ANALÝZA STAVU BEZPEČNOSTNÍCH POLITIK ZA ROK 2022

CRP-KYBER22: Podpora zavedení Systému řízení bezpečnosti informací v prostředí VVŠ

PS2 Bezpečnostní politiky

Verze: 2022/12

OBSAH

1 ANALÝZA STAVU BEZPEČNOSTNÍCH POLITIK

Systém řízení bezpečnosti informací (dále jen „SŘBI“) představuje soubor politik, procesů a opatření, které jsou zaměřené na ochranu informací v organizaci. Cílem SŘBI je identifikovat, ochránit, zachovat důvěrnost, integritu a dostupnost informací v organizaci. Principy spojené s SŘBI se skládají z několika základních prvků, jako jsou politiky bezpečnosti, standardy, procedury, řízení rizik a kontrolní mechanismy. Implementace SŘBI v organizaci vyžaduje neustálou údržbu a revizi, aby se zajistilo, že se organizace vyrovnává s neustále se měnícími hrozbami a riziky pro bezpečnost informací.

Problematika zavedení *Systému řízení kybernetické bezpečnosti a bezpečnosti informací* v tak specifickém a heterogenním prostředí jako je vysoká škola (rozsáhlá infrastruktura, rozsah a důležitost informačních systémů, specifičnost požadavků a potřeby v rámci provozovaných ICT řešení, vysoký počet a různorodost uživatelů, řada zákonných povinností) je výzvou, kterou většina veřejných vysokých škol (dále jen „VVŠ“) není schopna vyřešit pouze vlastními silami. Je zapotřebí zvolit systematický a komplexní přístup těžící z již zavedené spolupráce. Navzdory různorodosti vysokých škol má většina problémů v rámci kybernetické bezpečnosti (dále jen „KB“) stejnou povahu, takže spojení sil a synergie ze společného řešení je přirozeným východiskem pro dosažení maximálního efektu s omezenými zdroji.

Analýza nastíněná v tomto dokumentu má za cíl zmapovat stav a procesy související s řešením bezpečnostních politik v rámci jednotlivých VVŠ v České republice. Report se zaměřuje primárně na identifikaci nedostatečně pokrytých oblastí z pohledu interního nastavení a provozu VVŠ a představuje zároveň distribuci politik v rámci organizací v průběhu roku 2022, a to s ohledem na vnitřní (procesní) a vnější (zákonné a jiné) povinnosti. Veškerá data byla získána v rámci dvoukolového dotazníkového šetření, jenž proběhlo v květnu a prosinci 2022, a které mělo za cíl identifikovat interní dokumenty (kapitoly, řády, směrnice) pro *Systém řízení bezpečnosti informací* v rámci organizace.

PS2 považuje získané informace za mimořádně citlivé, a proto jsou veškeré údaje v maximální míře anonymizovány. Jednotlivé VVŠ po vyhodnocení šetření posléze obdržely své odpovědi ve specifickém rozcestníku, jehož cílem je nastavení přehledu týkající se příslušných bezpečnostních politik v rámci konkrétní VVŠ. Výstup analýzy stavu bezpečnostních politik je primárně rozdělen na 3 základní oblasti:

- představení dotazníkového šetření a výstupů pro jednotlivé VVŠ v podobě rozcestníků;
- shrnující výsledky týkající se dostatečně a nedostatečně pokrytých oblastí z pohledu VVŠ;
- podrobná data mapující vznik bezpečnostních politik v průběhu projektu CRP-KYBER22.

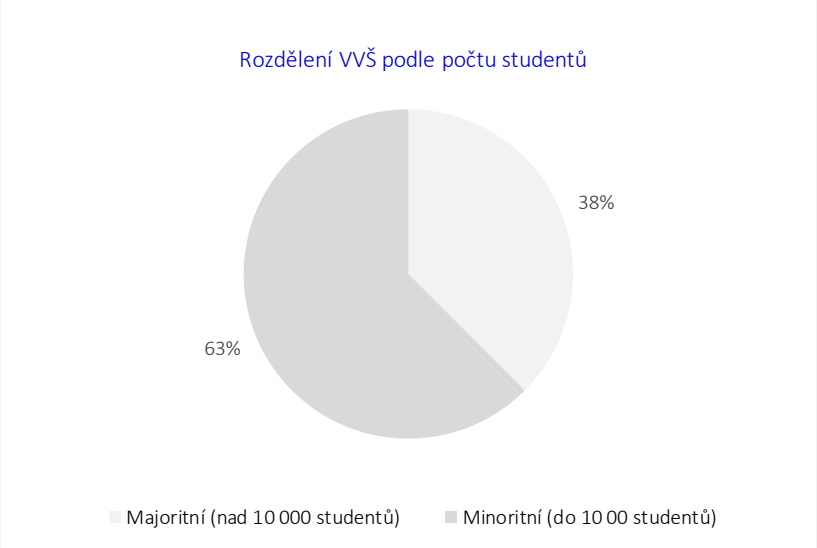
1.1. ZAPOJENÉ UNIVERZITY

Dotazníkové šetření bylo v obou kolech vyplněno 24 zástupci univerzit zapojených do projektu (celkový počet zapojených univerzit 25). Na základě výsledků dotazníkového šetření bylo dospěno k závěru, že u zúčastněných vysokých škol je možné s ohledem na jejich popisovaný stav kybernetické bezpečnosti a organizační struktury definovat vysoce rozdílné nastavení související s existencí politik v organizacích.

Jako vstupní bod pro analýzu byly jednotlivé VVŠ rozděleny na 2 základní velikostní skupiny dle počtu studentů – majoritní a minoritní. Hranice pro příslušné rozdělení byla stavena na 10 000 aktivně studujících. Toto dělení bylo provedeno z toho důvodu, že existence bezpečnostních politik úzce souvisí s organizačním a personálním pokrytím v rámci univerzit, a tedy se odvíjí od případné velikosti VVŠ, jenž souvisí s počtem studujících.[1]

- MAJORITNÍ (počet studentů nad 10 000): Univerzita Karlova, Masarykova univerzita, Univerzita Palackého v Olomouci, Česká zemědělská univerzita v Praze, Vysoké učení technické v Brně, České vysoké učení technické v Praze, Vysoká škola ekonomická v Praze, Západočeská univerzita v Plzni, Vysoká škola báňská – technická univerzita v Ostravě.

- MINORITNÍ (počet studentů do 10 000): Univerzita Tomáše Bati ve Zlíně, Mendelova univerzita, Jihočeská univerzita v Českých Budějovicích, Ostravská univerzita, Univerzita J. E. Purkyně v Ústí nad Labem, Univerzita Pardubice, Technická univerzita v Liberci, Vysoká škola chemicko-technologická v Praze, Vysoká škola technická a ekonomická v Českých Budějovicích, Vysoká škola polytechnická Jihlava, Veterinární univerzita Brno, Akademie múzických umění v Praze, Janáčkova akademie múzických umění v Brně, Akademie výtvarných umění v Praze, Slezská univerzita v Opavě.



[1] https://dsia.msmt.cz/vystupy/vu_vs.html

2 NASTAVENÍ DOTAZNÍKOVÉHO ŠETŘENÍ

Dotazníkové šetření bylo rozděleno na 12 základních oddílů, které mají mapovat ucelenou strukturu, jenž v sobě zahrnuje oblasti systému řízení bezpečnosti informací, a to na základě následujících sekcí:

1 - ORGANIZAČNÍ ŘÁD

2 - ŘÍZENÍ VNITŘNÍCH PŘEDPISŮ

3 - BEZPEČNOST INFORMACÍ

4 - ŘÍZENÍ INFORMAČNÍCH AKTIV A RIZIK

5 - SPISOVÝ A SKARTAČNÍ ŘÁD

6 - INTERNÍ AUDITY

7 - DODAVATELÉ

8 - FYZICKÁ BEZPEČNOST

9 - PRACOVNÍ ŘÁD

10 - INFORMAČNÍ BEZPEČNOST

11 - BEZPEČNOSTNÍ UDÁLOSTI A INCIDENTY

12 - SPECIFICKÉ POSTUPY ZAMĚSTNANCŮ

2.1. STRUKTURA ŠETŘENÍ

Dotazníkové šetření, jenž proběhlo v průběhu května a prosince 2022 mělo za cíl zmapovat stav bezpečnostních politik v jednotlivých organizacích. Šetření se skrze sérii otázek zaměřovalo na to, zda příslušné dokumenty popisují témata (nastíněna výše), která jsou v organizaci zpracována z pohledu bezpečnostních politik = existujících dokumentů.

