUJE DO KANCELÁŘSKÝCH BALÍČKŮ FUNGUJÍCÍCH V CLOUDU 20 001 KČ MĚSÍČNĚ A VÍCE. TŘETINA PŘESNĚ NEVÍ, KOLIK INVESTUJE.

Kolik měsíčně jako firma investujete do kancelářských balíčků, které fungují v cloudu? (v %)





Komentář AMSP ČR:

Firmy mnohdy nerozlišují mezi používanými softwary či službami, které jsou na bázi cloudu nebo například na bázi dodávaného softwarového řešení (například sklad, finance, CRM apod.), proto může být obtížné v okamžitém respondentském interview přesně stanovit částku.

Obecně ale tento slide dokresluje situaci nastíněnou na jednom z těch předchozích, tj. že část firem spoléhá spíše na vlastní serverové řešení (i v oblasti kancelářských aplikací/softwarů) a ke cloudu inklinuje jen v určitých případech.

D9b. Kolik měsíčně jako firma investujete (platíte) do kancelářských balíčků, které fungují v cloudu? Uveďte odpověď v korunách.
N=202/124/78/83/45/74

FIRMY PRŮMĚRNĚ INVESTUJÍ DO KANCELÁŘSKÝCH BALÍČKŮ V CLOUDU 16 122 KČ.

Kolik firmy měsíčně investují do kancelářských balíčků fungujících v cloudu? (v %)

(Pouze dotazovaní, kteří uvedli, že do těchto balíčků investují)

Celkem

Průměr: 16 122,- Kč

4-49 zaměstnanců

Průměr: 14 251,- Kč

50-249 zaměstnanců

Průměr: 19 665,- Kč

Výroba, průmysl

Průměr: 17 721,- Kč

Obchod

Průměr: 18 280,- Kč

Služby

Průměr: 12 885,- Kč

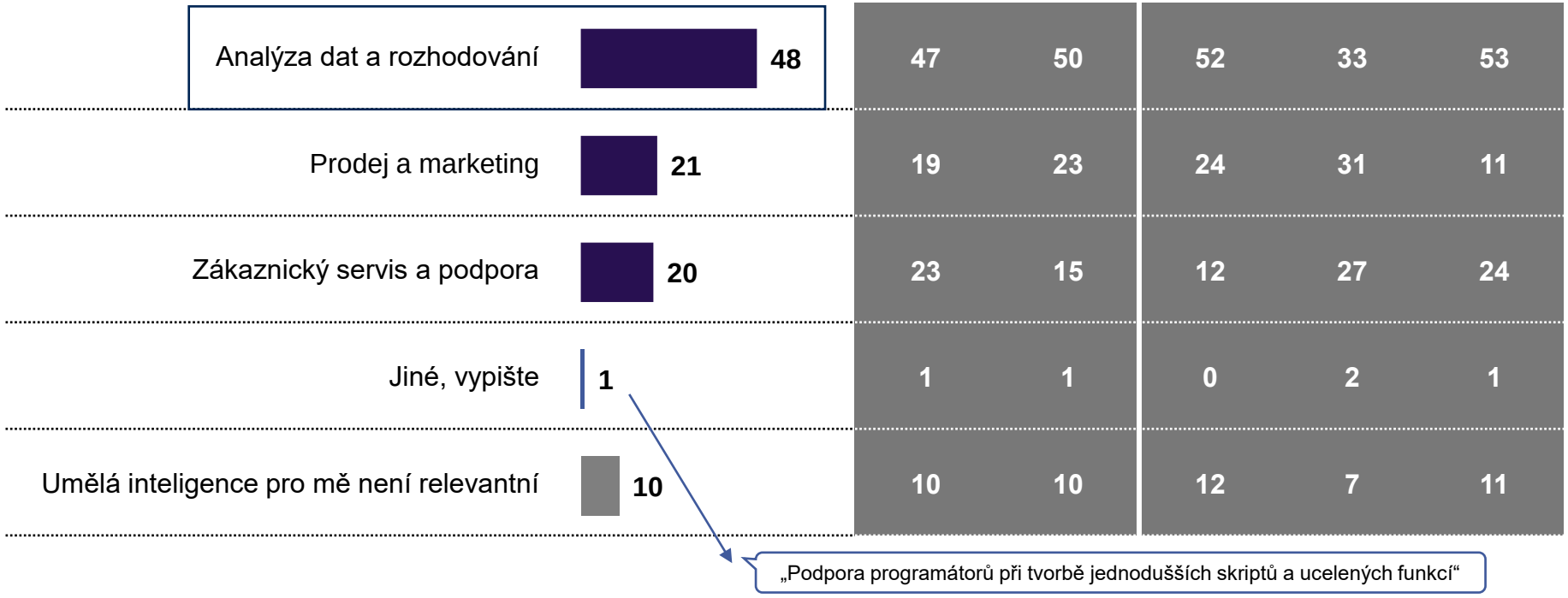
Komentář AMSP ČR:

Firmy, které byly schopny zodpovědět dotaz na investice do kancelářských balíčků v cloudu, uvádějí v průměru částku 16 tisíc Kč. Podle očekávání je to o něco více u firem větších v rámci segmentu MSP. Oborově je to přibližně stejná částka u obchodu a výroby, zatímco u služeb se jeví být o třetinu nižší.

D9b. Kolik měsíčně jako firma investujete (platíte) do kancelářských balíčků, které fungují v cloudu? Uveďte odpověď v korunách.
N=136/89/47/52/35/49

TÉMĚŘ POLOVINA FIREM UDÁVÁ, ŽE UMĚLÁ INTELIGENCE MÁ NEJVĚTŠÍ POTENCIÁL V OBLASTI ANALÝZY DAT A ROZHODOVÁNÍ.

Oblasti, ve kterých má umělá inteligence (AI) největší potenciál (v %)



	Firma s 4 až 49 zaměstnanci	Firma s 50 až 249 zaměstnanci	Výroba, průmysl	Obchod	Služby
Analýza dat a rozhodování	47	50	52	33	53
Prodej a marketing	19	23	24	31	11
Zákaznický servis a podpora	23	15	12	27	24
Jiné, vypište	1	1	0	2	1
Umělá inteligence pro mě není relevantní	10	10	12	7	11

Komentář AMSP ČR:

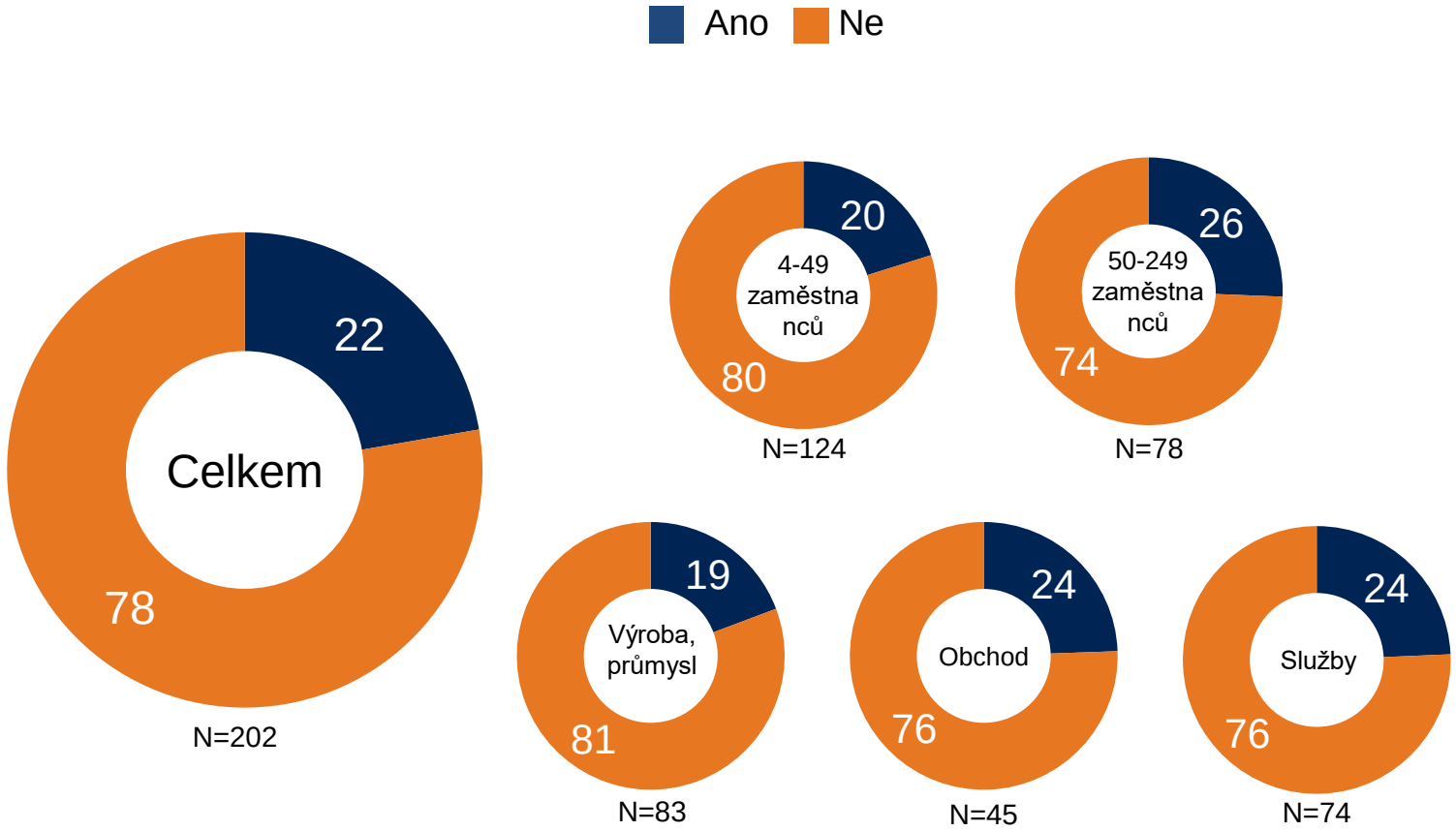
Na dotaz, v jakých činnostech vidí firmy největší potenciál využití AI, téměř polovina uvádí oblast ANALÝZY DAT A ROZHODOVÁNÍ (48 %), což jsou zásadně interní procesy.

Naopak jen kolem 20 % firem vidí potenciál procesech typu prodej, marketing či zákaznická podpora.

