Prieskum kybernetickej bezpečnosti v mimovládnom sektore na Slovensku v roku 2023

Autor: Viliam Kaliňák

Názov výstupu: Prieskum kybernetickej bezpečnosti v mimovládnom sektore na Slovensku v roku 2023
Názov výstupu z opisu: **Samostatný analytický prieskum, mapovanie a zber kvalitatívnych a kvantitatívnych dát**
Zadávateľ: Úrad splnomocnenca vlády SR pre rozvoj občianskej spoločnosti
Národný projekt: PODPORA PARTNERSTVA A DIALÓGU V OBLASTI PARTICIPATÍVNEJ TVORBY VEREJNÝCH POLITÍK II.
ITMS kód projektu: 314011CQM9
Operačný program: Efektívna verejná správa
Obdobie vyhotovenia /spracovania: október – november 2023

Tento projekt je podporený z Európskeho sociálneho fondu.

Zhrnutie

Vo viacerých krajinách Európy sú dlhodobo evidované kybernetické útoky a špionáž namierené proti mimovládnym neziskovým organizáciám. Prehľad o takýchto útokoch ako aj dáta o stave kybernetickej bezpečnosti v mimovládnom sektore na Slovensku však doteraz chýbali. Úrad splnomocnenca vlády SR pre rozvoj občianskej spoločnosti preto v roku 2023 zrealizoval anonymný, nereprezentatívny prieskum, ktorý mal túto realitu poodhaliť.

Z výsledkov prieskumu vyplýva, že mimovládny sektor na Slovensku nebol v roku 2023 v oblasti kybernetickej bezpečnosti pripravený predovšetkým po finančnej, metodickej, analytickej a normatívnej stránke. Značná časť organizácií tiež neposkytovala školenia pre svojich zamestnancov a nemala určené osoby zodpovedné za riadenie kybernetickej bezpečnosti ani ochranu osobných údajov. Po technickej stránke organizácie implementovali len niektoré základné bezpečnostné opatrenia a technológie. Tieto nedostatky mohli v konečnom dôsledku kumulatívne viesť k skreslenému situačnému prehľadu o hrozbách, ktorým organizácia čelí, a implementácii neadresných bezpečnostných opatrení a technológií či dokonca k pravdepodobnejšiemu scenáru zanedbávania kybernetickej bezpečnosti.

Z pohľadu kybernetických bezpečnostných incidentov väčšina opýtaných organizácii neevidovala žiadne. V ostatných prípadoch išlo najčastejšie o menej závažné incidenty s minimálnymi finančnými škodami, ktoré boli vyriešené do jedného dňa. Vzhľadom na vyššie uvedené ukazovatele je však na mieste sa domnievať, že situačný prehľad osoby poverenej za vyplnenie dotazníka mohol byť skreslený neschopnosťou detegovať niektoré typy incidentov ako aj absenciou postupov pri ich riešení, ktorá mohla viesť k tomu, že incident nebol nahlásený.

Záverom správy sú odporúčania pre mimovládne neziskové organizácie spolu s užitočnými odkazmi na ich implementáciu.

Tento projekt je podporený z Európskeho sociálneho fondu.

Úvod

Vo viacerých krajinách Európy sú dlhodobo evidované kybernetické útoky zahraničných aktérov proti mimovládnemu sektoru s cieľom zneprístupniť ním poskytované služby alebo exfiltrovať z neho dáta. Pred parlamentnými voľbami v roku 2017 zaznamenalo takéto pokusy proti dvom nadáciám pridruženým k politickým stranám nemecké ministerstvo vnútra v rámci kyberšpionážnej kampane skupiny APT28.[1] Na podobné pokusy o preniknutie do počítačových sietí a e-mailových schránok mimovládnych neziskových organizácií (MNO) upozorňuje od roku 2020 tiež česká Bezpečnostná a informačná služba,[2] pričom uvádza, že s najväčšou pravdepodobnosťou za týmito útokmi stoja štátni, resp. štátom podporovaní aktéri spájaní s Ruskom a Čínou.[3] Od vypuknutia ozbrojeného konfliktu na Ukrajine v roku 2022 zmapovala organizácia CyberPeace Institute celkovo 34 kybernetických útokov proti MNO v Európe, ktoré mali najčastejšie povahu DDoS útokov proti ich webstránkam.[4]

Prehľad o kybernetických útokoch proti mimovládnemu sektoru na Slovensku však chýba. Otvorené zdroje ako napr. štatistiky o hláseniach kybernetických incidentov vo výročných správach Národného bezpečnostného úradu o stave kybernetickej bezpečnosti v SR neuvádzajú mimovládny sektor ako samostatnú kategóriu. Nápad kybernetických útokov proti mimovládnemu sektoru, ktoré napĺňajú skutkovú podstatu trestných činov kybernetickej kriminality a boli nahlásené, sa neuvádza ani v štatistikách Policajného zboru.

Okrem nápadu kybernetických útokov nie je ďalej možné posúdiť ani stav kybernetickej bezpečnosti priamo v MNO. Z prieskumu organizácie PDCS, ktorý bol zrealizovaný v roku 2023 na približne dvoch desiatkach MNO, vyplýva, že len menej ako tretina z nich má vyriešenú otázku bezpečnej správy hesiel, dvojstupňového overovania, aktualizácií či pravidelných záloh.[5] Táto štúdia však opomenula otázky vzdelávania zamestnancov, dodržiavania technických noriem pri implementácii bezpečnostných opatrení či vyhotovenia analýzy rizík. Zahraničné prieskumy realizované napr. vo Veľkej Británii pritom poukazujú na nedostatočné opatrenia v mimovládnom sektore – len 27 % charitatívnych organizácií vypracovalo analýzu kyberbezpečnostných rizík, len 17 % z nich poskytlo zamestnancom školenie alebo osvetovú aktivitu v oblasti kybernetickej bezpečnosti, a len 5 % z nich dodržiavalo technickú normu ISO 27001.[6]

Úrad splnomocnenca vlády SR pre rozvoj občianskej spoločnosti preto v rámci európskeho mesiaca kybernetickej bezpečnosti zrealizoval v októbri 2023 anonymný dotazníkový prieskum o stave kybernetickej bezpečnosti v mimovládnom sektore na Slovensku.

[1] https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/sicherheit/vsb-2017.pdf?__blob=publicationFile&v=11
[2] https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2020-vz-cz-2.pdf
[3] https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2021-vz-cz-2.pdf
[4] https://cyberconflicts.cyberpeaceinstitute.org/threats/timeline
[5] https://backend.en.pdcs.sk/storage/app/media/Projects/Mapovanie_dezinformacii_a_obcianskej_spolocnosti_Slovensko.pdf
[6] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023

Metodika

Nereprezentatívny prieskum bol realizovaný prostredníctvom anonymného elektronického dotazníka vo forme Google formulára. Bol rozdelený do dvoch hlavných častí. V rámci prvej, organizačnej časti sa zisťovali personálne, technické, normatívne, metodické, analytické a finančné predpoklady na zaistenie kybernetickej bezpečnosti. Druhá, procesná časť sa zamerala na skúseností s kybernetickými bezpečnostnými incidentami. Pri tvorbe dotazníka sa vychádzalo z technických a právnych noriem a metodických usmernení vydaných štátnymi inštitúciami SR. Otázky v dotazníku boli polouzatvorené s možnosťou doplnenia alternatívnych možností. Výnimkou bola nepovinná, otvorená otázka na záver, v ktorej mohli respondenti opísať priebeh a okolnosti incidentov, s ktorými mali skúsenosť.

Zber údajov prebiehal od 17. do 31. októbra 2023. Úrad splnomocnenca vlády SR pre rozvoj občianskej spoločnosti elektronicky oslovil so žiadosťou o vyplnenie dotazníka a jeho ďalšiu distribúciu nasieťované mimovládne neziskové organizácie zo svojich databáz. Dodatočne zároveň zverejnil tlačovú správu na webstránke[7] a príspevky na sociálnych sieťach Facebook[8] a Instagram[9] s výzvou na zapojenie sa do zberu údajov. Organizácie boli požiadané, aby dotazník vyplnila osoba zodpovedná za kybernetickú bezpečnosť, príp. osoba z manažmentu.

Respondenti boli následne klastrovaní dvojako. Na jednej strane podľa regiónov SK-NUTS, v ktorom organizácia sídli, a to na Bratislavský kraj, Západné Slovensko, Stredné Slovensko a Východné Slovensko.[10] Na strane druhej podľa veľkosti rozpočtu, s ktorým organizácie operovali v roku 2022, a to na malé (rozpočet nižší ako 100 000 eur), stredné (100 001 až 500 000 eur) a veľké organizácie (nad 500 000 eur).

Návrh dotazníka rovnako ako interpretácia dát bola konzultovaná s Kompetenčným a certifikačným centrom kybernetickej bezpečnosti.