IDENTIFIKOVANÉ DOKUMENTY

- měly mít formu směrnice, předpisu, příkazu, postupu, řádu či kapitoly apod.;
- měly být písemné, tedy mít fyzickou (tištěnou) nebo elektronickou podobu;
- měly popisovat bezpečnostní aspekty, tedy žádaný cílový stav dotazované oblasti;
- mohly být řízené (evidenční číslo v systému dokumentů), nebo neřízené (je to osobní písemný materiál příslušné zodpovědné osoby) dané oblasti.

V rámci jednotlivých otázek na existenci zpracovaných témat, bylo možné reagovat dle následující škály:

- Ano: téma je zpracováno v dokumentu komplexně (řízeně i neřízeně, ale je písemně);
- Spíše ano: důležité části tématu jsou buďto součástí dokumentu nebo jsou okrajově v dokumentu naznačeny;
- Spíše ne: téma není zakotveno písemně v dokumentu, ale činnost je prováděna;
- Ne: téma není vůbec zakotveno písemně v dokumentu;
- Nezodpovězeno: nemožnost odpovědi pro např. nedostatek informací, případně se jedná o informaci příliš citlivé povahy.

	Odpověď organizace	Název dokumentu	Období vzniku
Organizační schéma a organizační vazby	Ano: téma je zpracováno v dokumentu komplexně (řízeně i neřízeně, ale je písemně)	Organizační řád	Před CRP-KYBER22
Principy zastupitelnosti	Ne: téma není vůbec zakotveno písemně v dokumentu	X	X

3 VÝSLEDKY DOTAZNÍKOVÉHO ŠETŘENÍ

Bezpečnostní politika je základním dokumentem pro řízení bezpečnosti informací a je důležitá pro identifikaci a ochranu informací v organizaci. Je zásadní, aby byla bezpečnostní politika jasná, srozumitelná a snadno dostupná pro všechny zaměstnance organizace a aby se pravidelně revidovala a aktualizovala v souladu s aktuálními požadavky na ochranu dat a změnami v organizaci.

Vznik bezpečnostních politik byl v průběhu roku 2022 ovlivněn řadou vnějších (např. zákonných) i vnitřních (z pohledu probíhajícího projektu) faktorů, které zapříčinily svou působností existenci příslušných dokumentů v rámci organizačních struktur univerzit.

V případě nedostatečně pokrytých oblastí, které byly identifikovány, je nutné konstatovat, že v převážné většině případů chybí vysokým školám zakotvit procesy související se:

- systémem řízení bezpečnosti informací;
- identifikací bezpečnostních aktiv a rizik;
- bezpečnostním nastavením pravidel provozu v rámci ICT;
- obsazování zákonem definovaných pozic, a to konkrétně forma a poučení garantů aktiv;
- problematikou pokrytí mobilních zařízení.

Problém pokrytí a úpravy užívání mobilních zařízení byl nastíněn i v analýze *PS1 Nastavení kyberprostředí* z loňského roku. V analýze bylo vzneseno doporučení, že by měla být problematika mobilních zařízení specificky zmiňována i v rámci vytváření best-practice a návodů.

V případě dokumentů, jenž jsou úzkou součástí procesů souvisejících s dlouhodobým provozem univerzity, je možné konstatovat, že následující témata jsou zakotvena z pohledu bezpečnostních politik dostatečně:

- organizační a pracovní řády;
- směrnice týkající se provozu univerzitního prostředí;
- procesy upravující skartaci a archivaci významné dokumentace;
- činnosti upravující oblast auditů;
- apod.