D10. Ve kterých oblastech vašeho podnikání si myslíte, že má umělá inteligence největší potenciál?
N=202/124/78/83/45/74

PŘIBLIŽNĚ ČTVRTINA FIREM PŘIZNÁVÁ URČITÉ POTÍŽE BĚHEM PROCESU DIGITALIZACE.

Zažila vaše společnost během procesu digitalizace nějaké neúspěchy nebo selhání? (v %)



Komentář AMSP ČR:

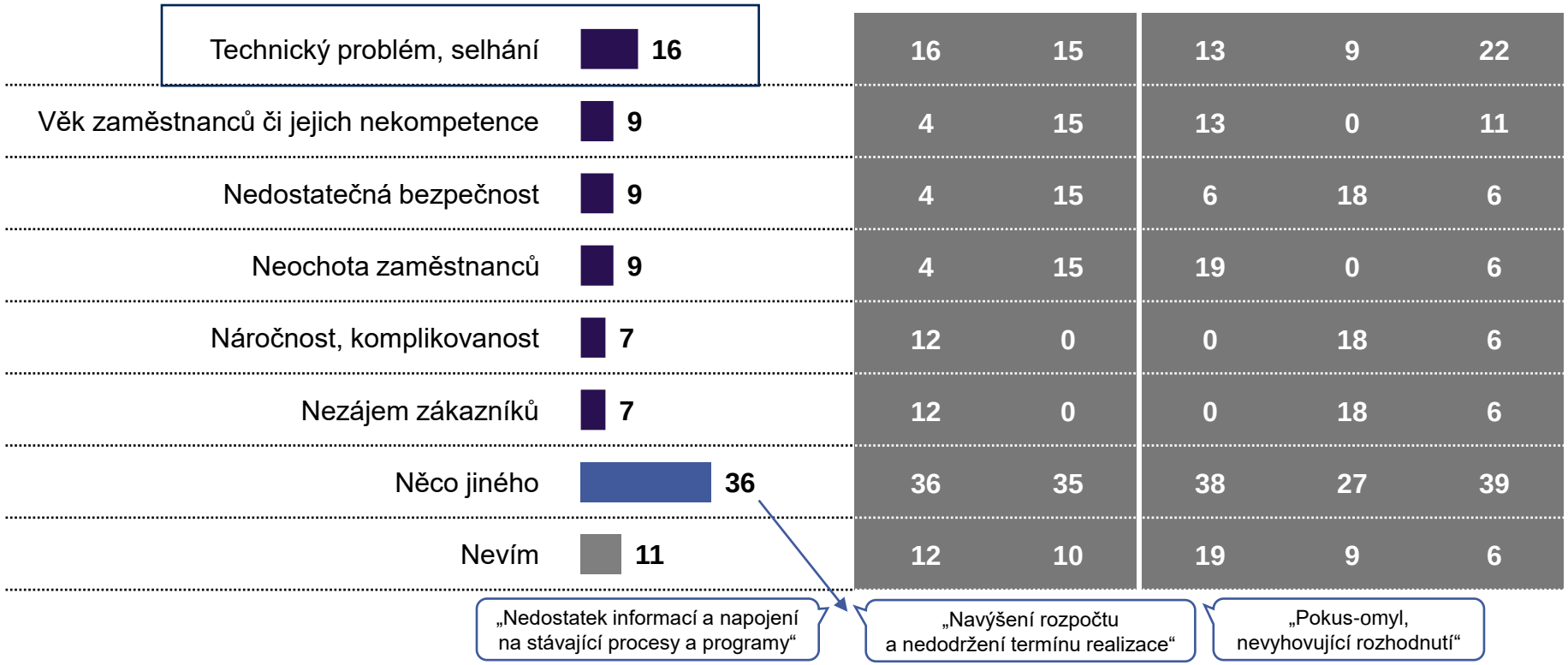
V průběhu implementace digitalizace do stávajících procesů není neobvyklé čelit dílčím neúspěchům, jak ukazuje náš průzkum. Více obvyklé je to v případě větších firem segmentu MSP (tj. 50-249 zaměstnanců), 26 %. To není překvapivé, protože čím větší je firma, tím rozsáhlejší a různě provázané procesy tam obvykle probíhají. Jinak jsou ale respondenti s provedenou digitalizací veskrze spokojeni.

D11. Zažila vaše společnost během procesu digitalizace nějaké neúspěchy nebo selhání?

FIRMY V PRŮBĚHU DIGITALIZACE ZAŽÍVALY ROZLIČNÉ POTÍŽE. V PŘÍPADĚ 16 % Z NICH SE JEDNALO O TECHNICKÝ PROBLÉM ČI SELHÁNÍ.

Povaha daného neúspěchu či selhání (v %)

(Pouze dotazovaní, kteří uvedli, že během průběhu digitalizace zažily jisté neúspěchy či selhání)



	Firma s 4 až 49 zaměstnanci	Firma s 50 až 249 zaměstnanci	Výroba, průmysl	Obchod	Služby
Technický problém, selhání	16	15	13	9	22
Věk zaměstnanců či jejich nekompetence	4	15	13	0	11
Nedostatečná bezpečnost	4	15	6	18	6
Neochota zaměstnanců	4	15	19	0	6
Náročnost, komplikovanost	12	0	0	18	6
Nezájem zákazníků	12	0	0	18	6
Něco jiného	36	35	38	27	39
Nevím	12	10	19	9	6

Komentář AMSP ČR:

Co se týká zmíněných překážek při implementaci digitalizace do firmy, zpravidla se jednalo o technický zádrhel a kompatibilitu jednotlivých systémů. Nelze totiž očekávat, že firma, která působí na trhu, zaměstnává zaměstnance, je digitálně nedotčena. Další digitalizační upgrady či změny a implementace tak musí být v souladu se systémy stávajícími / nebo je nutné zajistit hladký přechod na systém nový.

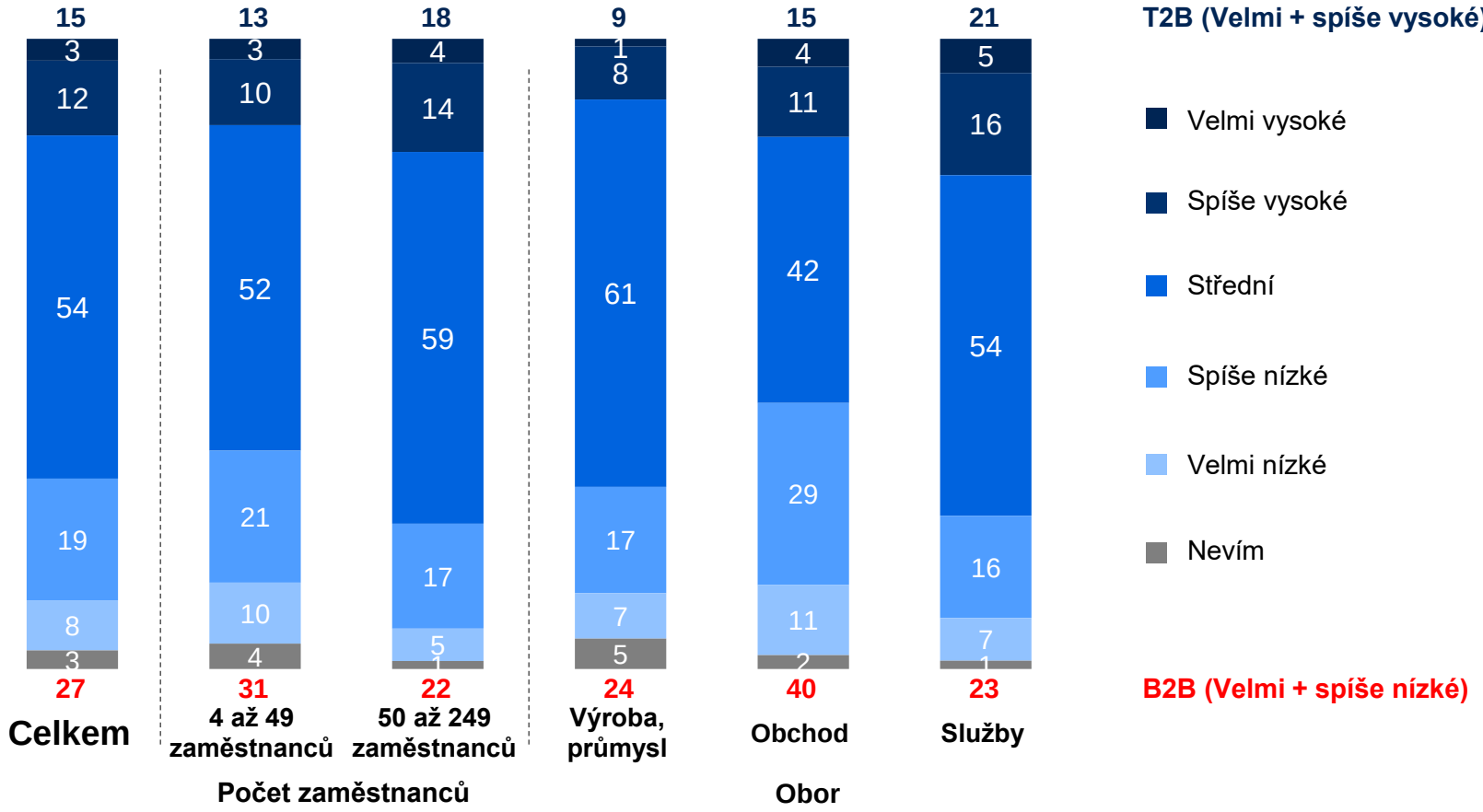
Kromě technického zádrhele však firmy čelily například i navýšení rozpočtu či nedodržení termínu realizace a fungování – to je pro firmy vždy tíživé.

D12. Popište prosím stručně povahu neúspěchu (neúspěchů) nebo selhání.
N=45/25!/20!/16!/11!/18!

! = Pozor! Nízká báze

VÍCE NEŽ POLOVINA FIREM HODNOTÍ ÚROVEŇ POVĚDOMÍ O KYBERNETICKÉ BEZPEČNOSTI VE SVÉ FIRMĚ JAKO STŘEDNÍ (PRŮMĚRNÉ).