[7] https://www.minv.sk/?ros_vsetky-spravy&sprava=zapojte-sa-do-dotaznikoveho-prieskumu-o-stave-kybernetickej-bezpecnosti-v-mimovladnom-sektore-na-slovensku

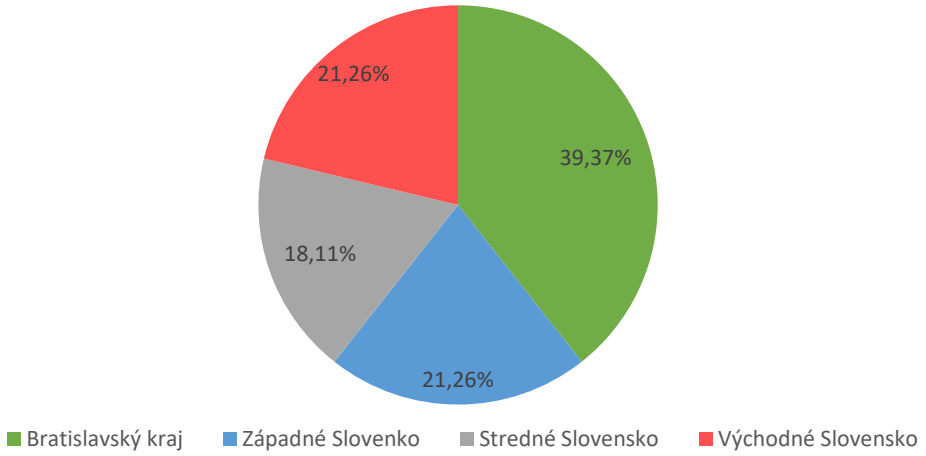
[8] https://www.facebook.com/SplnomocnenecROS/posts/pfbid02yrjUW1uaiwNt3sYyewA5TAufKov2gopx7xvAVePnJsHbHdWet5xi3td1QH44FEepl

[9] https://www.instagram.com/p/Cyx6ZXOImPg/

[10] https://ec.europa.eu/eurostat/web/regions/background

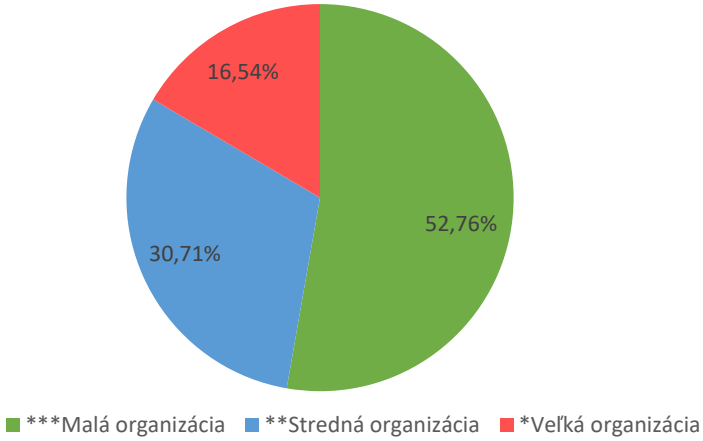
N=127

Profil respondentov podľa regiónu, v ktorom sídli organizácia



N=127

Profil respondentov podľa veľkosti rozpočtu, s ktorým organizácia operovala v roku 2022



* rozpočet vyšší ako 500 000 eur

** rozpočet 100 001 až 500 000 eur

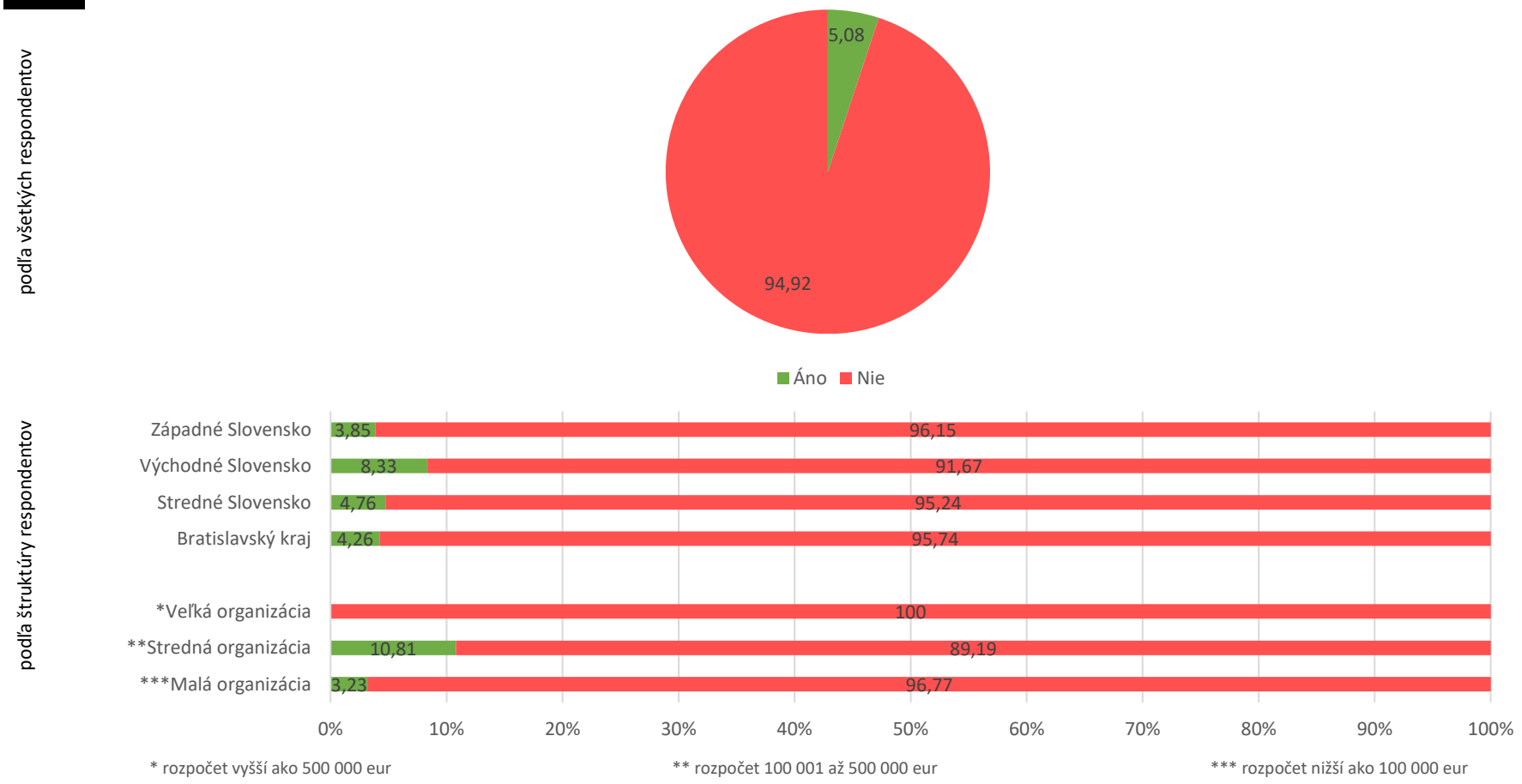
*** rozpočet nižší ako 100 000 eur

Tento projekt je podporený z Európskeho sociálneho fondu.

Stav kybernetickej bezpečnosti

Otázka č. 1: Má organizácia určeného manažéra kybernetickej bezpečnosti?

N=118

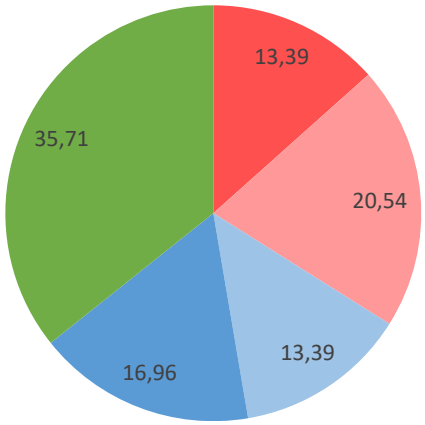


Tento projekt je podporený z Európskeho sociálneho fondu.