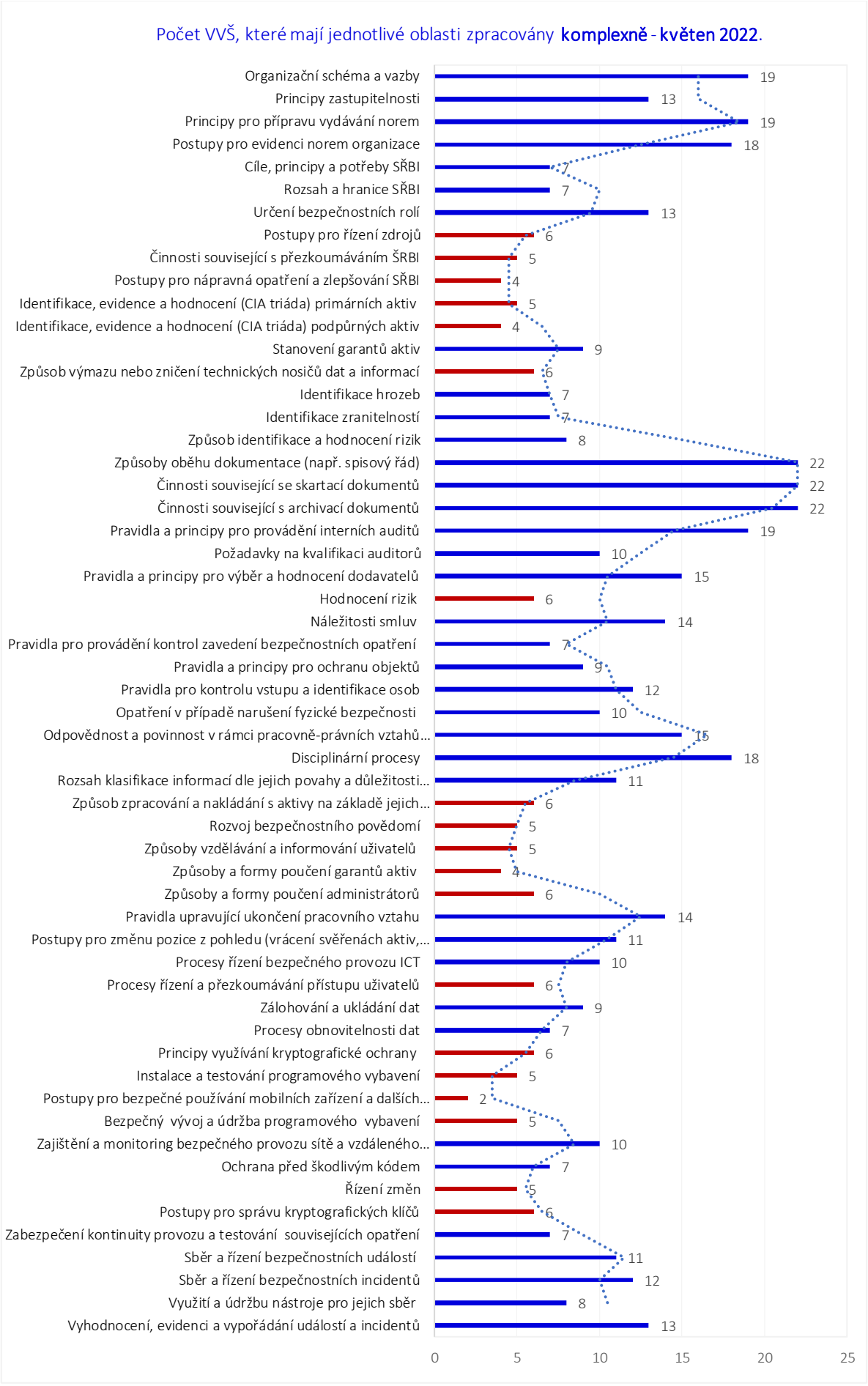
3.1. STAV BEZPEČNOSTNÍCH POLITIK – KVĚTEN A PROSINEC 2022

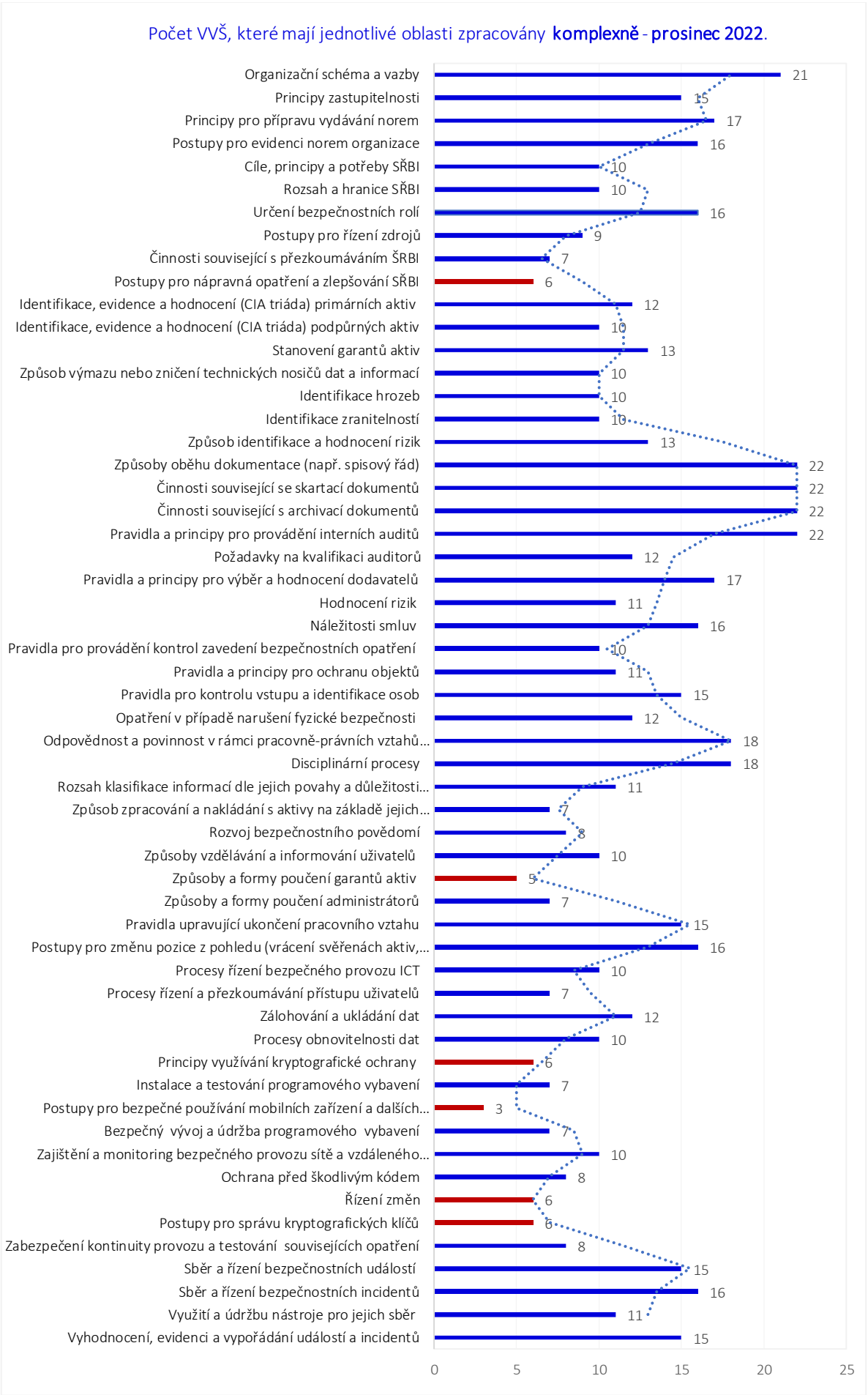
Na následujících řádcích budou představeny výsledky šetření, a to skrze dříve definované oblasti vycházející ze struktury vyplněných dotazníků. Níže uvedené grafy zobrazují, jaký **počet VVŠ pokrývá** konkrétní oblasti v rámci bezpečnostních politik, tedy které oblasti jsou většinově pokryty, a naopak které jsou podceňovány a stále nedostatečně ukotveny v rámci vnitřních struktur. Posuzovaná data jsou brána v souhrnu za celou dobu trvání projektu.

Je nutno dodat, že jednotlivé VVŠ měly na začátku a na konci projektu (květen a prosinec 2022) vytvořeny následující bezpečnostní politiky **komplexně**, což znamená, že jednotlivé oblasti byly zaznamenány písemně, zakotveny v příslušné formě (směrnice, řád), popisující cílový stav dotazované oblasti a vedeny řízeným či neřízeným způsobem. Grafy tedy ilustrují odpovědi, které v rámci dotazníku zastupovaly hodnotu:

- **Ano:** téma je zpracováno v dokumentu komplexně (řízeně i neřízeně, ale je písemně);
- **Spíše ano:** části tématu jsou buďto součástí dokumentu nebo jsou okrajově naznačeny.

Z grafu je také patrné, že v rámci bezpečnostních politik stále existují oblasti, které jsou nedostatečně zpracovány a ukotveny z pohledu vnitřní organizace příslušných VVŠ. Veškeré tyto oblasti jsou pro zdůraznění zaznačeny červeně.


Počet VVŠ, které mají jednotlivé oblasti zpracovány komplexně - květen 2022.
Organizační schéma a vazby 19
Principy zastupitelnosti 13
Principy pro přípravu vydávání norem 19
Postupy pro evidenci norem organizace 18
Cíle, principy a potřeby SŘBI 7
Rozsah a hranice SŘBI 7
Určení bezpečnostních rolí 13
Postupy pro řízení zdrojů 6
Činnosti související s přezkoumáváním ŠRBI 5
Postupy pro nápravná opatření a zlepšování SŘBI 4
Identifikace, evidence a hodnocení (CIA triáda) primárních aktiv 5
Identifikace, evidence a hodnocení (CIA triáda) podpůrných aktiv 4
Stanovení garantů aktiv 9
Způsob výmazu nebo zničení technických nosičů dat a informací 6
Identifikace hrozeb 7
Identifikace zranitelností 7
Způsob identifikace a hodnocení rizik 8
Způsoby oběhu dokumentace (např. spisový řád) 22
Činnosti související se skartací dokumentů 22
Činnosti související s archivací dokumentů 22
Pravidla a principy pro provádění interních auditů 19
Požadavky na kvalifikaci auditorů 10
Pravidla a principy pro výběr a hodnocení dodavatelů 15
Hodnocení rizik 6
Náležitosti smluv 14
Pravidla pro provádění kontrol zavedení bezpečnostních opatření 7
Pravidla a principy pro ochranu objektů 9
Pravidla pro kontrolu vstupu a identifikace osob 12
Opatření v případě narušení fyzické bezpečnosti 10
Odpovědnost a povinnost v rámci pracovně-právních vztahů... 15
Disciplinární procesy 18
Rozsah klasifikace informací dle jejich povahy a důležitosti... 11
Způsob zpracování a nakládání s aktivy na základě jejich... 6
Rozvoj bezpečnostního povědomí 5
Způsoby vzdělávání a informování uživatelů 5
Způsoby a formy poučení garantů aktiv 4
Způsoby a formy poučení administrátorů 6
Pravidla upravující ukončení pracovního vztahu 14
Postupy pro změnu pozice z pohledu (vrácení svěřenách aktiv,... 11
Procesy řízení bezpečného provozu ICT 10
Procesy řízení a přezkoumávání přístupu uživatelů 6
Zálohování a ukládání dat 9
Procesy obnovitelnosti dat 7
Principy využívání kryptografické ochrany 6
Instalace a testování programového vybavení 5
Postupy pro bezpečné používání mobilních zařízení a dalších... 2
Bezpečný vývoj a údržba programového vybavení 5
Zajištění a monitoring bezpečného provozu sítě a vzdáleného... 10
Ochrana před škodlivým kódem 7
Řízení změn 5
Postupy pro správu kryptografických klíčů 6
Zabezpečení kontinuity provozu a testování souvisejících opatření 7
Sběr a řízení bezpečnostních událostí 11
Sběr a řízení bezpečnostních incidentů 12
Využití a údržbu nástroje pro jejich sběr 8
Vyhodnocení, evidenci a vypořádání událostí a incidentů 13
0 5 10 15 20 25


Počet VVŠ, které mají jednotlivé oblasti zpracovány komplexně - prosinec 2022.
Organizační schéma a vazby 21
Principy zastupitelnosti 15
Principy pro přípravu vydávání norem 17
Postupy pro evidenci norem organizace 16
Cíle, principy a potřeby SŘBI 10
Rozsah a hranice SŘBI 10
Určení bezpečnostních rolí 16
Postupy pro řízení zdrojů 9
Činnosti související s přezkoumáváním ŠRBI 7
Postupy pro nápravná opatření a zlepšování SŘBI 6
Identifikace, evidence a hodnocení (CIA triáda) primárních aktiv 12
Identifikace, evidence a hodnocení (CIA triáda) podpůrných aktiv 10
Stanovení garantů aktiv 13
Způsob výmazu nebo zničení technických nosičů dat a informací 10
Identifikace hrozeb 10
Identifikace zranitelností 10
Způsob identifikace a hodnocení rizik 13
Způsoby oběhu dokumentace (např. spisový řád) 22
Činnosti související se skartací dokumentů 22
Činnosti související s archivací dokumentů 22
Pravidla a principy pro provádění interních auditů 22
Požadavky na kvalifikaci auditorů 12
Pravidla a principy pro výběr a hodnocení dodavatelů 17
Hodnocení rizik 11
Náležitosti smluv 16
Pravidla pro provádění kontrol zavedení bezpečnostních opatření 10
Pravidla a principy pro ochranu objektů 11
Pravidla pro kontrolu vstupu a identifikace osob 15
Opatření v případě narušení fyzické bezpečnosti 12
Odpovědnost a povinnost v rámci pracovně-právních vztahů... 18
Disciplinární procesy 18
Rozsah klasifikace informací dle jejich povahy a důležitosti... 11
Způsob zpracování a nakládání s aktivy na základě jejich... 7
Rozvoj bezpečnostního povědomí 8
Způsoby vzdělávání a informování uživatelů 10
Způsoby a formy poučení garantů aktiv 5
Způsoby a formy poučení administrátorů 7
Pravidla upravující ukončení pracovního vztahu 15
Postupy pro změnu pozice z pohledu (vrácení svěřenách aktiv,... 16
Procesy řízení bezpečného provozu ICT 10
Procesy řízení a přezkoumávání přístupu uživatelů 7
Zálohování a ukládání dat 12
Procesy obnovitelnosti dat 10
Principy využívání kryptografické ochrany 6
Instalace a testování programového vybavení 7
Postupy pro bezpečné používání mobilních zařízení a dalších... 3
Bezpečný vývoj a údržba programového vybavení 7
Zajištění a monitoring bezpečného provozu sítě a vzdáleného... 10
Ochrana před škodlivým kódem 8
Řízení změn 6
Postupy pro správu kryptografických klíčů 6
Zabezpečení kontinuity provozu a testování souvisejících opatření 8
Sběr a řízení bezpečnostních událostí 15
Sběr a řízení bezpečnostních incidentů 16
Využití a údržbu nástroje pro jejich sběr 11
Vyhodnocení, evidenci a vypořádání událostí a incidentů 15
0
5
10
15
20
25