Hodnocení povědomí o kybernetické bezpečnosti v dané společnosti (v %)

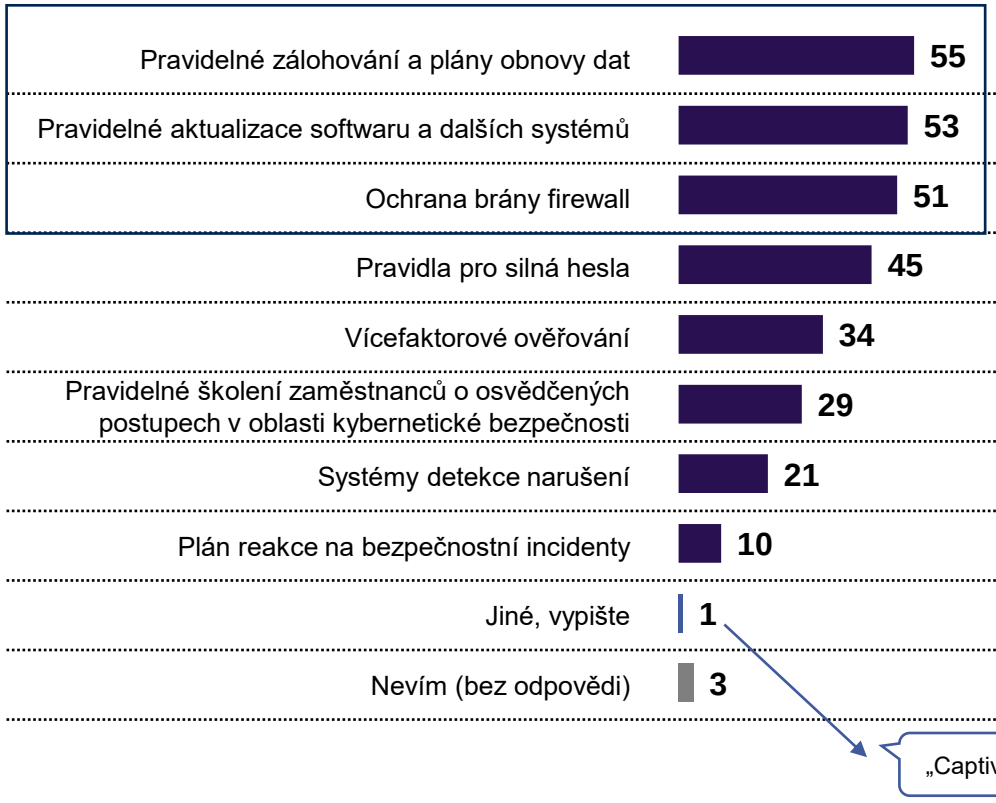


Komentář AMSP ČR:
Kybernetické riziko si firmy uvědomují, řada z nich již kyber-útokům také čelila. Nejvýše své povědomí o kybernetické bezpečnosti hodnotí větší firmy segmentu MSP.

K1. Jak hodnotíte celkovou úroveň povědomí o kybernetické bezpečnosti ve vaší společnosti?
N=202/124/78/83/45/74

POLOVINA FIREM MÁ ZAVEDENO PRAVIDELNÉ ZÁLOHOVÁNÍ A PLÁNY OBNOVY DAT, PRAVIDELNOU AKTUALIZACI SOFTWARU A OCHRANU BRÁNY FIREWALL.

Současná zavedená opatření kybernetické bezpečnosti (v %)



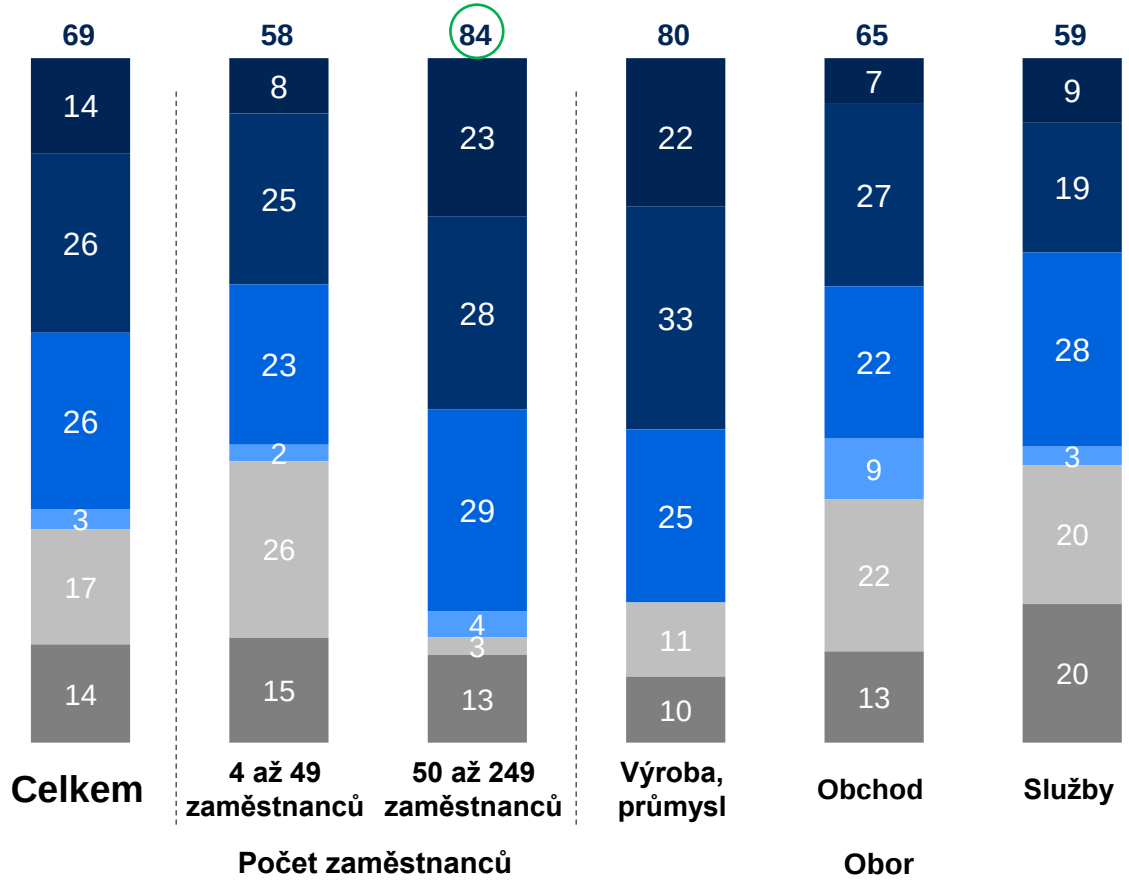
	Firma s 4 až 49 zaměstnanci	Firma s 50 až 249 zaměstnanci	Výroba, průmysl	Obchod	Služby
Pravidelné zálohování a plány obnovy dat	52	59	48	53	64
Pravidelné aktualizace softwaru a dalších systémů	51	58	48	49	62
Ochrana brány firewall	48	56	51	53	50
Pravidla pro silná hesla	46	44	40	38	55
Vícefaktorové ověřování	31	38	35	36	31
Pravidelné školení zaměstnanců o osvědčených postupech v oblasti kybernetické bezpečnosti	26	33	22	40	30
Systémy detekce narušení	13	33	30	13	15
Plán reakce na bezpečnostní incidenty	8	13	13	7	8
Jiné, vypište	1	1	1	0	1
Nevím (bez odpovědi)	5	1	6	4	0

Komentář AMSP ČR:
Na druhé straně jen o něco více než polovina firem systematicky ZÁLOHUJE svá data (55 %).Tam je jistě prostor pro zlepšení. Následují pravidelné aktualizace softwarů a dalších systémů (53 %).

K4. Která z následujících opatření kybernetické bezpečnosti má vaše společnost v současné době zavedena?
N=202/124/78/83/45/74

40 % FIREM PROVÁDÍ HODNOCENÍ RIZIK KYBERNETICKÉ BEZPEČNOSTI NEJMÉNĚ JEDNOU ZA ČTVRT ROKU.

Jak často Vaše společnost provádí hodnocení rizik kybernetické bezpečnosti? (v %)



Komentář AMSP ČR:

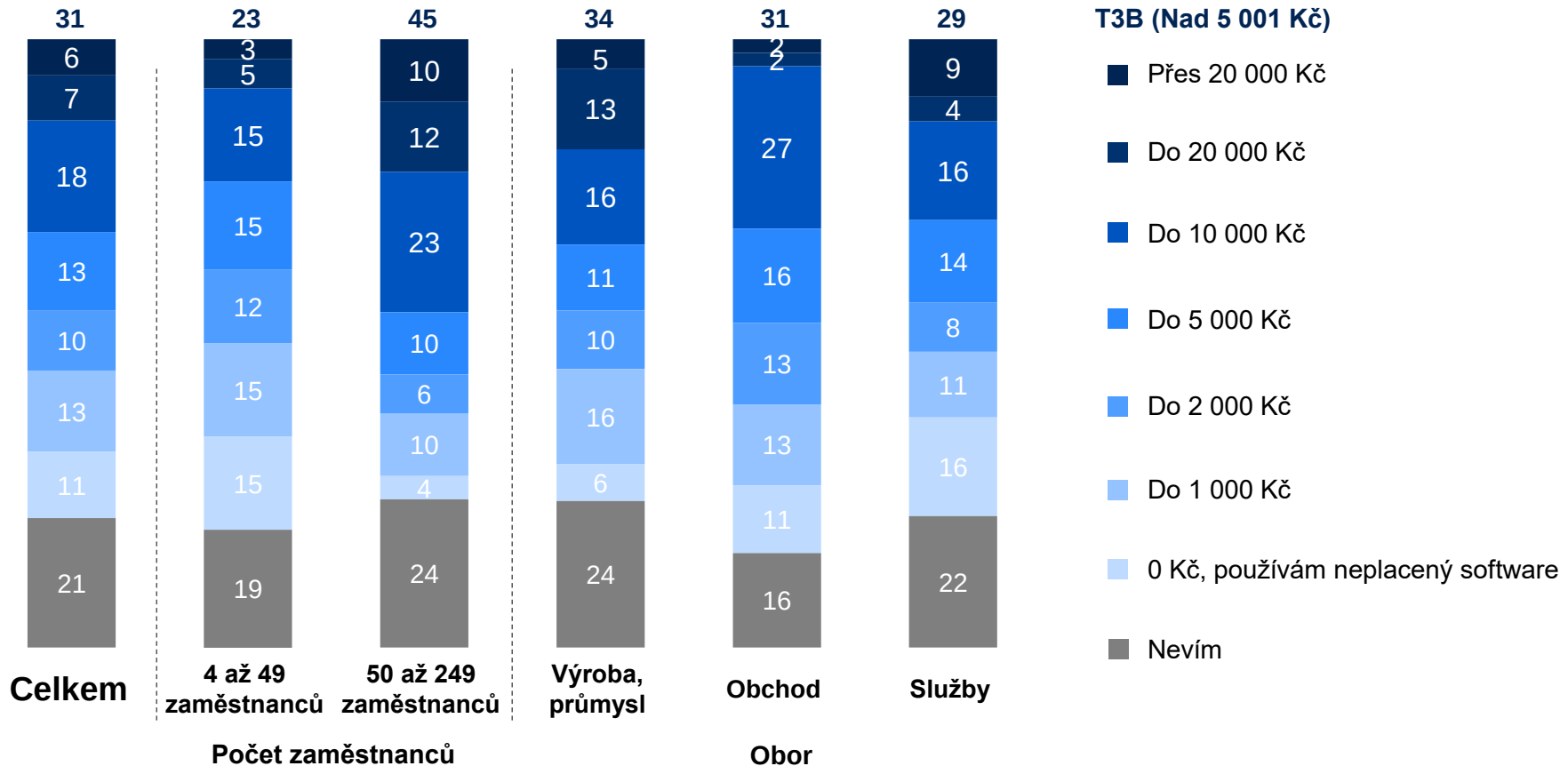
Hodnocení rizik kybernetické bezpečnosti minimálně jednou za kvartál provádí zhruba 40 % firem. Stejně jako hodnocení ostatních rizik podléhá i toto riziko rovněž mezinárodnímu management systému ISO, kde je popsání a hodnocení rizik povinné. Velmi typicky tak proto větší firmy segmentu MSP (50-249 zaměstnanců) vykazují opravdu vysokou míru hodnocení kyber-rizika (84 %), nejvíce pak v oblasti výroby a průmyslu, kde jsou systémy managementu na bázi ISO poměrně běžné. Nejméně běžné je toto hodnocení ve službovém sektoru (28 %), jak vyplývá z průzkumu.