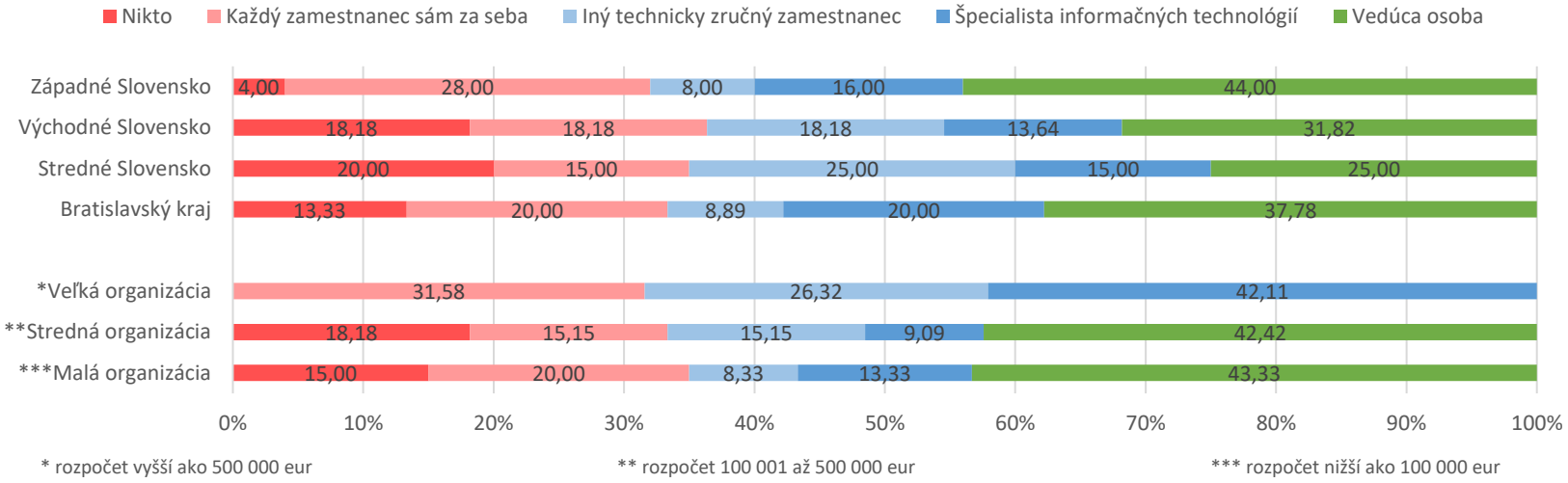
Otázka č. 1.1: Ak nie, kto zodpovedá za kybernetickú bezpečnosť v organizácii?

N=112

podľa všetkých respondentov



podľa štruktúry respondentov



* rozpočet vyšší ako 500 000 eur

** rozpočet 100 001 až 500 000 eur

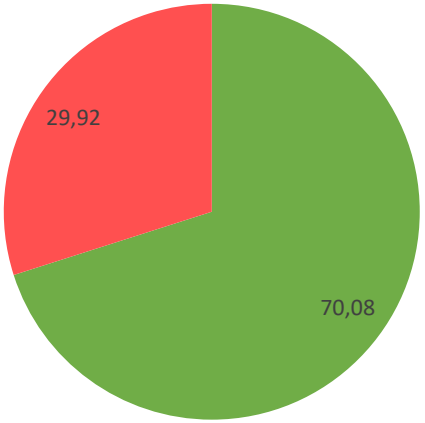
*** rozpočet nižší ako 100 000 eur

Tento projekt je podporený z Európskeho sociálneho fondu.

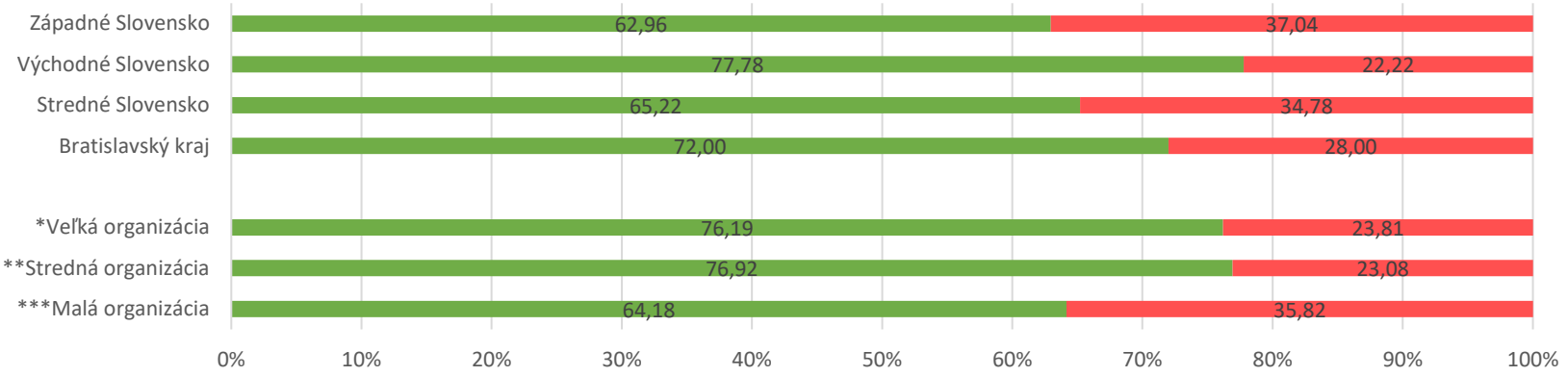
Otázka č. 2: Má organizácia určenú zodpovednú osobu za ochranu osobných údajov?

N=127

podľa všetkých respondentov



podľa štruktúry respondentov



* rozpočet vyšší ako 500 000 eur

** rozpočet 100 001 až 500 000 eur

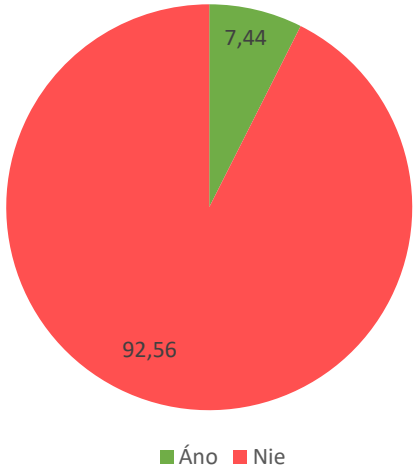
*** rozpočet nižší ako 100 000 eur

Tento projekt je podporený z Európskeho sociálneho fondu.

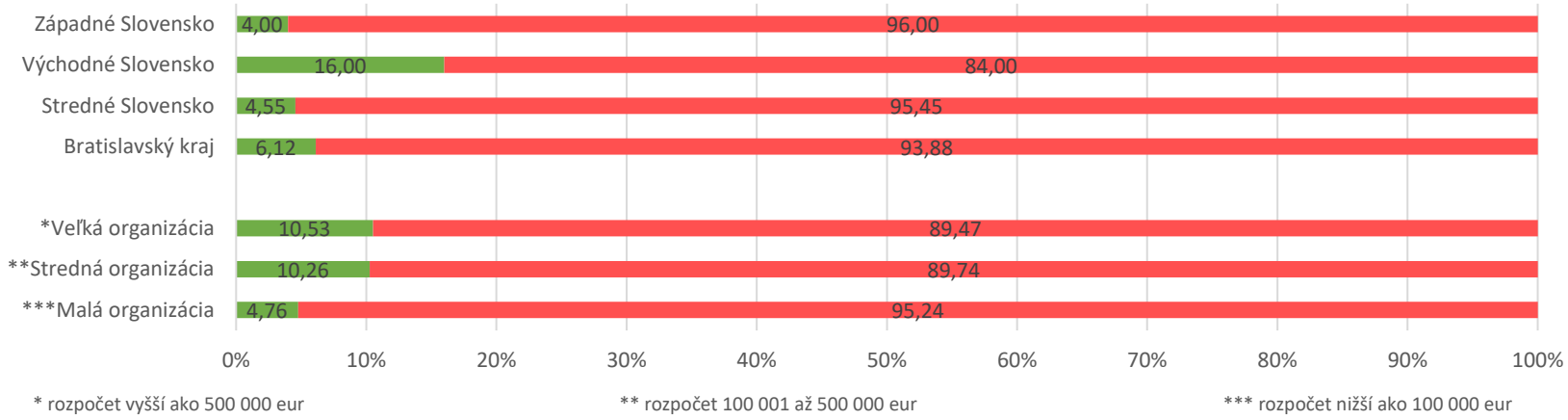
Otázka č. 3: Má vaša organizácia vypracovanú analýzu rizík v oblasti kybernetickej bezpečnosti?