3.2. ZASTOUPENÍ BEZPEČNOSTNÍCH POLITIK V ORGANIZACÍCH

Na následujících řádcích jsou představeny výsledky šetření, a to skrze oblasti vycházející ze struktury dotazníku. Tato data zobrazují časový interval květen–prosinec 2022. Ve výsledcích je možné naleznout primárně to, zda a v jaké míře došlo ke vzniku bezpečnostních politik za dobu projektu. Na závěr je zapotřebí dodat, že v jednotlivých grafech jsou zobrazeny odpovědi, které v rámci dotazníku zastupovaly hodnotu:

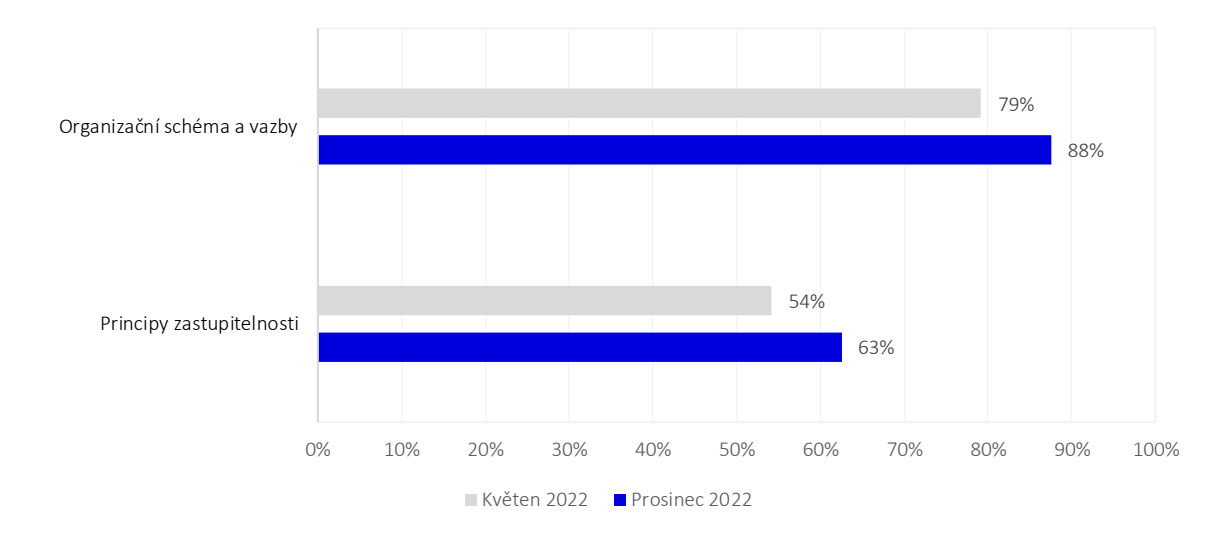
- **Ano:** téma je zpracováno v dokumentu komplexně (řízeně i neřízeně, ale je písemně);
- **Spíše ano:** části tématu jsou buďto součástí dokumentu nebo jsou okrajově naznačeny.

Dále je nutné zdůraznit, že v rámci činnosti PS2 vnikla řada bezpečnostních politik, které měly možnost si jednotlivé VVŠ implementovat. Jejich ucelený seznam je možné naleznout níže, případně v příloze vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti:

- Politika systému řízení bezpečnosti informací;
- Politika řízení aktiv;
- Politika organizační bezpečnosti
- Politika řízení dodavatelů;
- Politika bezpečnosti lidských zdrojů;
- Politika řízení provozu a komunikací;
- Politika řízení přístupu;
- Politika bezpečného chování uživatelů;
- Politika zálohování a obnovy dlouhodobého ukládání;
- Politika bezpečného předávání a výměny informací;
- Politika řízení technických zranitelností;
- Politika bezpečného používání mobilních zařízení;
- Politika akvizice, vývoje a údržby;
- Politika ochrany osobních údajů;
- Politika fyzické bezpečnosti;
- Politika bezpečnosti komunikační sítě;
- Politika ochrany před škodlivým kódem;
- Politika nasazení a používání nástroje pro detekci kybernetických incidentů;
- Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických incidentů;
- Politika bezpečného používání kryptografické ochrany;
- Politika řízení změn;
- Politika zvládání kybernetických bezpečnostních incidentů.

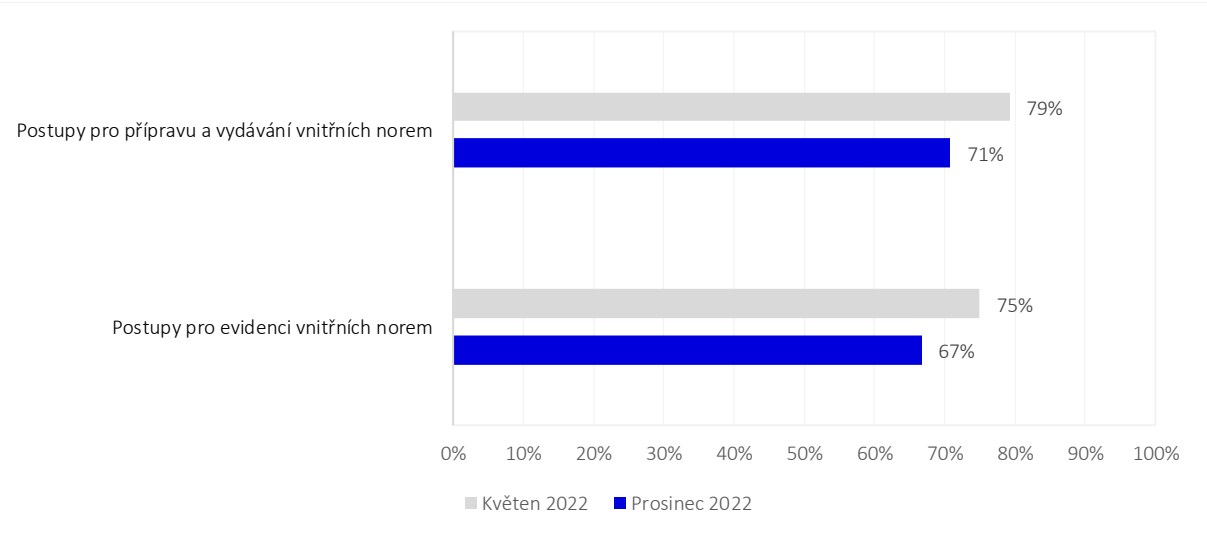
1 - ORGANIZAČNÍ ŘÁD

Z pohledu výsledků analýzy je možné konstatovat, že v případě oblastí, které souvisely s provozním a organizačním nastavením jednotlivých organizací, tak se přílišné změny týkající se vzniku bezpečnostních politik neudály. Je to částečně i z toho důvodu, že jsou tyto oblasti již náležitě pokryty s ohledem na historii působení a existenci samotných VVŠ.