K5. Jak často vaše společnost provádí hodnocení rizik kybernetické bezpečnosti?
N=202/124/78/83/45/74

Statisticky signifikantní

PĚTINA FIREM NEVÍ, KOLIK MĚSÍČNĚ INVESTUJE DO IT BEZPEČNOSTNÍCH TECHNOLOGIÍ, TŘETINA INVESTUJE NAD 5 001 KČ.

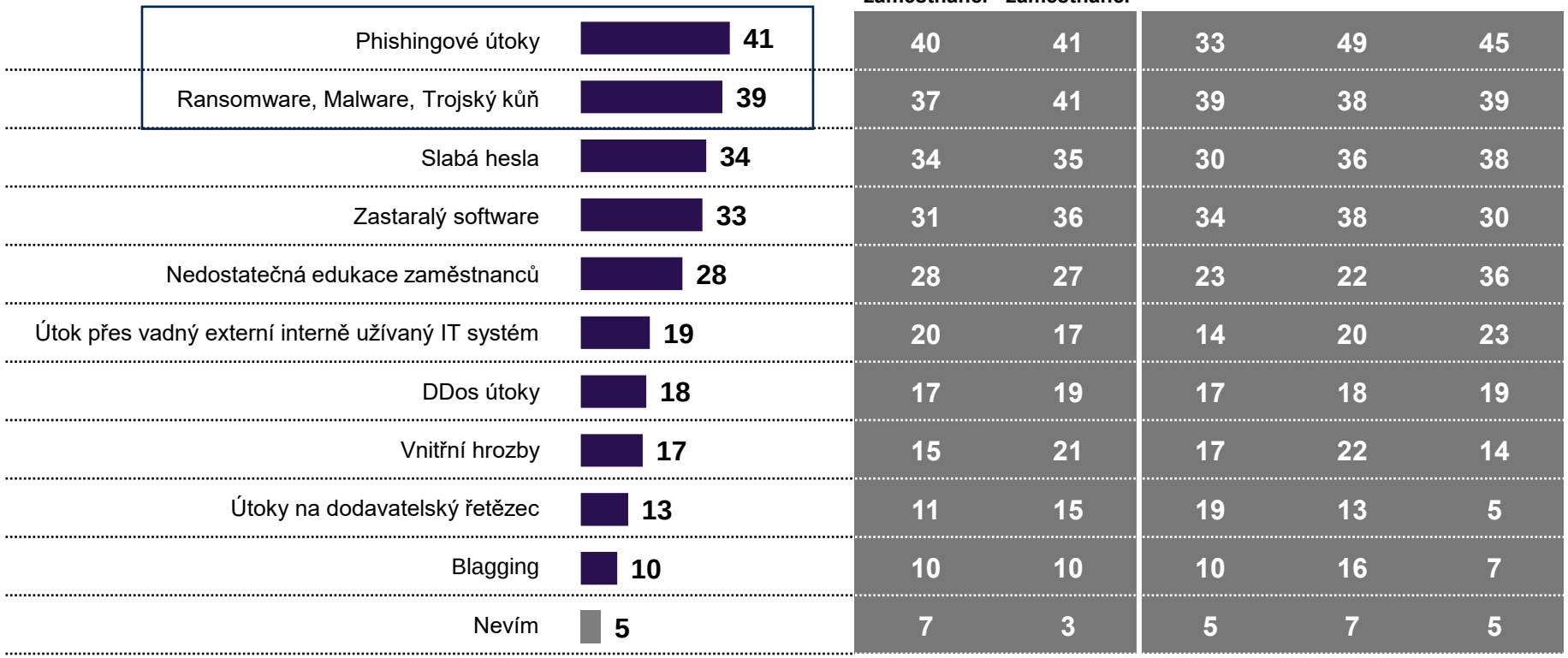
Kolik měsíčně investujete do IT bezpečnostních technologií? (v %)



K6. Kolik měsíčně investujete do IT bezpečnostních technologií?
N=202/124/78/83/45/74

PODNIKY VNÍMAJÍ JAKO NEJVĚTŠÍ HROZBU V RÁMCI KYBERNETICKÝCH ÚTOKŮ PHISHINGOVÉ ÚTOKY A RANSOMWARE ČI MALWARE.

Největší hrozby kybernetické bezpečnosti pro firmy (v %)



	Firma s 4 až 49 zaměstnanci	Firma s 50 až 249 zaměstnanci	Výroba, průmysl	Obchod	Služby
Phishingové útoky	40	41	33	49	45
Ransomware, Malware, Trojský kůň	37	41	39	38	39
Slabá hesla	34	35	30	36	38
Zastaralý software	31	36	34	38	30
Nedostatečná edukace zaměstnanců	28	27	23	22	36
Útok přes vadný externí interně užívaný IT systém	20	17	14	20	23
DDos útoky	17	19	17	18	19
Vnitřní hrozby	15	21	17	22	14
Útoky na dodavatelský řetězec	11	15	19	13	5
Blagging	10	10	10	16	7
Nevím	7	3	5	7	5

Komentář AMSP ČR:

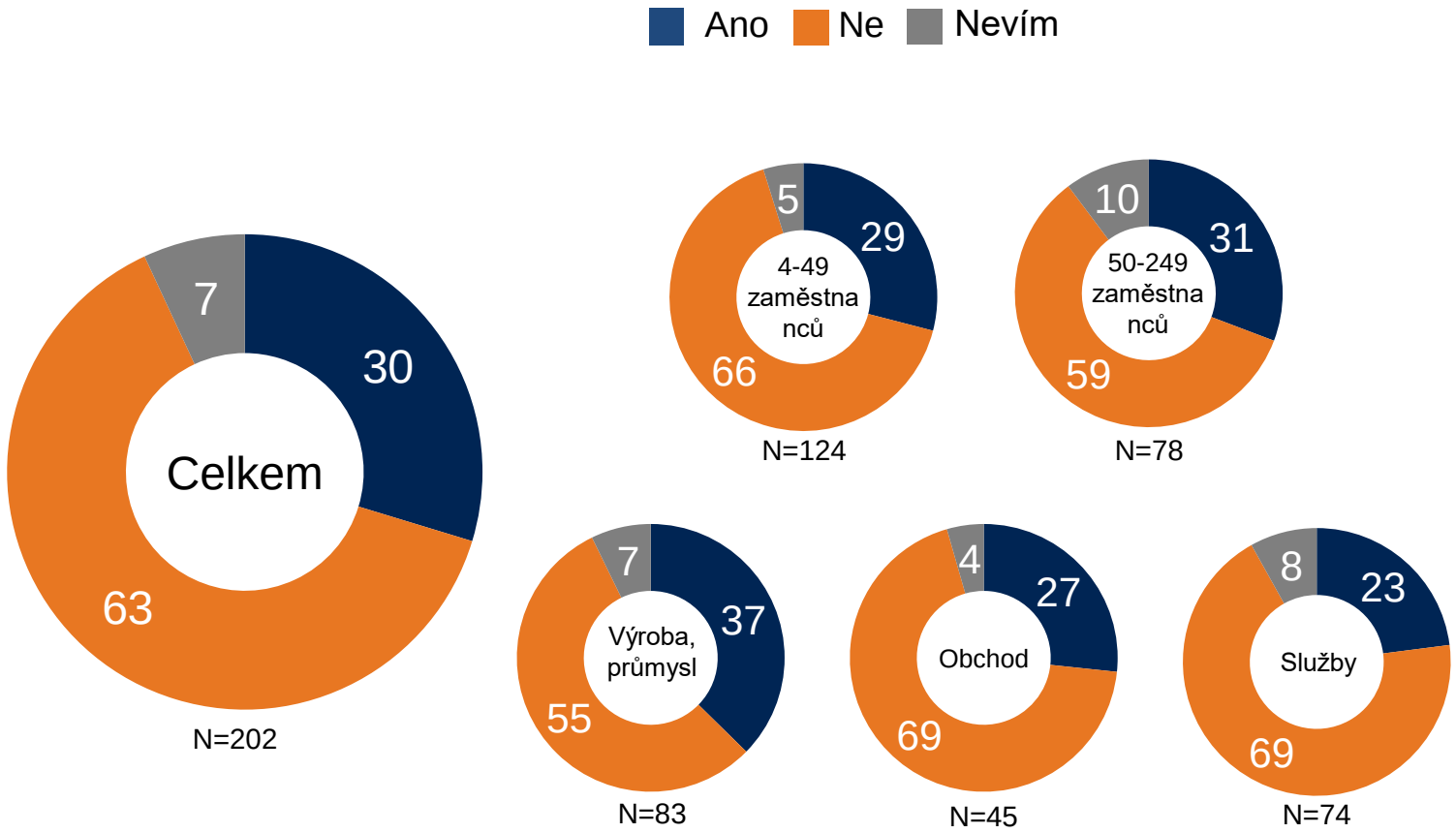
Nejčastěji se firmy setkávají s kybernetickým pirátstvím v oblasti PHISHINGU, RANSOMWARE či MALWARE apod.