N=121

podľa všetkých respondentov



podľa štruktúry respondentov



* rozpočet vyšší ako 500 000 eur

** rozpočet 100 001 až 500 000 eur

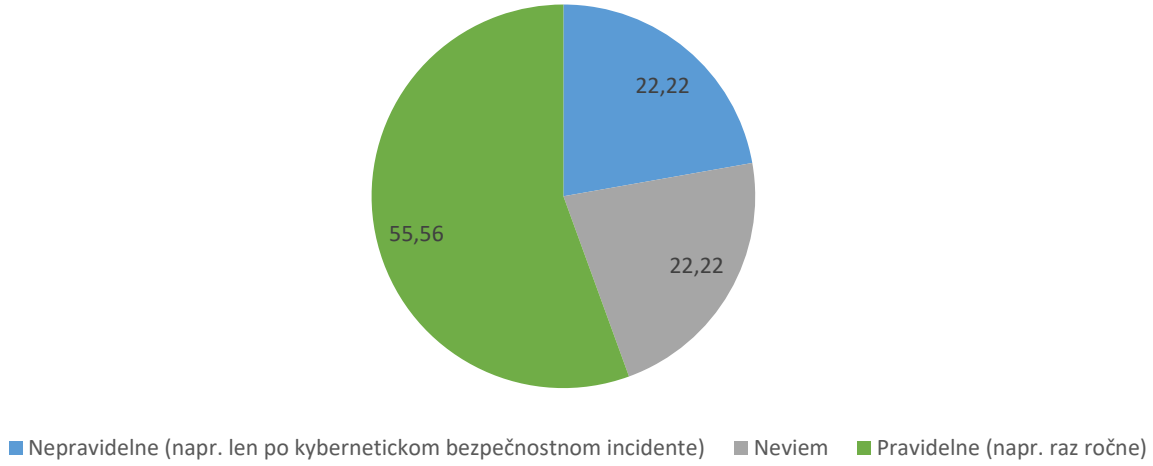
*** rozpočet nižší ako 100 000 eur

Tento projekt je podporený z Európskeho sociálneho fondu.

Otázka č. 3.1: Ak áno, ako často je analýza rizík aktualizovaná?

N=9

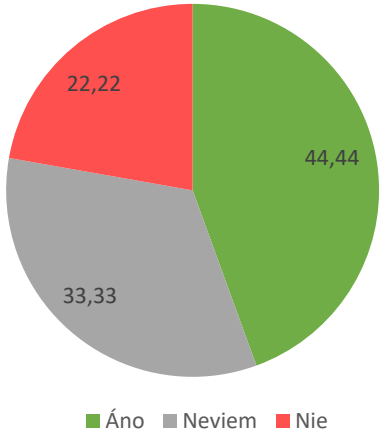
podľa všetkých respondentov



Otázka č. 3.2: Ak áno, je táto analýza založená na štandardizovanom procese riadenia rizík?

N=9

podľa všetkých respondentov

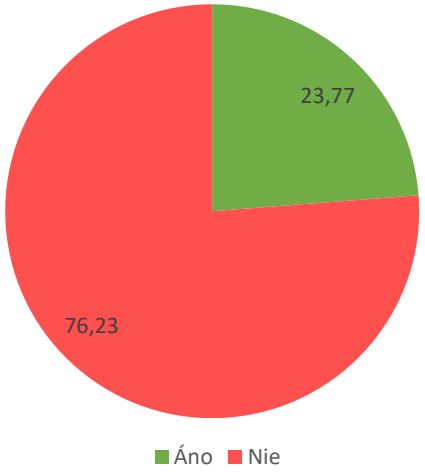


Tento projekt je podporený z Európskeho sociálneho fondu.

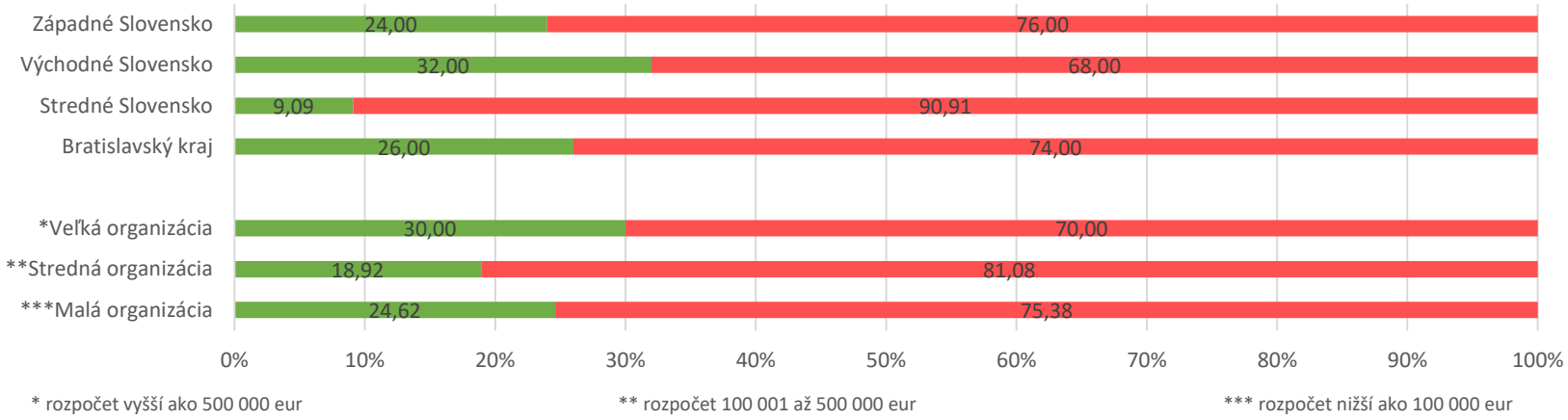
Otázka č. 4: Poskytuje organizácia svojim zamestnancom možnosti školenia na zvyšovanie ich znalostí?

N=122

podľa všetkých respondentov



podľa štruktúry respondentov



* rozpočet vyšší ako 500 000 eur

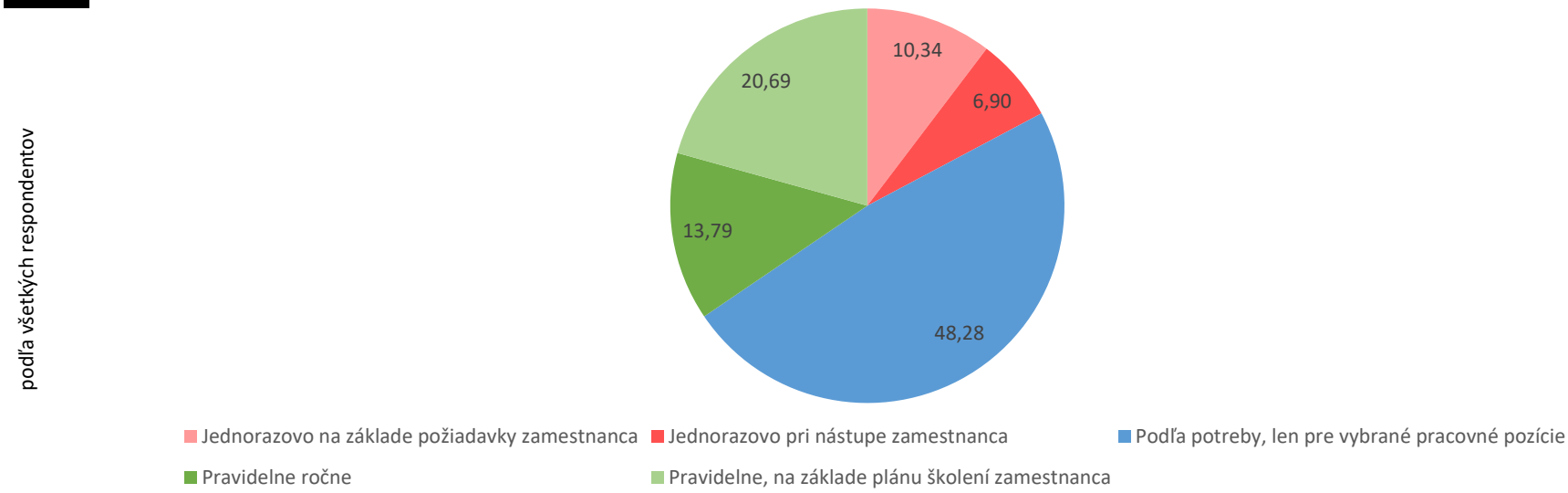
** rozpočet 100 001 až 500 000 eur

*** rozpočet nižší ako 100 000 eur

Tento projekt je podporený z Európskeho sociálneho fondu.