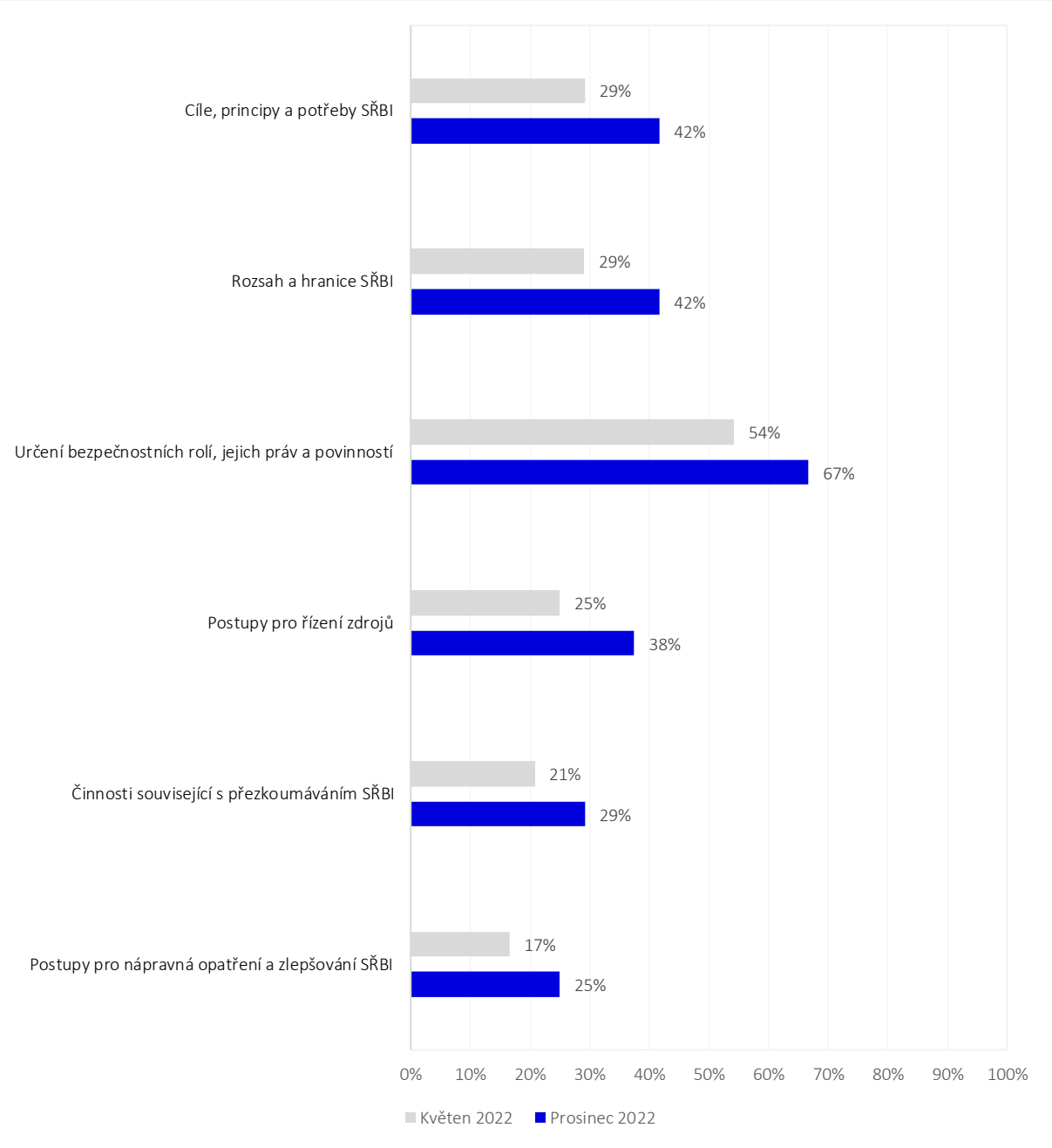
2 - ŘÍZENÍ VNITŘNÍCH PŘEDPISŮ

V případě odpovědí, které souvisely s *postupy pro evidenci vnitřních norem* a *činnostmi souvisejícími s přípravou a vydáváním vnitřních norem*, je potřeba upozornit na to, že s ohledem na klesající trend příslušných odpovědí by měly být výsledky vnímány orientačně.



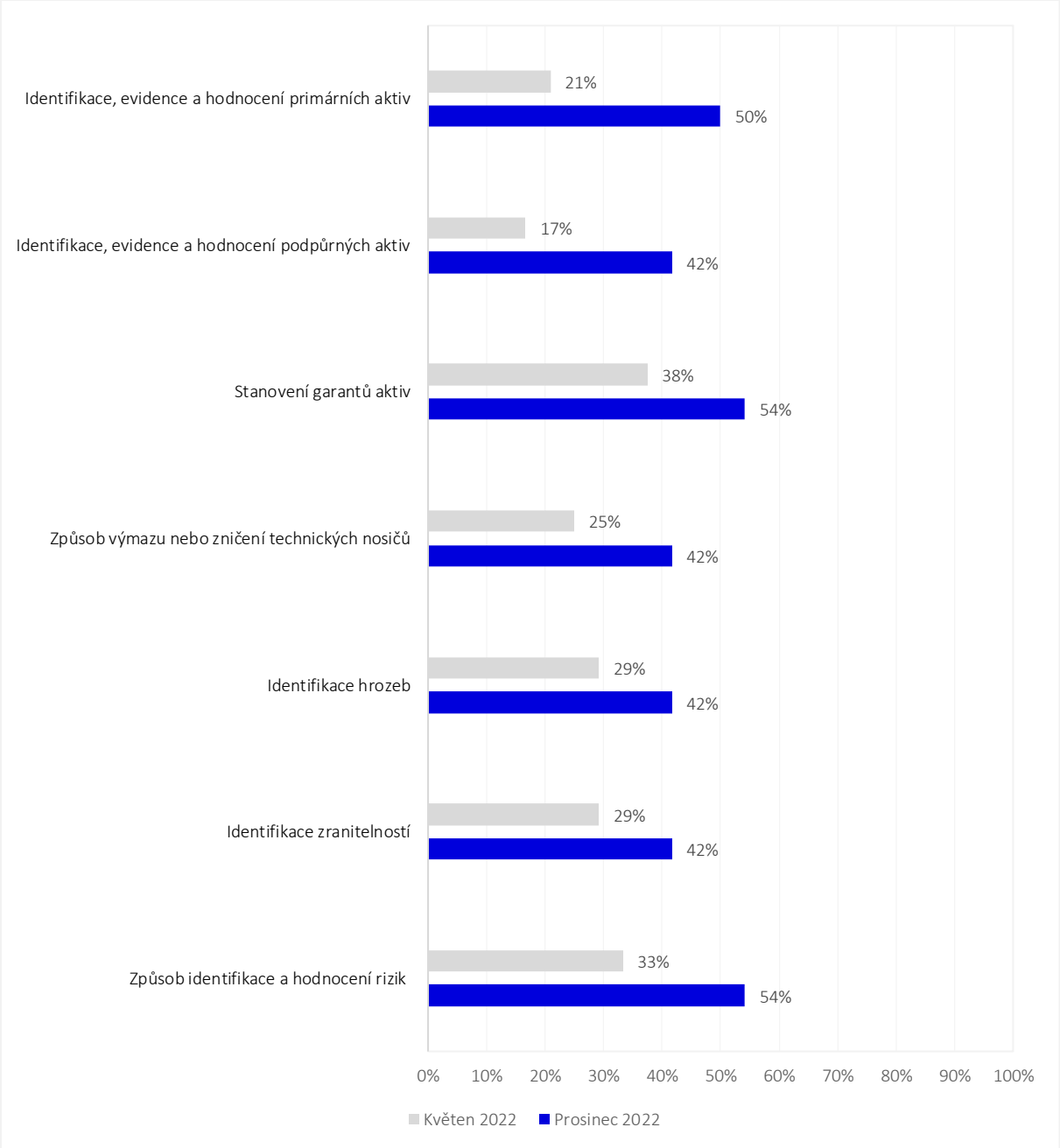
3 – BEZPEČNOST INFORMACÍ

Oblast *Bezpečnosti informací* lze klasifikovat jako nedostatečně pokrytou. S ohledem na směřování a cíle projektu je však možné poukázat na to, že v jeho průběhu došlo ke konzistentnímu nárůstu v případě jednotlivých kategorií. Tato data mimo jiné deklarují i to, že problematika *Systému řízení kybernetické bezpečnosti a bezpečnosti informací* ve specifickém prostředí jakou je VVŠ je tématem, jehož aktuálnost a důležitost je zapotřebí brát náležitě v zřetel, neboť se z pohledu šetření jednalo o jednu z nejméně pokrytých v případě odpovědí VVŠ.