Jako hrozbu firmy MSP vnímají též poměrně SLABÁ HESLA, ale také zmiňují nedostatečnou edukaci lidského faktoru, který bývá obecně nejslabším článkem v celém procesu kybernetické bezpečnosti.

K7. Co považujete za největší hrozby kybernetické bezpečnosti pro vaši firmu?
N=202/124/78/83/45/74

DVĚ TŘETINY FIREM NIKDY NEVYHLEDALY EXTERNÍ POMOC ZA ÚČELEM ZLEPŠENÍ SVÉ KYBERNETICKÉ BEZPEČNOSTI.

Vyhledala společnost někdy externí pomoc za účelem zlepšení své kybernetické bezpečnosti? (v %)



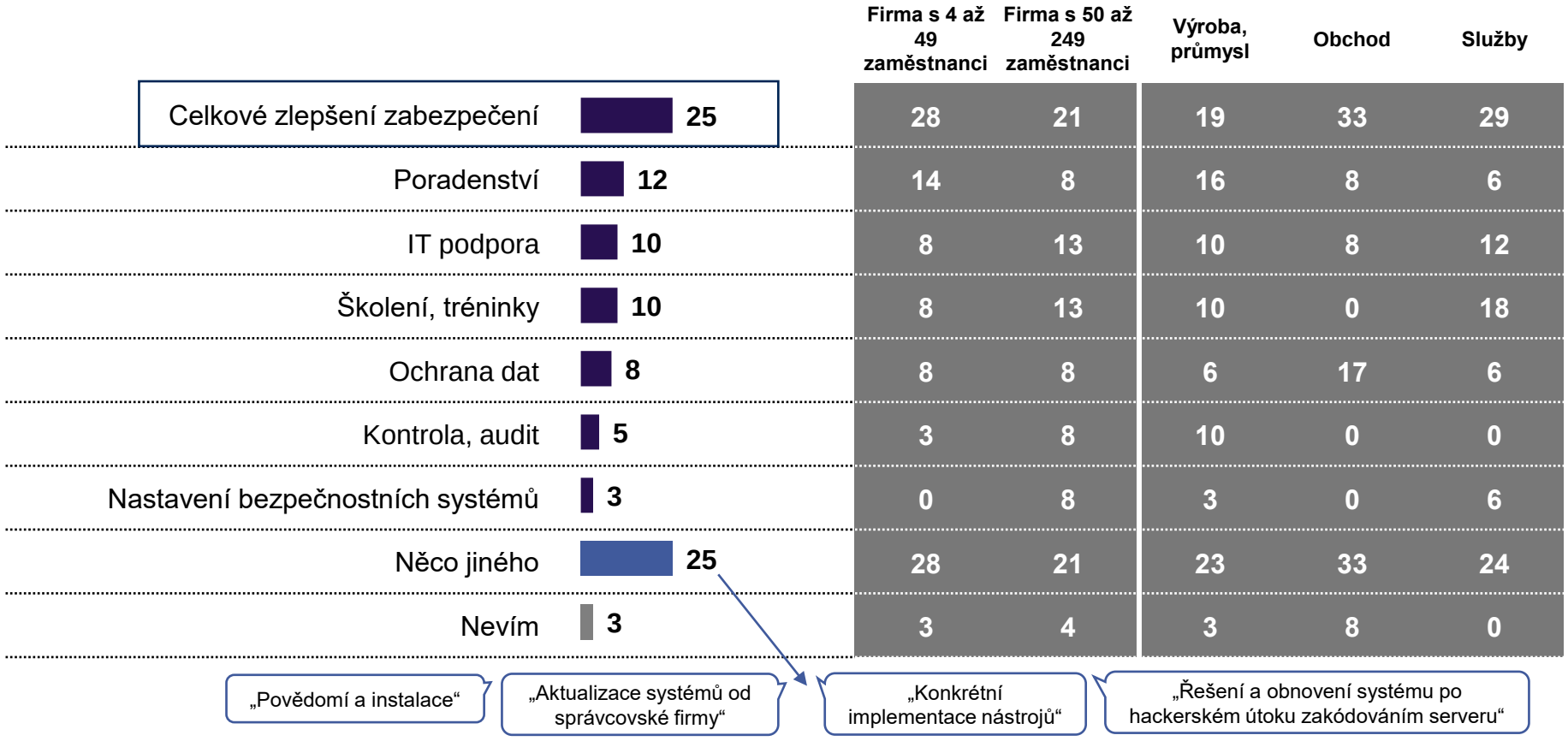
Komentář AMSP ČR:
Kybernetickou bezpečnost firmy MSP obvykle neřeší samostatně, spíše v rámci komplexnějšího řešení či digitální implementace.

K8. Vyhledala vaše společnost někdy externí pomoc nebo poradenské služby za účelem zlepšení své kybernetické bezpečnosti?

ČTVRTINA FIREM, KTERÉ VYHLEDALY EXTERNÍ POMOC, UDÁVAJÍ, ŽE SE TATO POMOC TÝKALA CELKOVÉHO ZLEPŠENÍ ZABEZPEČENÍ.

Typy pomoci vyhledané za účelem zlepšení kybernetické bezpečnosti (v %)

(Pouze dotazovaní, kteří uvedli, že vyhledali externí pomoc za účelem zlepšení jejich kybernetické bezpečnosti)



	Firma s 4 až 49 zaměstnanci	Firma s 50 až 249 zaměstnanci	Výroba, průmysl	Obchod	Služby
Celkové zlepšení zabezpečení 25	28	21	19	33	29
Poradenství 12	14	8	16	8	6
IT podpora 10	8	13	10	8	12
Školení, tréninky 10	8	13	10	0	18
Ochrana dat 8	8	8	6	17	6
Kontrola, audit 5	3	8	10	0	0
Nastavení bezpečnostních systémů 3	0	8	3	0	6
Něco jiného 25	28	21	23	33	24
Nevím 3	3	4	3	8	0

Komentář AMSP ČR:

Odpověď respondentů v tomto slidu potvrzují ten předchozí: firmy MSP řeší kyberbezpečnost spíše v rámci nějakého širšího řešení (balíčku) či digitální implementace.

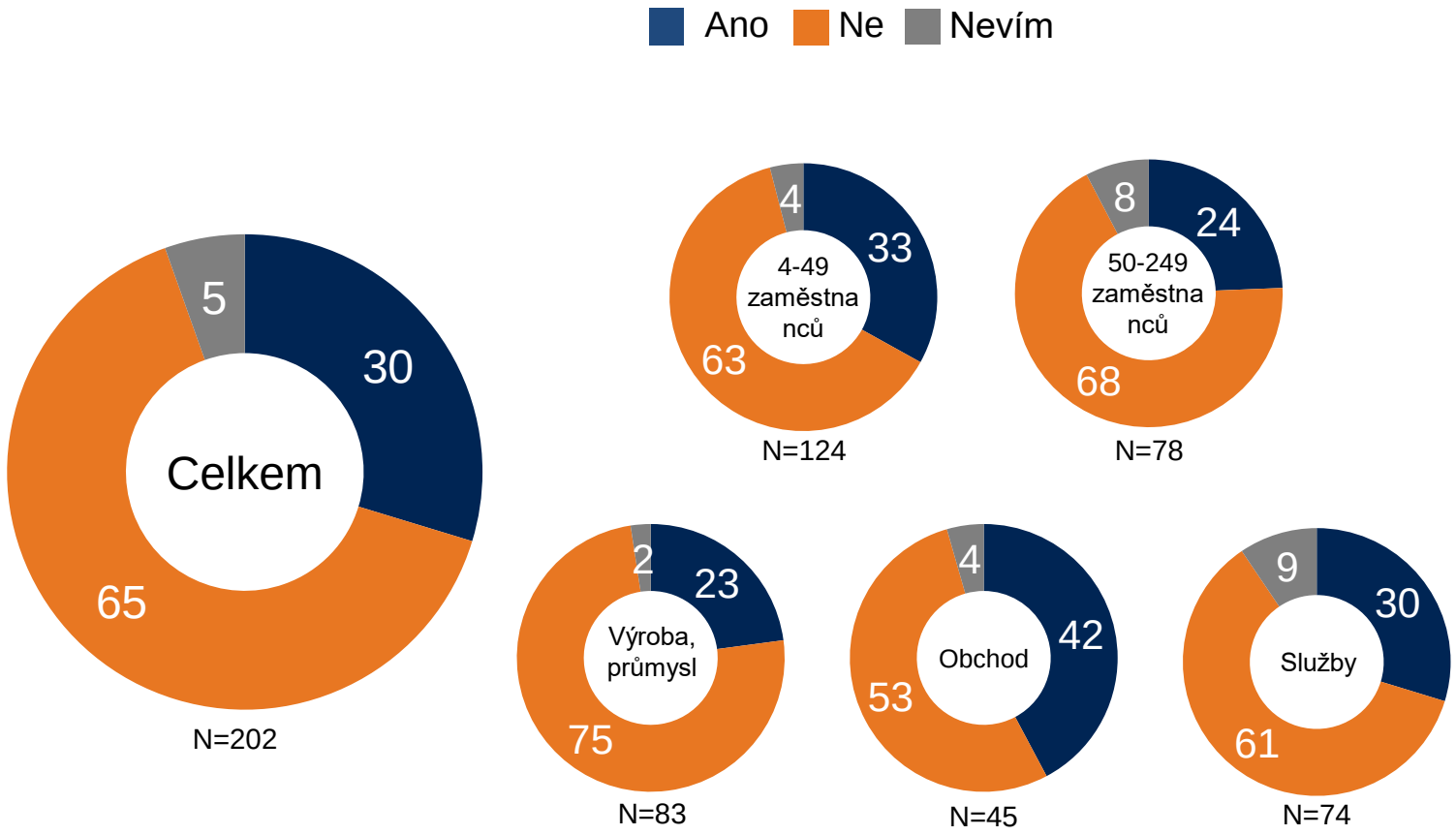
Firmy, které vyhledaly externí pomoc, uvádějí, že šlo o celkové zlepšení zabezpečení firmy, netýkalo se tedy nutně jen samotné kyberbezpečnosti.