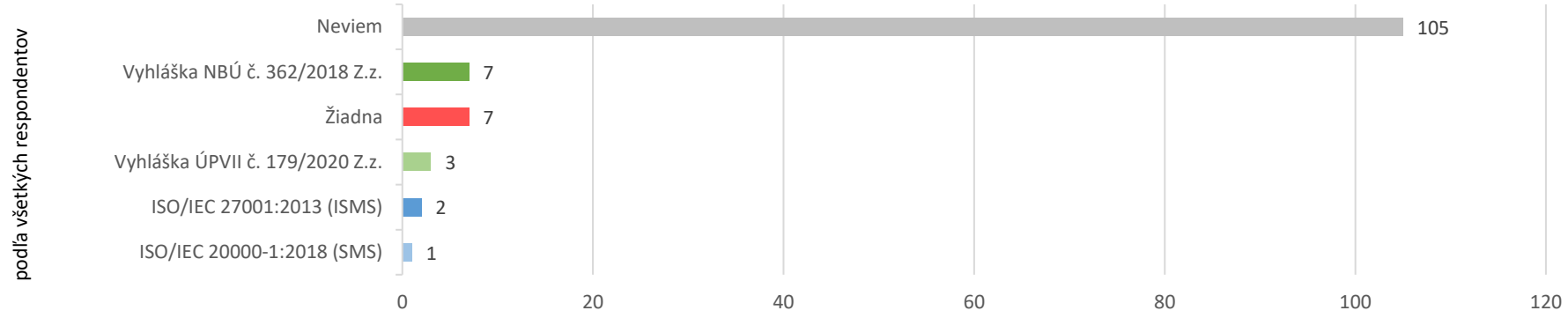
Otázka č. 4.1: Ak áno, na základe akého podnetu, akej požiadavky?

N=29



Otázka č. 5: Podľa ktorej technickej alebo právnej normy postupuje organizácia pri implementácii bezpečnostných opatrení v kybernetickej bezpečnosti?

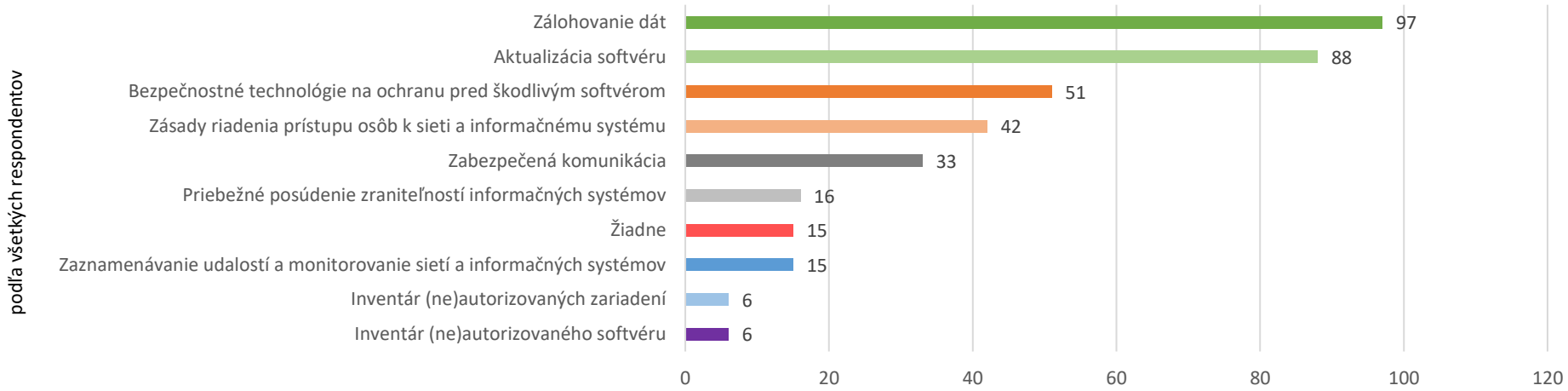
N=125



Tento projekt je podporený z Európskeho sociálneho fondu.

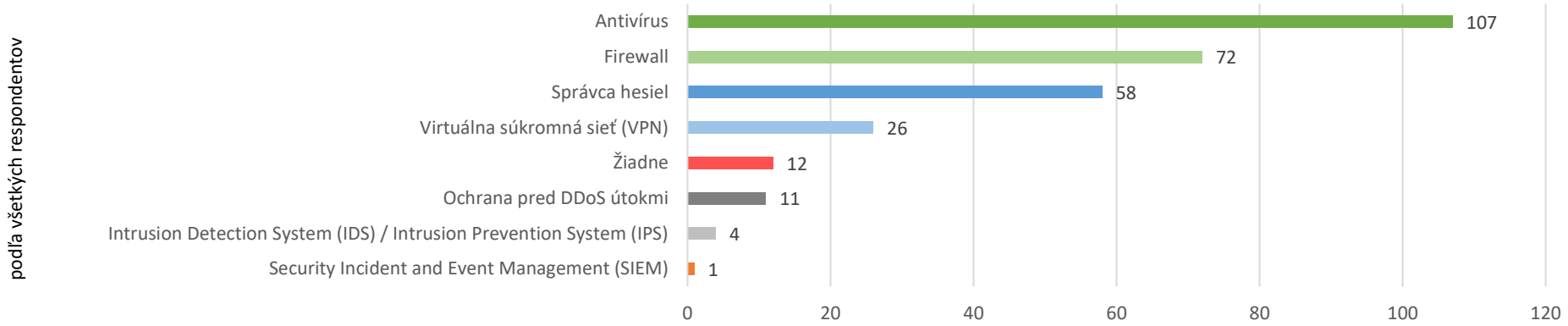
Otázka č. 6: Ktoré z nasledujúcich bezpečnostných opatrení organizácia aplikuje?

N=127



Otázka č. 7: Ktoré z nasledujúcich bezpečnostných technológií organizácia používa?

N=127

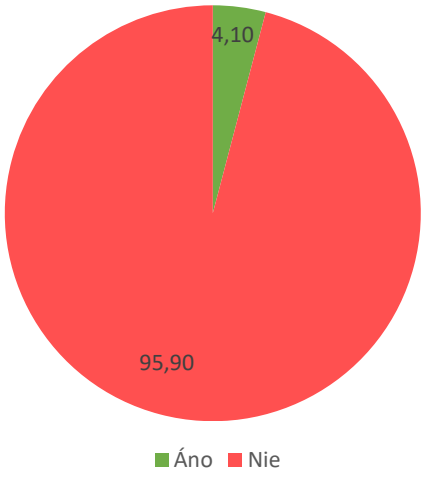


Tento projekt je podporený z Európskeho sociálneho fondu.

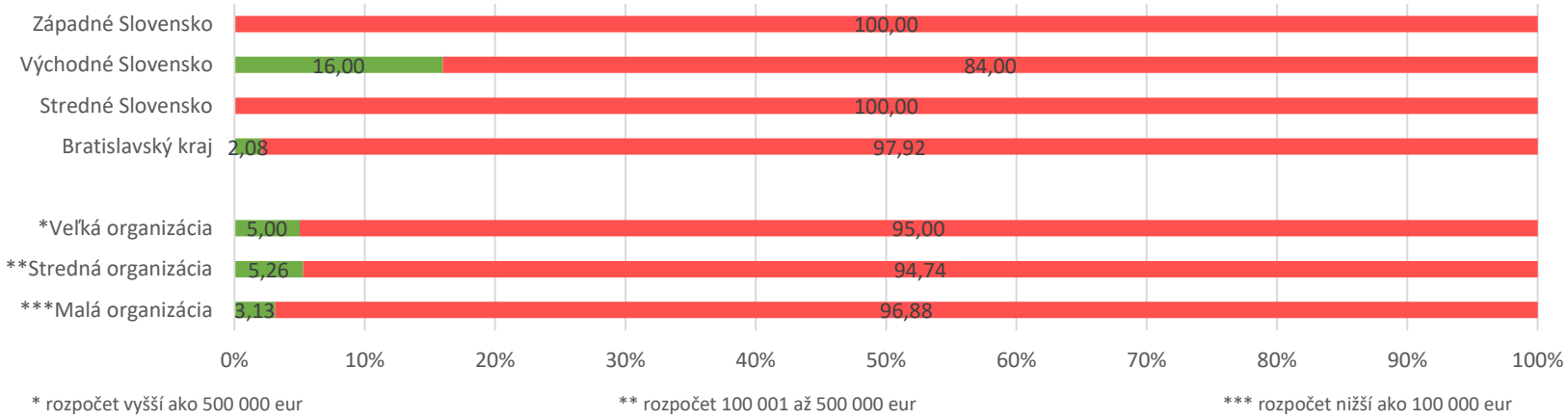
Otázka č. 8: Je rozpočet na kybernetickú bezpečnosť súčasťou rozpočtu organizácie ako samostatná časť

N=122

podľa všetkých respondentov



podľa štruktúry respondentov



* rozpočet vyšší ako 500 000 eur

** rozpočet 100 001 až 500 000 eur

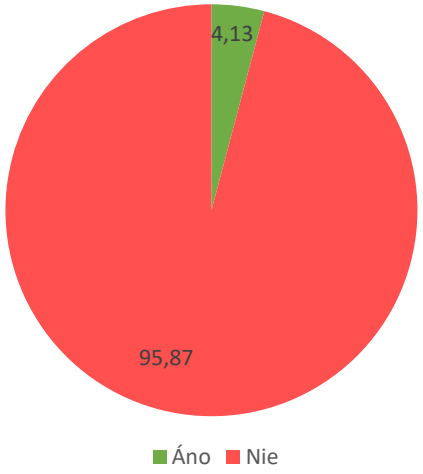
*** rozpočet nižší ako 100 000 eur

Tento projekt je podporený z Európskeho sociálneho fondu.