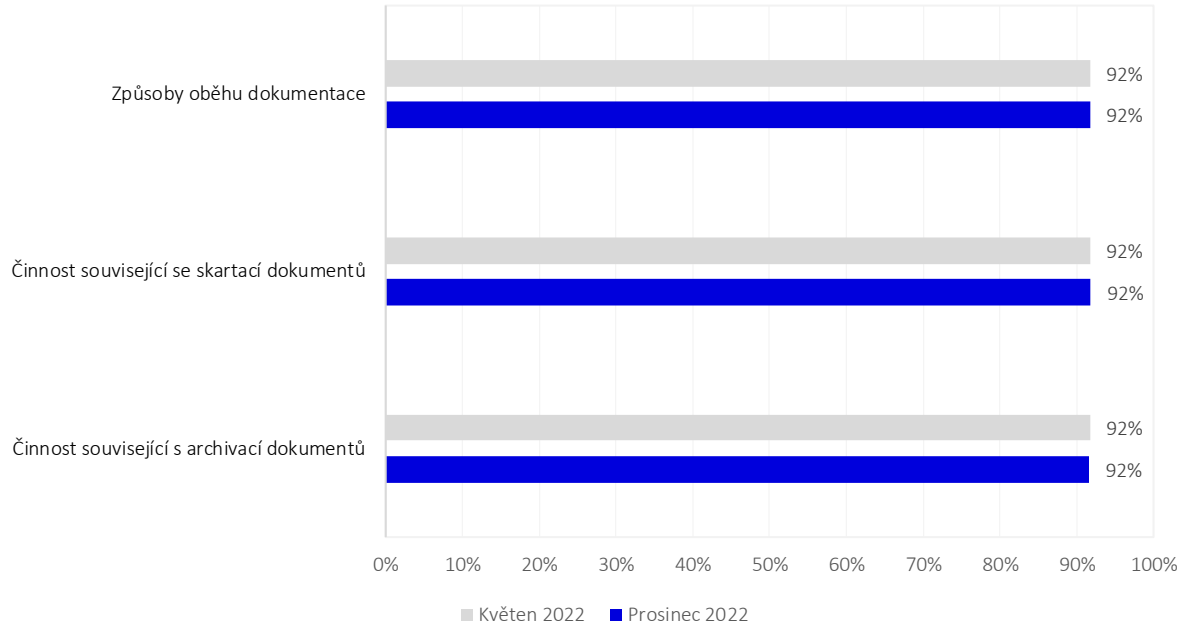


4 – ŘÍZENÍ INFORMAČNÍCH AKTIV A RIZIK

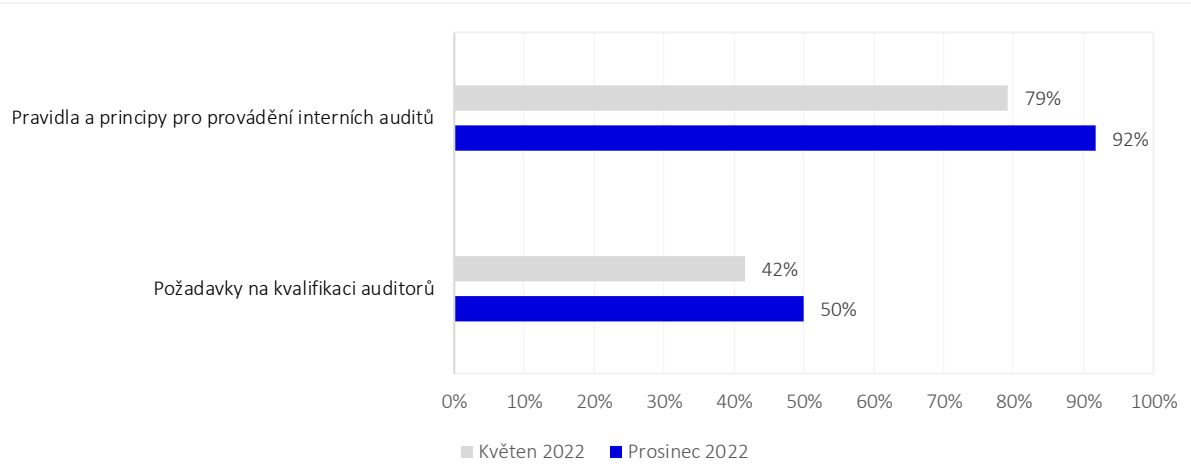
Řízení informačních aktiv a rizik je důležitou součástí řízení bezpečnosti informací. Cílem je identifikovat, ochránit a zachovat důvěrnost, integritu a dostupnost informací v organizaci. S ohledem na významnost tématu je možné konstatovat, že z pohledu existence bezpečnostních politik jsou stále nedostatečně pokryty oblasti související s řízením informačních aktiv a rizik. Tím, že VVŠ provozují významné informační systémy, a to na základě zákona č. 181/2014 Sb., o kybernetické bezpečnosti a vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, které stojí právě na přístupu založeném na posuzování rizik, tak je nutné dbát zvýšené důraz na vznik příslušných politik s těmito tématy souvisejícími.