K9. A o jako pomoc šlo?
N=60/36/24!/31!/12!/17

! = Pozor! Nízká báze

TÉMĚŘ TŘETINA DOTAZOVANÝCH FIREM SE NĚKDY SETKALA S KYBERÚTOKEM U FIREM ZE SEKTORU OBCHODU TO BYLO DOKONCE 42 %.

Setkali jste se s jakýkoli kyberútokem na Vaši firmu? (v %)

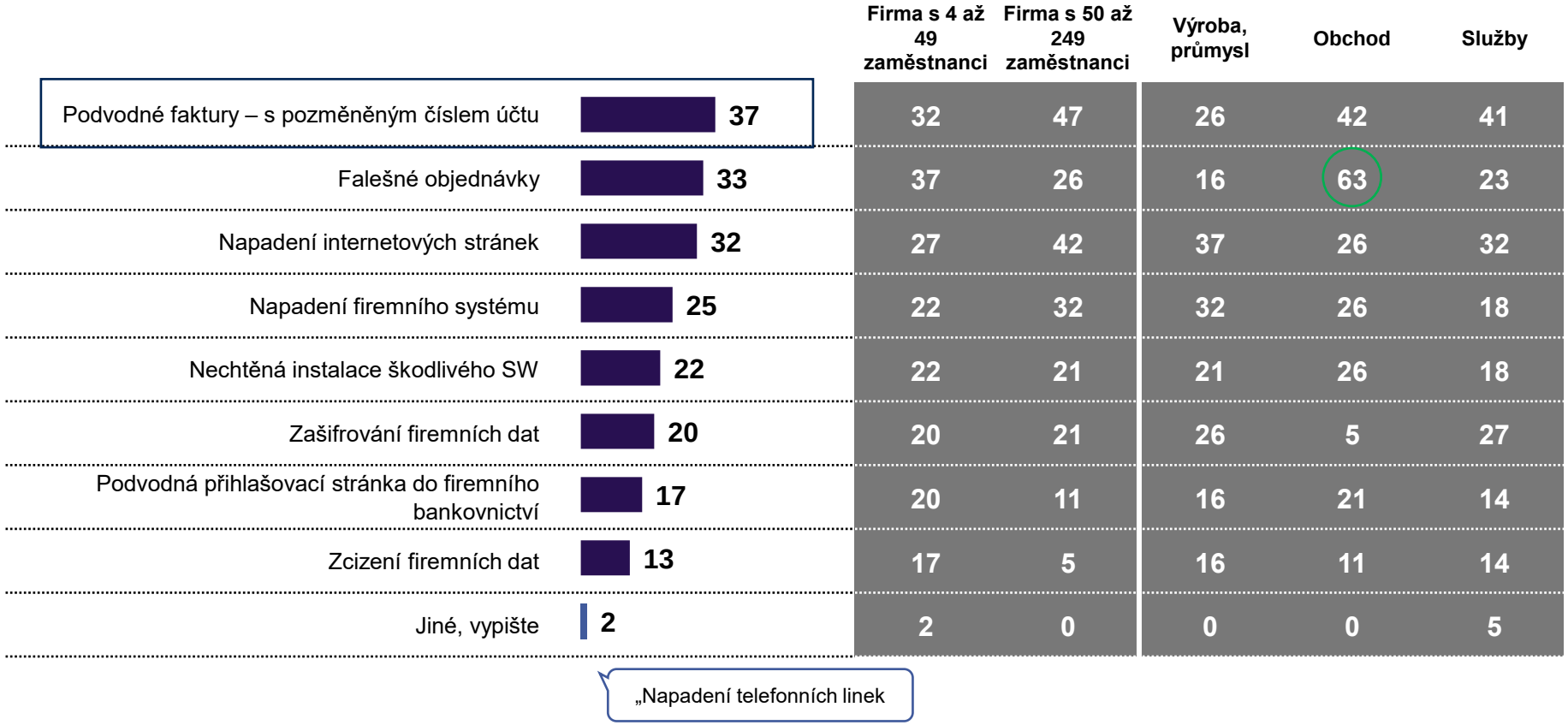


K10. Setkali jste se s jakýmkoli kyberútokem na Vaši firmu?

FIRMY SE NEJČASTĚJI SETKÁVAJÍ S PODVODNÝMI FAKTURAMI. S FALEŠNÝMI OBJEDNÁVKAMI SE ČASTĚJI SETKÁVAJÍ FIRMY ZE SEKTORU OBCHODU.

Typy kyberútoků, se kterými se firmy setkaly (v %)

(Pouze dotazovaní, kteří uvedli, že se někdy setkali s kyberútokem na jejich firmu)



	Firma s 4 až 49 zaměstnanci	Firma s 50 až 249 zaměstnanci	Výroba, průmysl	Obchod	Služby
Podvodné faktury – s pozměněným číslem účtu	32	47	26	42	41
Falešné objednávky	37	26	16	63	23
Napadení internetových stránek	27	42	37	26	32
Napadení firemního systému	22	32	32	26	18
Nechtěná instalace škodlivého SW	22	21	21	26	18
Zašifrování firemních dat	20	21	26	5	27
Podvodná přihlašovací stránka do firemního bankovnictví	20	11	16	21	14
Zcizení firemních dat	17	5	16	11	14
Jiné, vypište	2	0	0	0	5

Komentář AMSP ČR:

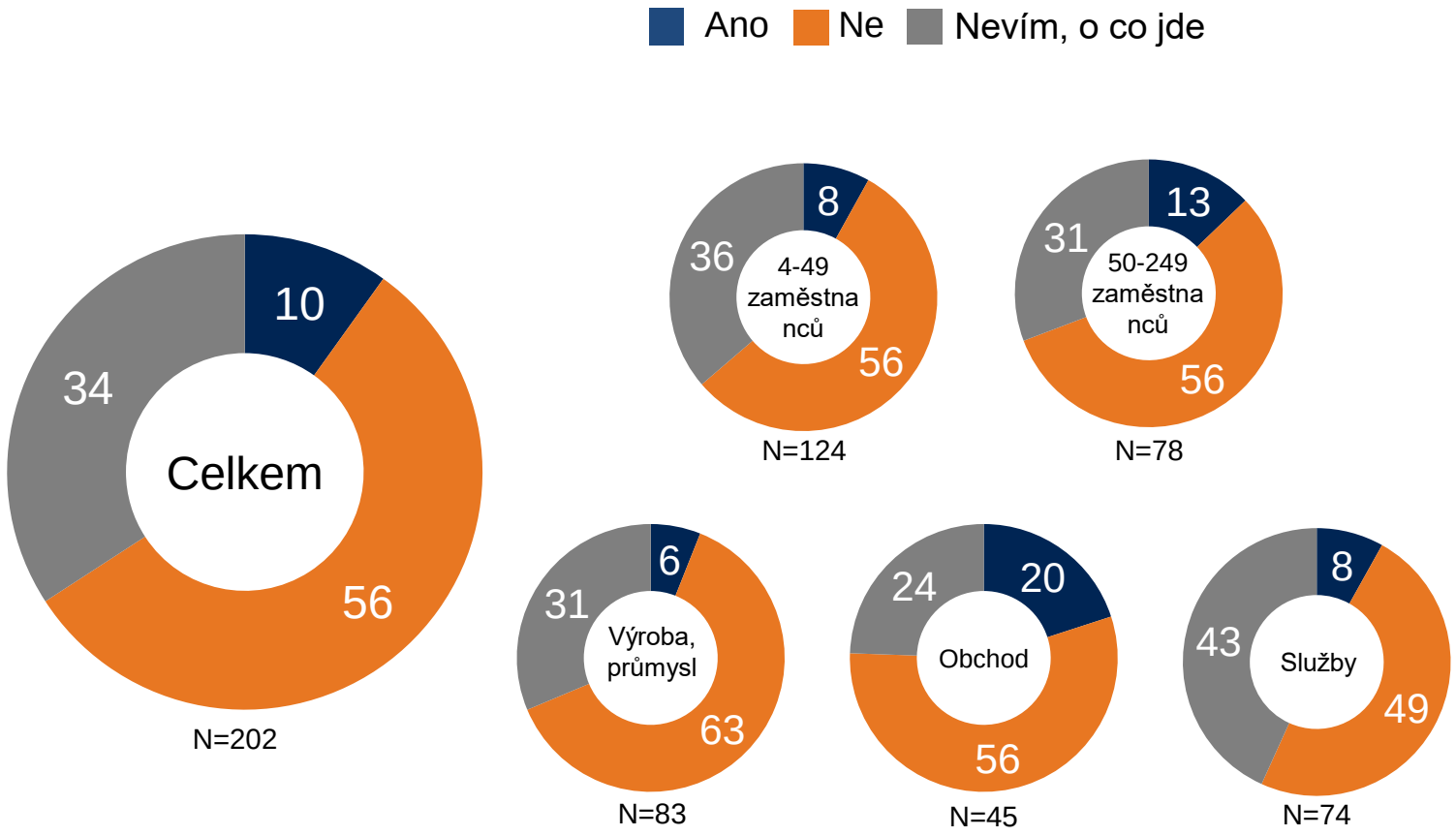
PODVODNÉ FAKTURY a FALEŠNÉ OBJEDNÁVKY jsou poměrně běžnou formou podvodů, s nimiž se firmy setkávají. Dokonce je překvapivé, že jej uvádějí pouze v cca 37 %.

Velmi závažnou formou kyberútoků je napadení FIREMNÍHO SYSTÉMU či nechtěná INSTALACE ŠKODLIVÉHO SW. Neobvyklé není ani ZAŠIFROVÁNÍ FIREMNÍCH DAT a požadavek na jejich „vykoupení“. S těmito vyděračskými praktikami se setkala nejméně pětina firem, jde o vážný problém.