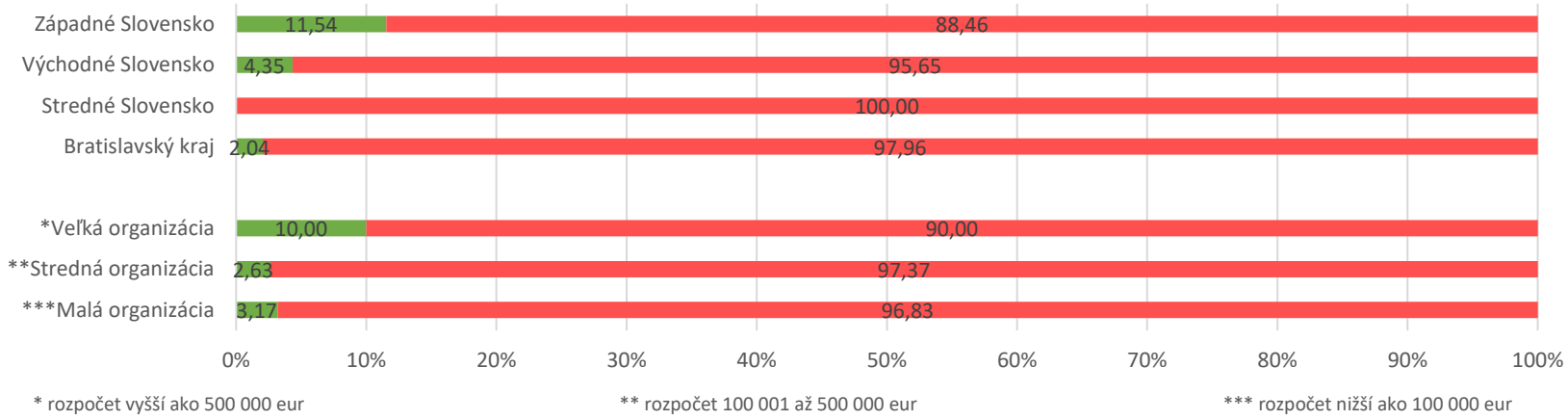
Otázka č. 9: Má organizácia vypracované štandardy a postupy riešenia kybernetických bezpečnostných incidentov?

N=121

podľa všetkých respondentov



podľa štruktúry respondentov



* rozpočet vyšší ako 500 000 eur

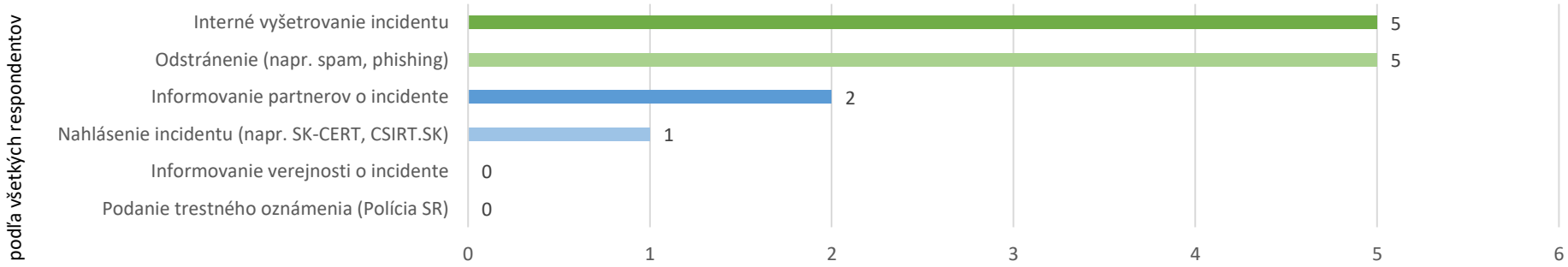
** rozpočet 100 001 až 500 000 eur

*** rozpočet nižší ako 100 000 eur

Tento projekt je podporený z Európskeho sociálneho fondu.

Otázka č. 9.1: Ak áno, akým spôsobom organizácia rieši incident?

N=5

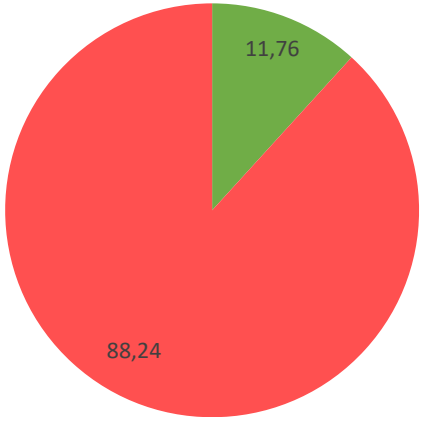


Prehľad kybernetických bezpečnostných incidentov

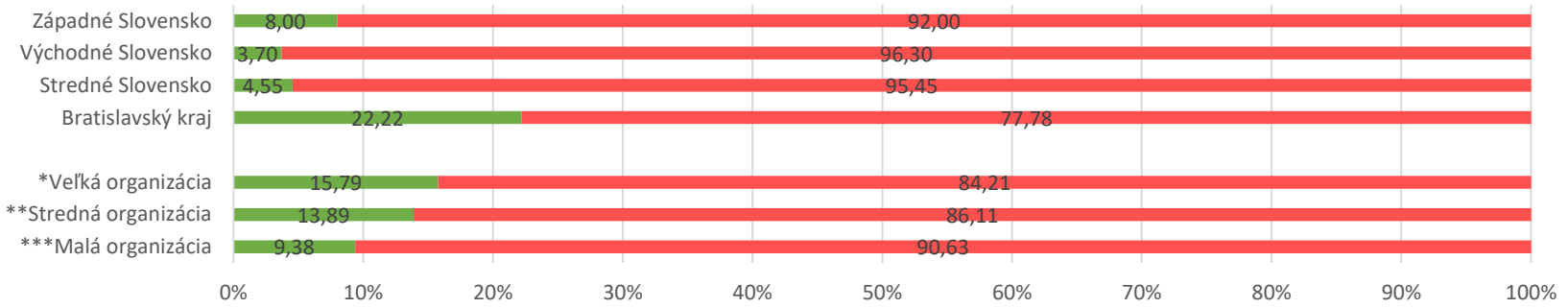
Otázka č. 10: Zaznamenala organizácia kyberbezpečnostné incidenty od začiatku roku 2023?

N=119

podľa všetkých respondentov



podľa štruktúry respondentov



* rozpočet vyšší ako 500 000 eur

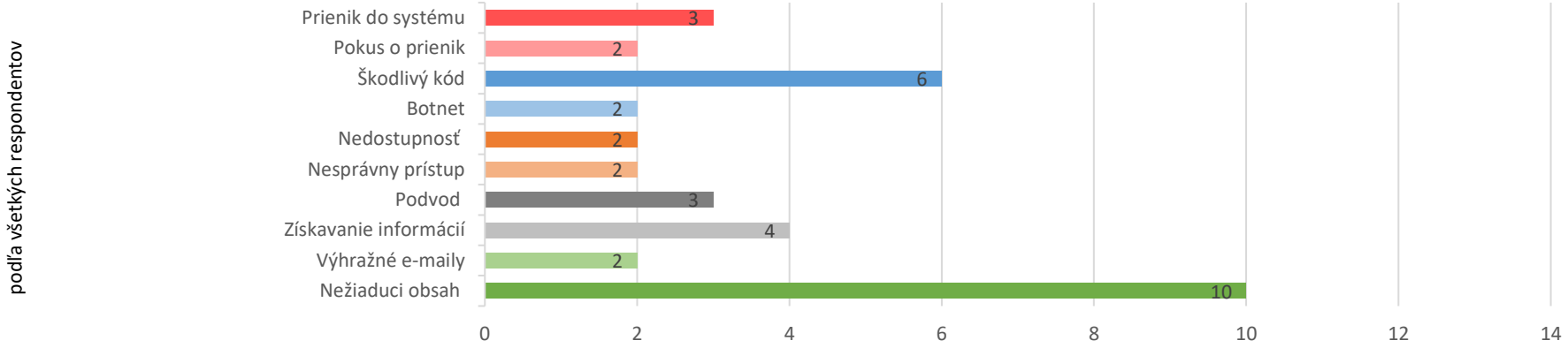
** rozpočet 100 001 až 500 000 eur

*** rozpočet nižší ako 100 000 eur

Tento projekt je podporený z Európskeho sociálneho fondu.