5 - SPISOVÝ A SKARTAČNÍ ŘÁD

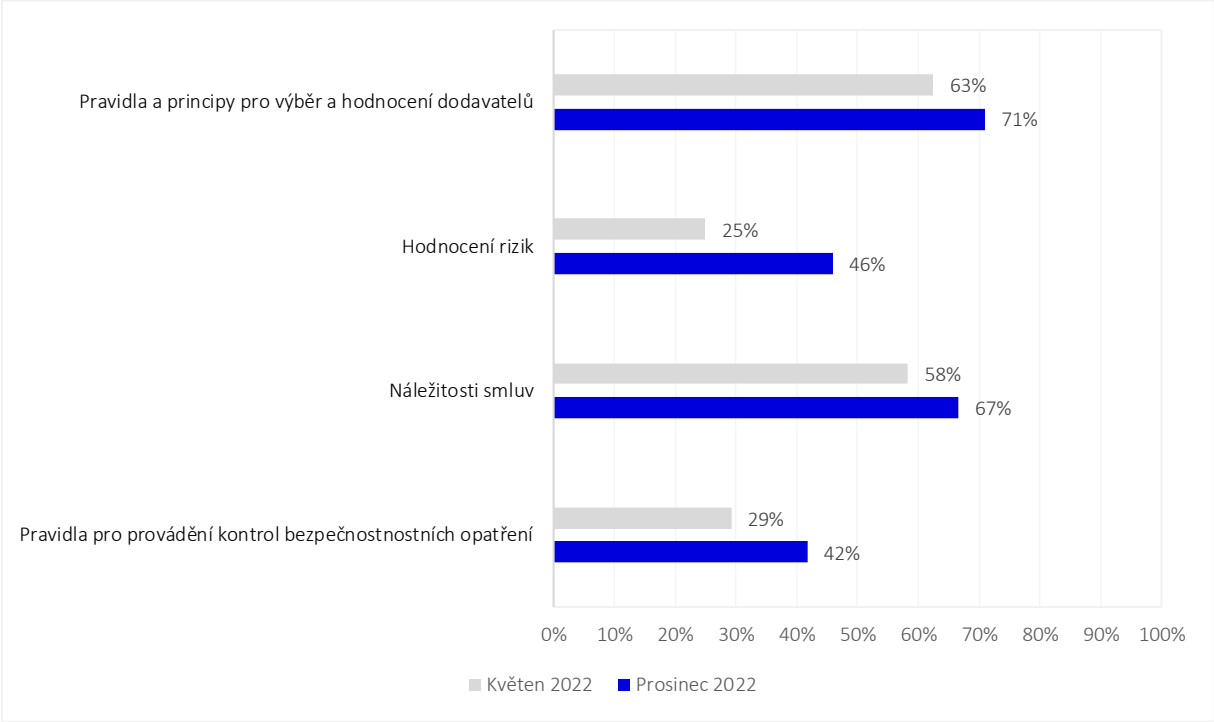


6 - INTERNÍ AUDITY

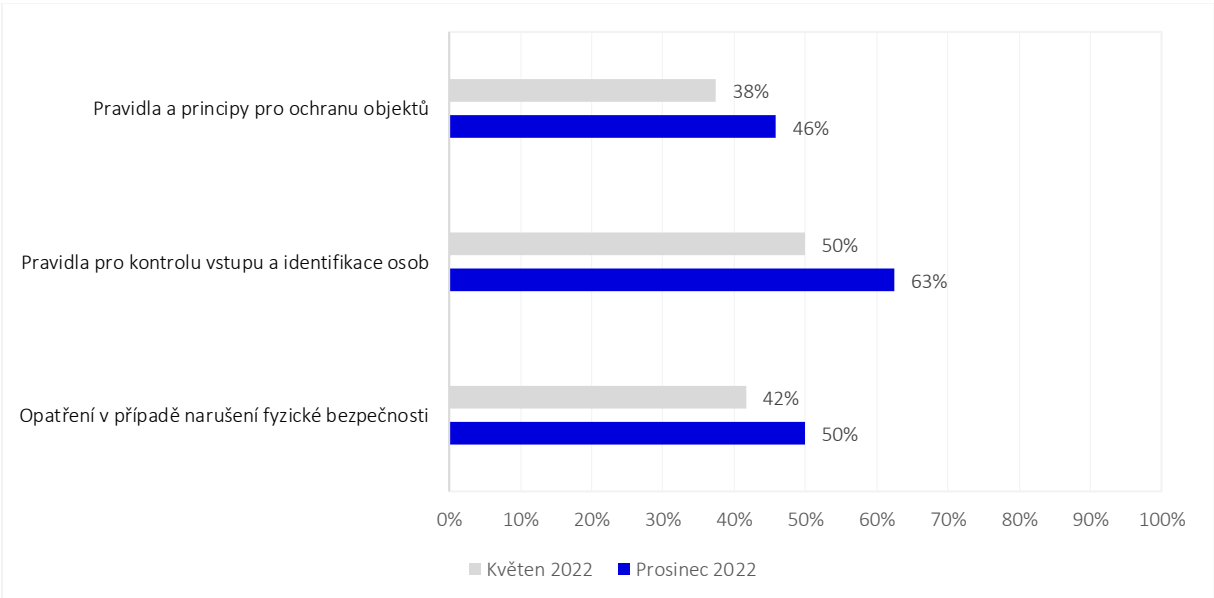


7 - DODAVATELÉ

Problémy související s nastavením příslušných mechanismů z pohledu zajištění spolupráce v rámci dodavatelských řetězců mohou vzniknout z různých důvodů. Je možné mezi ně např. zařadit nedodržování standardů a pravidel organizace nebo nedostatečné dodržování bezpečnostních opatření ze strany dodavatele. Tyto problémy mohou vést k rizikům pro bezpečnost dat, která se přenášejí mezi organizací a dodavatelem, či případně k narušení integrity systému organizace. Je tedy nezbytné stanovit jasná pravidla a postupy pro dodržování bezpečnostních politik a kontrolovat dodržování těchto pravidel.

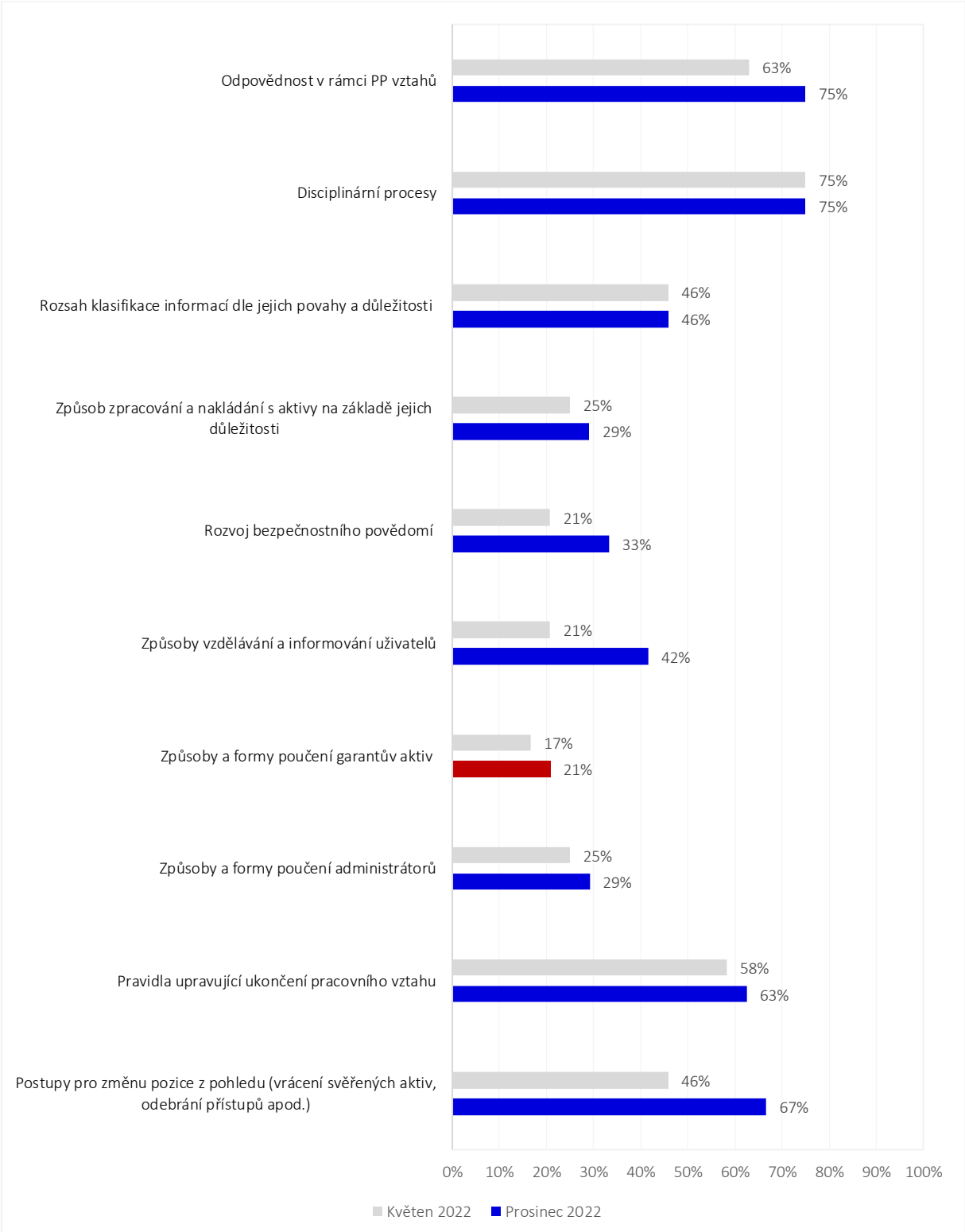


8 - FYZICKÁ BEZPEČNOST



9/10 - INFORMAČNÍ BEZPEČNOST / PRACOVNĚ-PRÁVNÍ VZTAHY

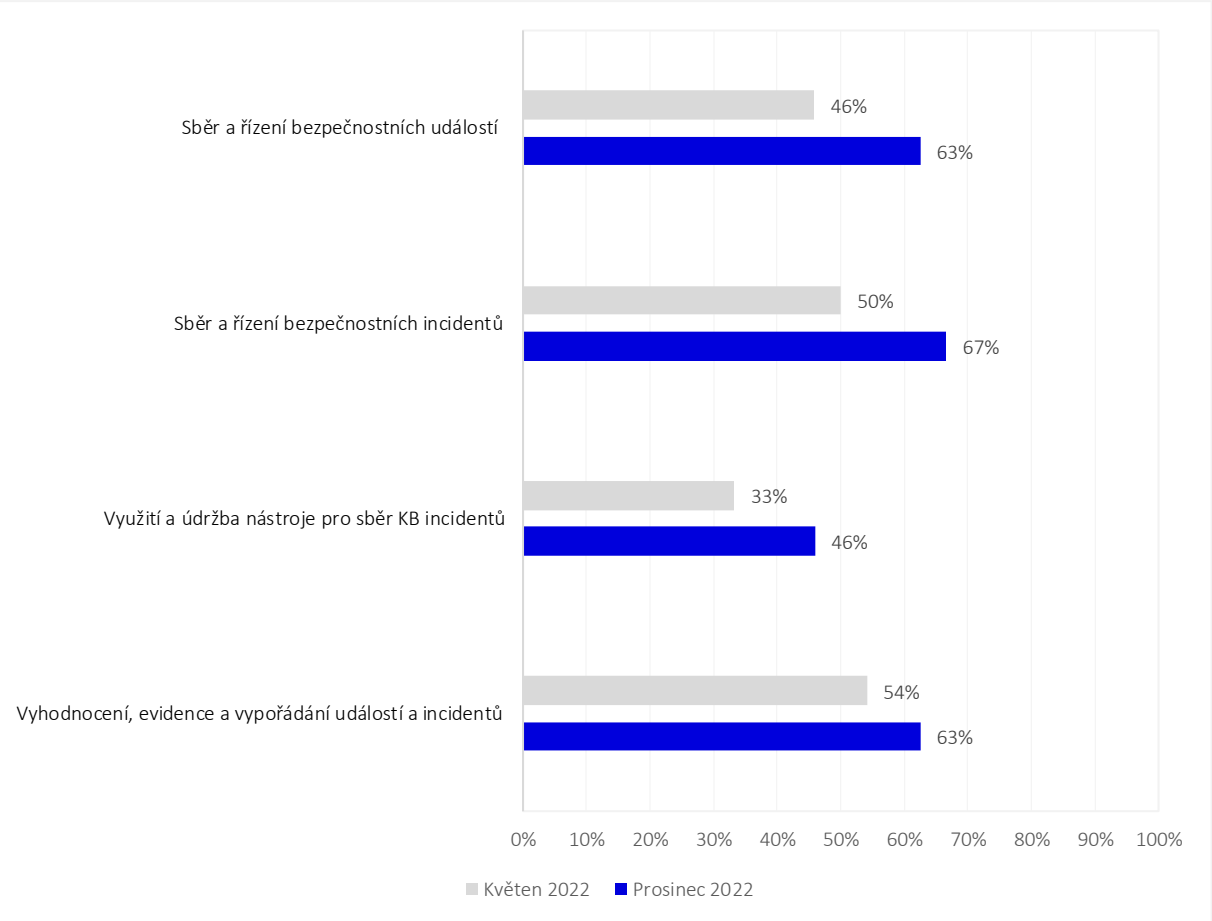
V případě oblastí souvisejících s dlouhodobým provozním chodem univerzit, tak je možné konstatovat, že z pohledu VVŠ jsou dostatečně podchyceny skrze příslušné politiky. Co ovšem rapidně pokulhává je úprava nově definovaných rolí z pohledu vyhlášky, a to konkrétně oblastí souvisejících se způsoby a formami poučení garantů aktiv.