K11. A o jaký útok šlo?
N=60/41/19!/19!/19!/22!

NA VĚTŠINU FIREM SMĚRNICE NIS2 TÝKAJÍCÍ SE KYBERBEZPEČNOSTI NEDOPADÁ, NEBO NEVÍ, O CO SE JEDNÁ.

Dopadá na Vaší firmu Směrnice týkající se kyberbezpečnosti - NIS2? (v %)

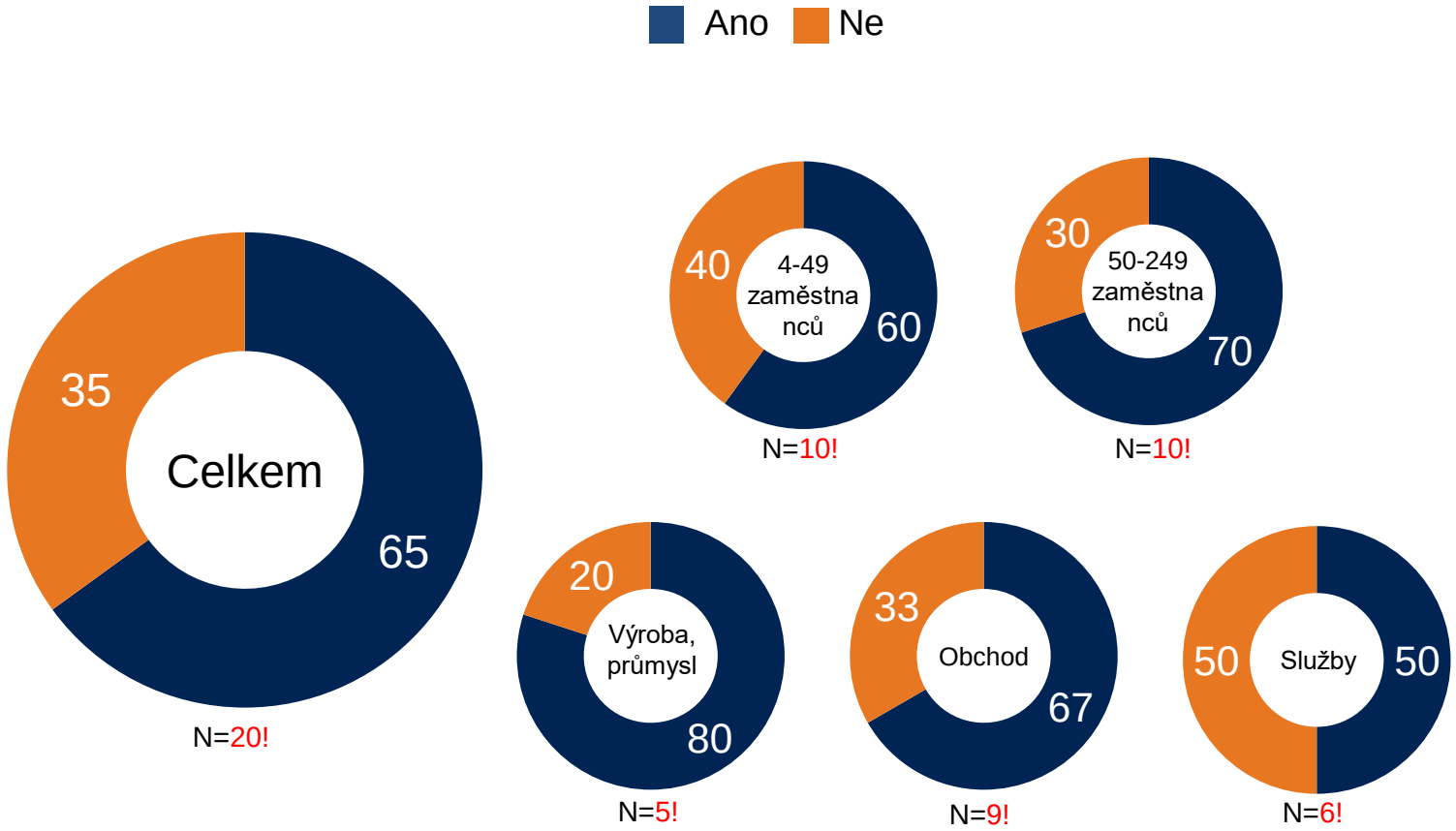


K12. Dopadá na Vaší firmu Směrnice týkající se kyberbezpečnosti - NIS2?

DVĚ TŘETINY FIREM SE PŘIPRAVUJÍ NA REGULACI PODLE NIS2, OVŠEM Z DŮVODU NÍZKÉ BÁZE JE NUTNO VÝSLEDKY VNÍMAT JAKO INDIKATIVNÍ.

Připravujete se již nyní ve vaší firmě v současnosti na regulaci podle NIS2? (v %)

(Pouze dotazovaní, kteří uvedli, že na jejich firmu dopadá směrnice NIS2 týkající se kyberbezpečnosti)

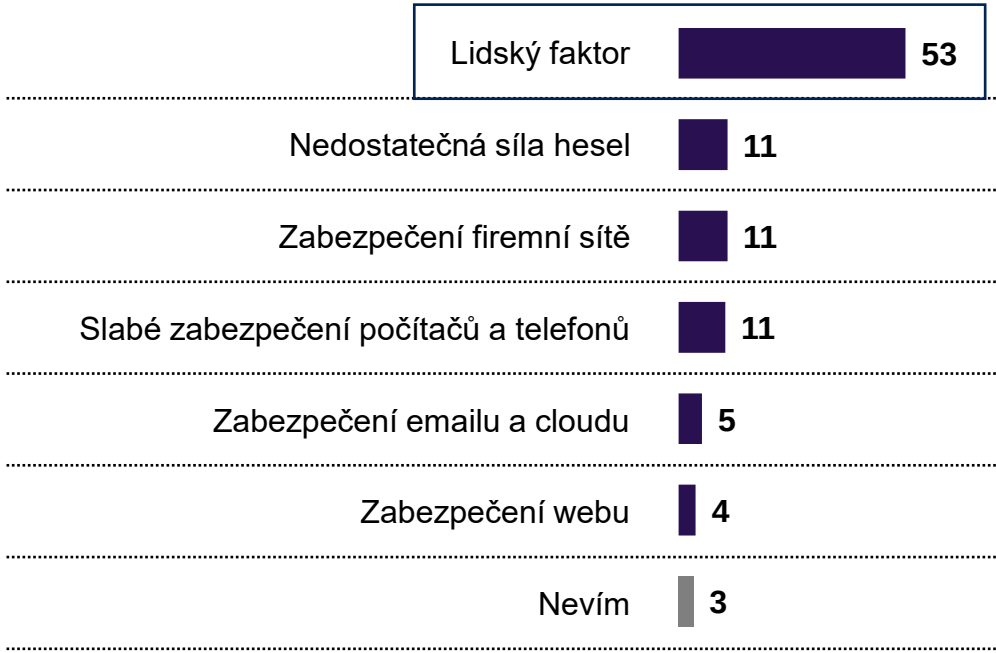


K13. Připravujete se již nyní ve vaší firmě v současnosti na regulaci podle NIS2?

Ze všech zkoumaných firem pouze 10 % udává, že se jich směrnice NIS2 týká, pouze 6,5 % firem se na ní v současnosti připravuje.

FIRMY SE OBECNĚ NEJVÍCE OBÁVAJÍ V RÁMCI ZABEZPEČENÍ SELHÁNÍ LIDSKÉHO FAKTORU, TUTO MOŽNOST UDÁVÁ VÍCE NEŽ POLOVINA.

Největší rizika z hlediska zabezpečení firmy (v %)



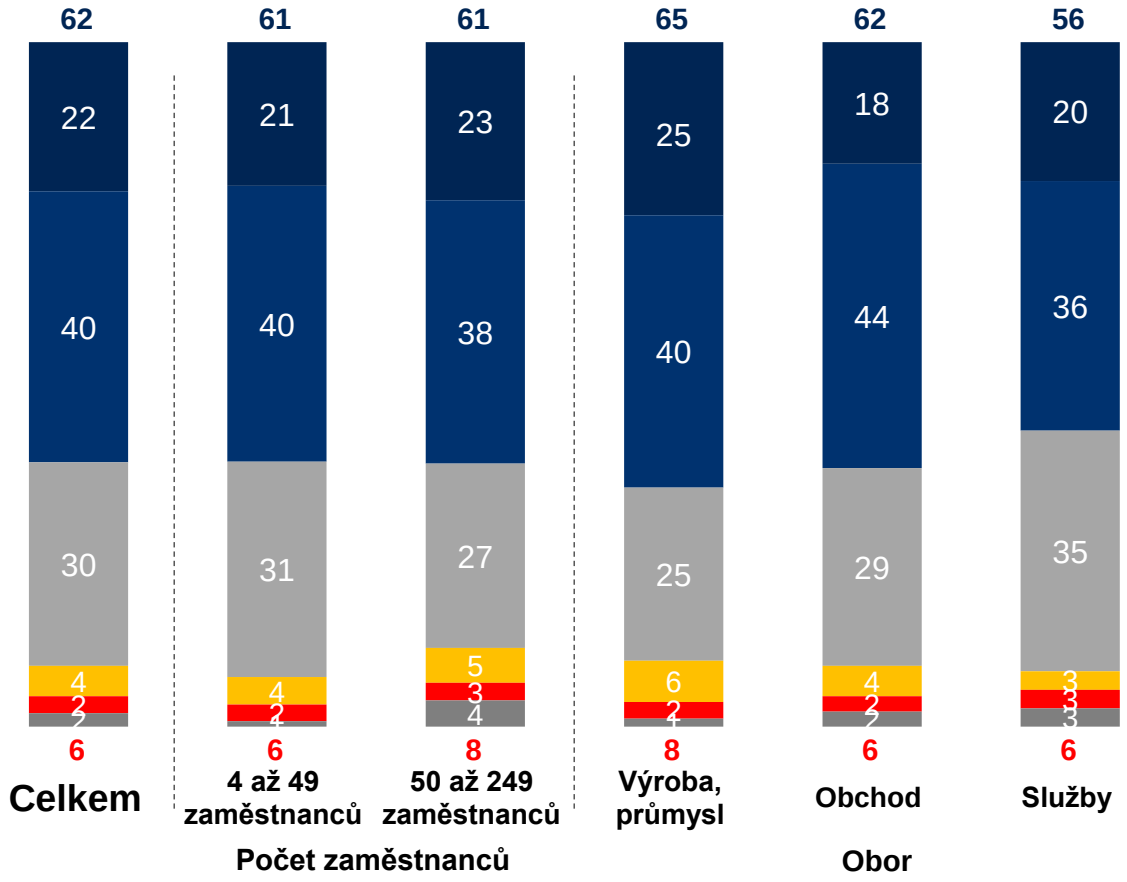
	Firma s 4 až 49 zaměstnanci	Firma s 50 až 249 zaměstnanci	Výroba, průmysl	Obchod	Služby
Lidský faktor	51	56	42	51	66
Nedostatečná síla hesel	10	14	13	11	9
Zabezpečení firemní sítě	14	8	14	11	8
Slabé zabezpečení počítačů a telefonů	10	12	17	11	4
Zabezpečení emailu a cloudu	6	5	5	9	4
Zabezpečení webu	4	4	4	2	5
Nevím	5	1	5	4	1

Komentář AMSP ČR:
Ano, lidský faktor je považován obecně za nejslabší článek celého kybernetického zabezpečení, to ukázaly zcela neomylně odpovědi více než poloviny našich respondentů. To riziko si firmy uvědomují, pravidelně edukují, ale i přesto se nelze na tuto bariéru spolehnout stoprocentně.