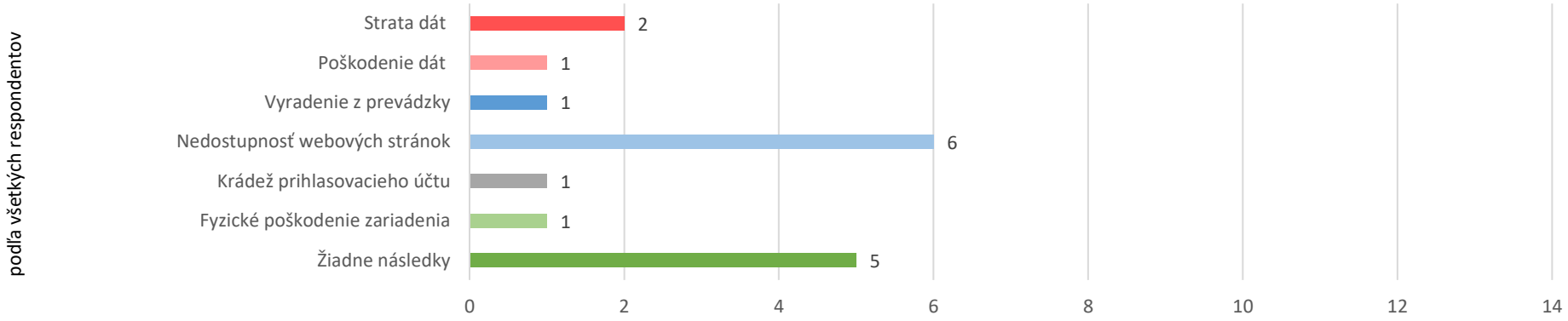
Otázka č. 10.1: Ak áno, o aké typy incidentov sa jednalo?

N=14



Otázka č. 10.2: Ak áno, aké následky mali incidenty?

N=14

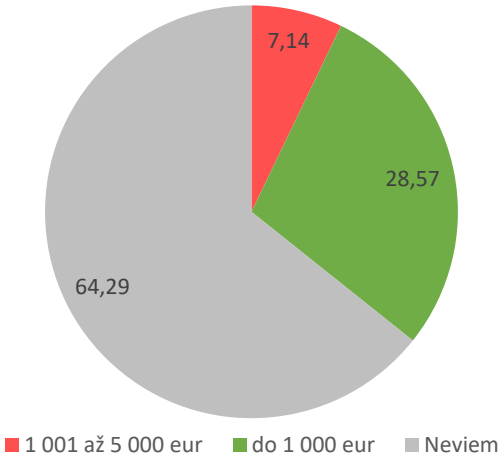


Tento projekt je podporený z Európskeho sociálneho fondu.

Otázka č. 10.3: Ak áno, akú škodu incidenty spôsobili?

N=14

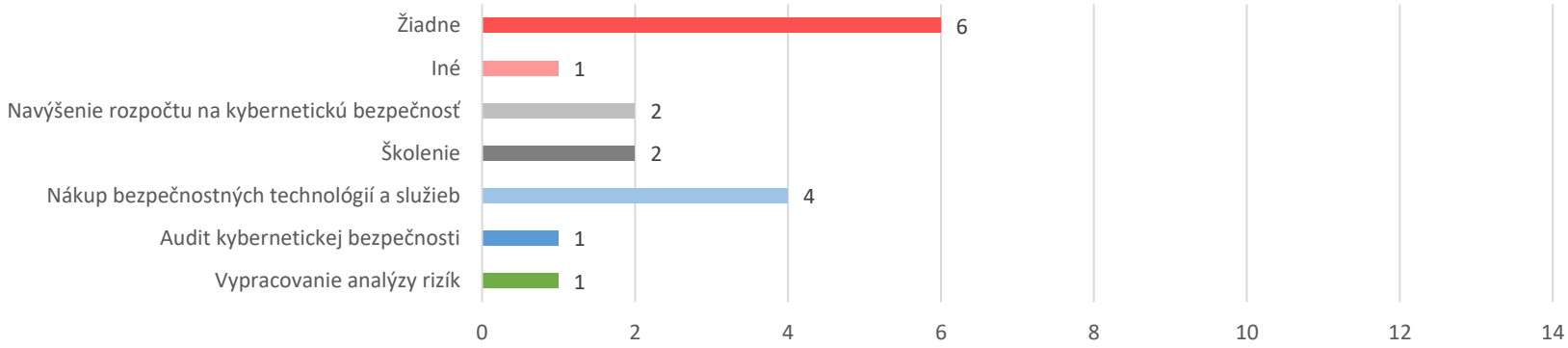
podľa všetkých respondentov



Otázka č. 10.4: Ak áno, aké následné opatrenia prijala organizácia po kybernetickom bezpečnostnom incidente?

N=14

podľa všetkých respondentov

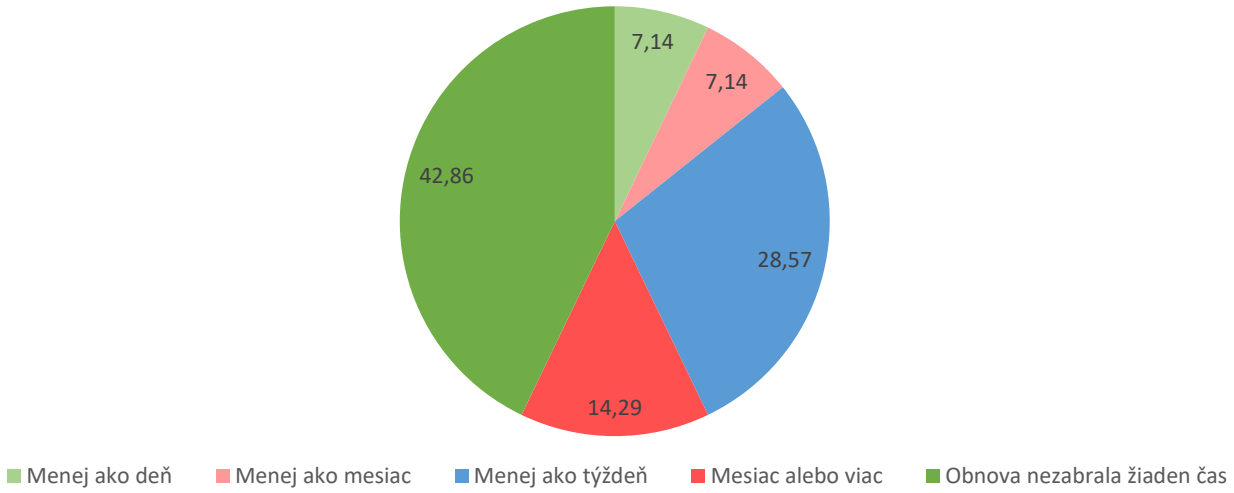


Tento projekt je podporený z Európskeho sociálneho fondu.

Otázka č. 10.5: Ak áno, ako dlho trvala obnova činnosti organizácie po kybernetickom bezpečnostnom incidente?

N=14

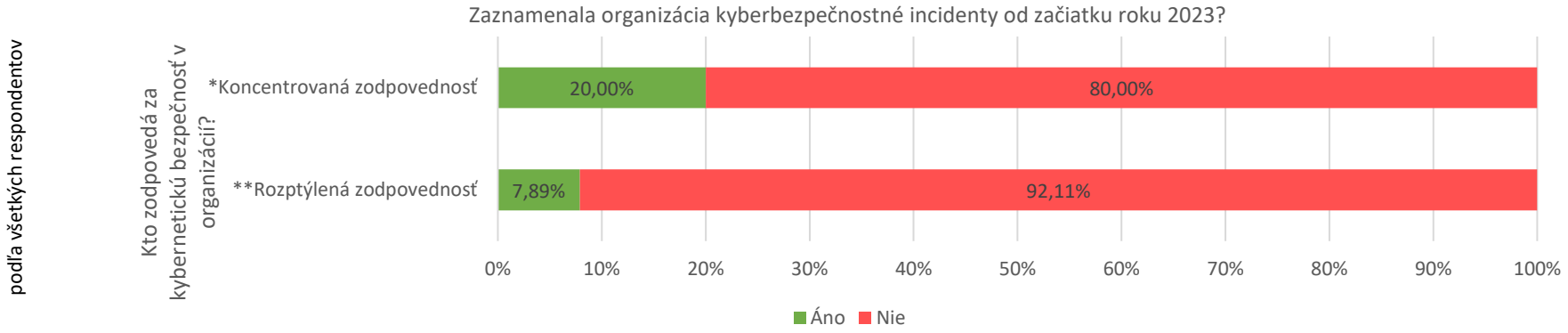
podľa všetkých respondentov



Vybrané ukazovatele

Zodpovednosť za riadenie vs. evidencia kybernetických bezpečnostných incidentov

N=118



* Vedúca osoba, špecialista informačných technológií alebo iný technicky zručný zamestnanec

** Nikto alebo každý zamestnanec sám za seba

Tento projekt je podporený z Európskeho sociálneho fondu.