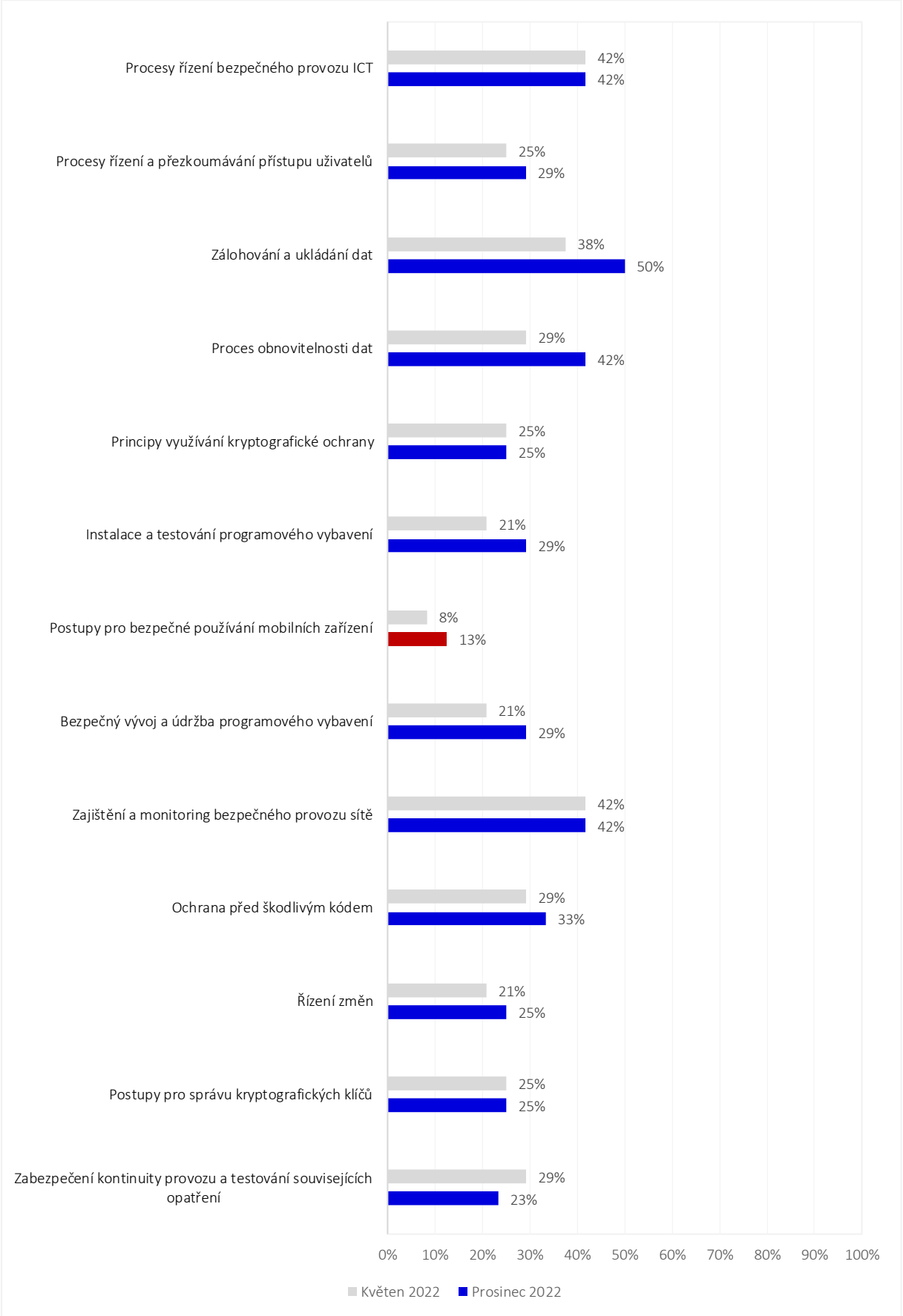
11 - BEZPEČNOSTNÍ UDÁLOSTI A INCIDENTY

Kybernetické bezpečnostní události a incidenty jsou stále častějšími problémy ve všech odvětvích a strukturách společnosti. Mohou mít závažné důsledky, a to jak pro organizaci samotnou, tak i její uživatele. Navzdory tomu, že se v posledních letech zvýšilo povědomí o důležitosti kybernetické bezpečnosti, tak stále existují významné nedostatky týkající se řešení bezpečnostních událostí a incidentů z pohledu nastavených procesů.

V případě VVŠ je možné konstatovat, že aktuálně jsou jednotlivé procesy související s řešením incidentů, jenž mají být zakotveny v rámci bezpečnostních politik na „dobré cestě“. Za zmínku stojí i to, že tato oblast byla jednou z nejprogresivnějších, co se týče výstupů v rámci aktuálního (CRP-KYBER22) a uplynulého (CRP-KYBER21) projektu.



12 - SPECIFICKÉ POSTUPY ZAMĚSTNANCŮ ICT



4 ZÁVĚR

Bezpečnostní politiky jsou jedním ze základních pilířů, na kterém stojí *Systém řízení bezpečnostních informací*. Ze své podstaty jsou důležitým nástrojem pro zajištění nejen bezpečnosti informací v rámci prostředí vysokých škol, ale také pro zachování důvěryhodnosti a integrity dat. Je tedy důležité, aby vysoké školy pečlivě zvážily problematiku související s jejich vytvářením a implementací, a aby se zajistilo, že budou jednotlivé politiky účinné a v souladu s potřebami organizace.

S ohledem na zmíněné, jsou kroky, které se v průběhu roku uskutečnily v rámci PS2 zásadní pro možný vývoj a vznik politik v tak specifickém prostředí, jako je vysoká škola. Z pohledu výsledků dotazníkového šetření za uplynulý rok, je možné konstatovat, že právě i díky výstupům PS2, která po dobu projektu jednotlivé politiky vytvářela, bylo vysokým školám umožněno si mnohé z politik implementovat, a to i na základě např. jejich omezených lidských zdrojů.

Přes tato úskalí lze s jistotou prohlásit **3 významné skutečnosti**, které v průběhu projektu nastaly:

1. Celková úroveň organizační bezpečnosti na VVŠ se jednoznačně zlepšila.
2. Bezpečnostní politiky byly vypracovány pro všechny oblasti organizační bezpečnosti, které vyžaduje zákon o kybernetické bezpečnosti a projekt nezůstal jen u klíčových oblastí, které byly původním cílem projektu.
3. Podařilo se usnadnit zavedení bezpečnostních politik do vnitřních legislativ VVŠ a zkrátit tak dobu potřebnou na zajištění jejich souladu se zákonem.

Je zapotřebí zdůraznit, že i přes pokroky, které byly v oblasti bezpečnostních politik na vysokých školách učiněny, tak stále existují některé oblasti, kterým je zapotřebí věnovat zvýšenou pozornost. Mezi tyto oblasti spadají zejména politiky související s:

- identifikací bezpečnostních aktiv a rizik;
- systémem řízení bezpečnosti informací;
- bezpečnostním nastavení pravidel provozu v rámci ICT;
- obsazování zákonem definovaných pozic, konkrétně pak forma a poučení garantů aktiv;
- problematika pokrytí mobilních zařízení.

Tyto oblasti jsou stále pro mnohé vysoké školy výzvou a vyžadují další práci a pozornost, která by se jim měla z pohledu procesů souvisejících se konstituováním politik věnovat.

V závěru této analýzy je zapotřebí poděkovat primárně členům PS2 za jejich úsilí a práci v průběhu roku, která se kladně podepsala na procesech souvisejících se vznikem bezpečnostních politik v rámci vnitřních organizací VVŠ za dobu trvání projektu CRP-KYBER22.