K14. Z hlediska zabezpečení vaší firmy, co vnímáte jako její nejslabší článek nebo největší riziko?
N=202/124/78/83/45/74

VĚTŠINA FIREM SE DOMNÍVÁ, ŽE STAV ZABEZPEČENÍ INTERNETOVÉHO BANKOVNICTVÍ U JEJICH BANKY JE VYSOKÝ.

Vnímaný stav zabezpečení internetového bankovnictví vůči kybernetickým hrozbám (v %)



T4B (hodnoty na škále 7+8+9+10)

- 9+10 – Velmi vysoké zabezpečení
- 7+8
- 4+5+6
- 2+3
- 0+1 – – Velmi nízké zabezpečení
- Nevím (bez odpovědi)

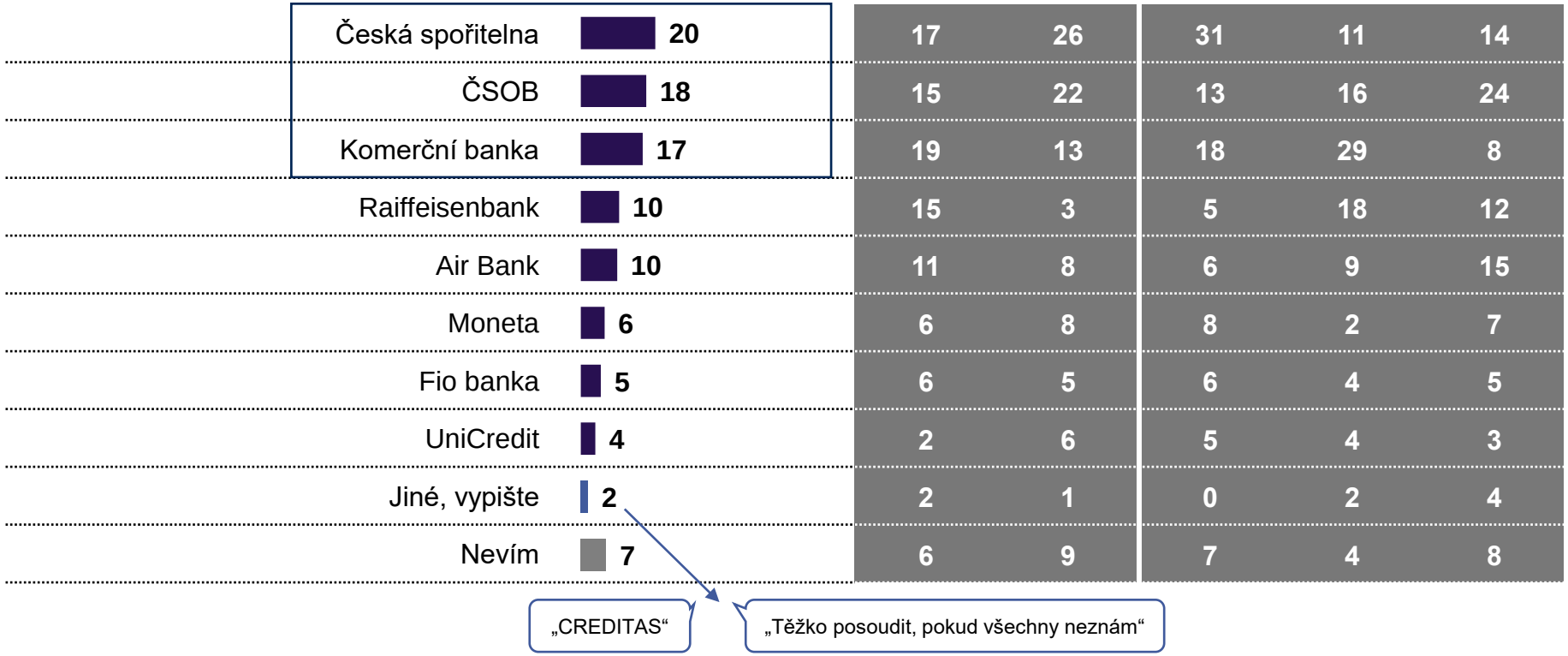
B4B (hodnoty na škále 0+1+2+3)

Komentář AMSP ČR:
Jakkoli nejsou útoky na bankovní domy ojedinělé, firmy přesto z větší části zabezpečení internetového bankovnictví poměrně silně důvěřují.

K15. Na škále od 0 do 10 uveďte, jak vnímáte stav zabezpečení vašeho internetového bankovnictví vůči kybernetickým hrozbám u své banky.
N=202/124/78/83/45/74

ČESKÁ SPOŘITELNA, ČSOB A KOMERČNÍ BANKA JSOU VNÍMÁNY JAKO LÍDŘI V OBLASTI BEZPEČNÉHO ONLINE BANKOVNICTVÍ.

Banky vnímané jako lídři v oblasti bezpečného online bankovnictví (v %)

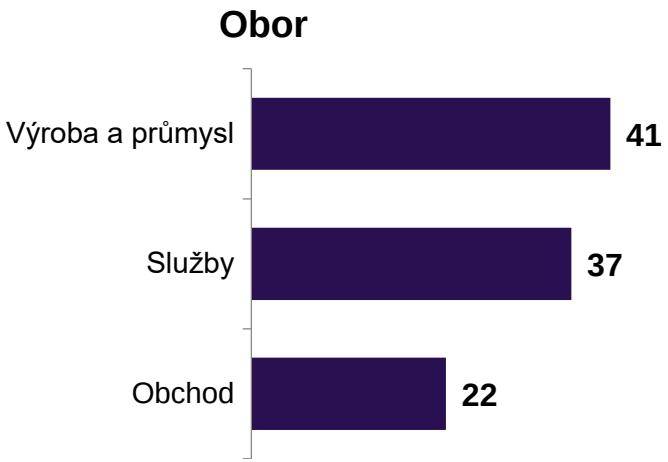


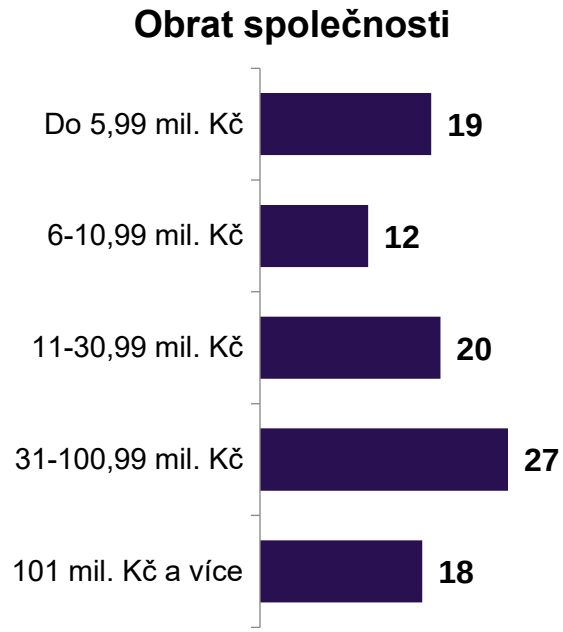
	Firma s 4 až 49 zaměstnanci	Firma s 50 až 249 zaměstnanci	Výroba, průmysl	Obchod	Služby
Česká spořitelna	17	26	31	11	14
ČSOB	15	22	13	16	24
Komerční banka	19	13	18	29	8
Raiffeisenbank	15	3	5	18	12
Air Bank	11	8	6	9	15
Moneta	6	8	8	2	7
Fio banka	6	5	6	4	5
UniCredit	2	6	5	4	3
Jiné, vypište	2	1	0	2	4
Nevím	6	9	7	4	8

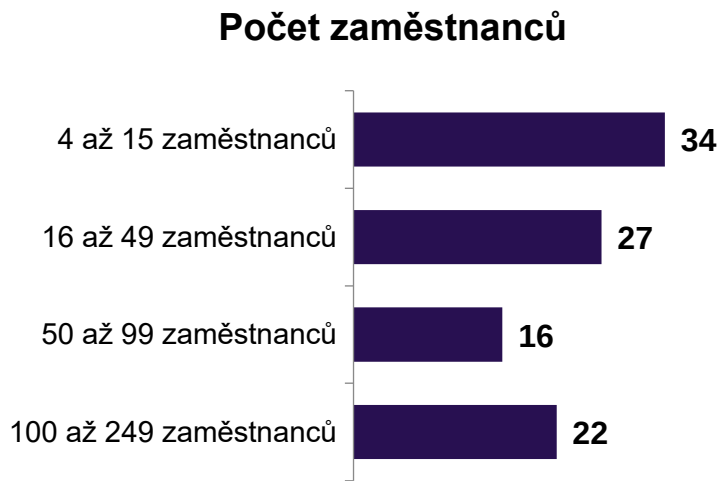
K16. Kterou z tuzemských bank, vnímáte jako lídra v oblasti bezpečného online bankovnictví?
N=202/124/78/83/45/74

STRUKTURA VZORKU

STRUKTURA VZORKU







N=202