Diskusia

Výsledky prieskumu ukazujú, že mimovládne neziskové organizácie neboli v roku 2023 na riadenie kybernetickej bezpečnosti, poťažmo zvládanie kybernetických bezpečnostných incidentov, pripravené po finančnej, metodickej, analytickej ani normatívnej stránke. Drvivej väčšine organizácii chýbala samostatná kapitola pre kybernetickú bezpečnosť v rozpočte (96 %), postupy pri riešení incidentov (96 %) a vypracovanie analýzy rizík (93 %). Väčšina organizácií tiež nepostupovala alebo nevedela odpovedať či sa pri implementácii bezpečnostných opatrení riadila právnymi alebo technickými normami (90 %). Zmienené nedostatky môžu v konečnom dôsledku kumulatívne viesť k skreslenému situačnému prehľadu o hrozbách, ktorým organizácia čelí, a implementácii neadresných bezpečnostných opatrení a technológií či dokonca zanedbávaniu kybernetickej bezpečnosti, ktoré sa s prihliadnutím na ďalšie nižšie uvedené ukazovatele javí ako pravdepodobnejší scenár.

Po technickej stránke mala väčšina organizácii implementované len niektoré základné bezpečnostné opatrenia a technológie ako zálohovanie dát (76 %) a aktualizácia softvéru (69 %), resp. antivírus (84 %) a firewall (57 %). Absentovali však ďalšie dôležité opatrenia ako zásady riadenia prístupu osôb k sieti a informačným systémom (33 %), zaznamenávanie udalostí (12 %) či inventáre (ne)autorizovaných zariadení a softvéru (zhodne po 5 %). Tieto opatrenia pritom súvisia so znižovaním rizík bežnej každodennej praxe a správania zamestnancov ako napr. s používaním súkromných zariadení na pracovné účely, ku ktorým môžu mať prístup viacerí členovia v domácnosti, či s používaním nelicencovaných, cracknutých verzií softvéru stiahnutých z internetu.

V menšej, ale nie menej podstatnej miere chýbali tiež po edukatívnej stránke školenia zamestnancov na posilňovanie ich zručností a znalostí v oblasti kybernetickej bezpečnosti (76 %), ako aj po personálnej stránke zodpovedné osoby určené za riadenie kybernetickej bezpečnosti (32 %) a ochranu osobných údajov (30 %). Koncentrácia zodpovednosti za riadenie kybernetickej bezpečnosti v rukách jednej osoby mala pritom u sledovaných organizácií pozitívny vplyv na druhú sledovanú oblasť, a to na vyššiu evidenciu kybernetických bezpečnostných incidentov.

Napriek tomu však väčšina opýtaných mimovládnych neziskových organizácií nemala v roku 2023 skúsenosti s kybernetickými bezpečnostnými incidentami (88 %). V ostatných prípadoch išlo najčastejšie o incidenty typu nežiadúci obsah a škodlivé kódy. Osobitne za zmienku stoja špecifické prípady z Bratislavského kraja, v ktorom organizácie čelili tiež výhražným e-mailom, krádeži súkromného účtu riaditeľa organizácie na sociálnej sieti či prieniku do systému s cieľom zresetovať záložný server.

Incidenty najčastejšie viedli k nedostupnosti webstránok a spôsobili minimálne škody za menej ako 5 000 eur. Najdlhšia obnova činnosti, ktorá zabrala viac ako mesiac, sa týkala webstránky napadnutej škodlivým kódom, ktorý presmerovával návštevníkov na iný web. Napadnutá organizácia v tomto prípade paralelne s riešením starého webu, ktorý dovtedy nikto nespravoval, začala pripravovať nový pod správou dobrovoľníkov.

Vzhľadom na vysokú absenciu interných predpisov o postupoch riešenia kybernetických bezpečnostných incidentov ako aj absenciu zaznamenávania udalostí v sieťach a informačných systémov a niektoré technológie je však na mieste sa domnievať, že osoba poverená vyplnením dotazníka nemusela disponovať informáciami o všetkých incidentoch, s ktorými sa organizácia, resp. jej zamestnanci, v roku 2023 potýkali. V takých prípadoch nemuseli byť niektoré typy incidentov detegované, ako napr. škodlivé kódy alebo botnet, alebo nahlásené tejto osobe, ako napr. podvod, získavanie informácií či pokus o prienik.

Záver

Mimovládny sektor na Slovensku nebol v roku 2023 v oblasti kybernetickej bezpečnosti pripravený predovšetkým po finančnej, metodickej, analytickej a normatívnej stránke. Značná časť organizácií zapojených do prieskumu tiež neposkytovala školenia pre svojich zamestnancov a nemala určené osoby zodpovedné za riadenie kybernetickej bezpečnosti ani ochranu osobných údajov. Po technickej stránke organizácie implementovali len niektoré základné bezpečnostné opatrenia a technológie. Z pohľadu kybernetických bezpečnostných incidentov väčšina opýtaných organizácii neevidovala žiadne. V ostatných prípadoch išlo najčastejšie o menej závažné incidenty s minimálnymi finančnými škodami, ktoré boli vyriešené do jedného dňa.

Odporúčania pre mimovládne neziskové organizácie

1. Určiť jednu zodpovednú osobu za riadenie kybernetickej bezpečnosti v organizácií spomedzi dostupných personálnych kapacít.
2. Vyčleniť pre zodpovednú osobu za riadenie kybernetickej bezpečnosti samostatnú kapitolu v rozpočte organizácie na vzdelávanie, implementáciu bezpečnostných opatrení a technológií či konzultácie s odborníkmi v prípade, že ona sama ňou nie je.
3. Zabezpečiť implementáciu odporúčaní zodpovednej osoby za ochranu osobných údajov.
4. Vypracovať analýzu rizík v oblasti kybernetickej bezpečnosti.
5. Zvážiť preventívne posilnenie ochrany webstránok pred škodlivými kódmi a útokmi na odopretie služby.
6. Vypracovať zásady riadenia prístupu osôb k sieti a informačným systémom, a to najmä s prihliadnutím na fluktuáciu zamestnancov, stážistov, dobrovoľníkov a návštevníkov v organizácii a jej sídle.
7. Vypracovať inventár (ne)autorizovaných zariadení a softvéru, a to najmä s prihliadnutím na politiku „bring your own device“ a používanie súkromných zariadení na pracovné účely.
8. Vypracovať postupy pri riešení kybernetických bezpečnostných incidentov.
9. Viesť si evidenciu kybernetických bezpečnostných incidentov.
10. Informovať štátne orgány o kybernetických bezpečnostných incidentoch. V prípade potreby aj partnerov, na ktorých mohol mať incident vplyv, alebo verejnosť.

Tento projekt je podporený z Európskeho sociálneho fondu.

Užitočné odkazy

Oblasť	Inštitúcia	Názov	Odkaz	Poznámka
Osveta a vzdelávanie	Odbor počítačovej kriminality, Prezídium Policajného zboru	Infografiky	www.minv.sk/?pocitacova-kriminalita	Infografiky k rôznym druhom podvodov, phishingu, smishingu a ransomvérom.
	CSIRT.SK	Phishingový test	www.csirt.gov.sk/archiv/osvedcene-postupy/navody-a-odporucania/phishingovy-test-871.html?csrt=16549278073353684665	17 testovacích otázok na rozpoznanie a odhalenie falošných e-mailov
Riadenie kybernetickej bezpečnosti	Kompetenčné a certifikačné centrum kybernetickej bezpečnosti	Knižnica	www.cybercompetence.sk/kniznica	Letáky, brožúry a metodiky k základným bezpečnostným opatreniam, vypracovaniu analýzy rizík v oblasti kybernetickej bezpečnosti či výberu dodávateľa služieb kybernetickej bezpečnosti.
Riešenie kybernetických bezpečnostných incidentov	SK-CERT	Nahlasovanie incidentov	www.sk-cert.sk/sk/rady-a-navody/kedy-nas-kontaktovat/index.html	E-mailová adresa pre dobrovoľné nahlasovanie kybernetických bezpečnostných incidentov.
	Odbor prevencie kriminality, Ministerstvo vnútra SR	Informačné kancelárie pre obete trestných činov	www.minv.sk/?narodny-projekt-zlepsenie-pristupu-obeti-trestnych-cinov-k-sluzbam-a-vytvorenie-kontaktnych-bodov-pre-obete-o-projekte	Právna, sociálna a psychologická pomoc pre obete trestných činov, napr. podvodov.
	EUROPOL; Holandská polícia	No More Ransom!	www.nomoreransom.org/sk/index.html	Webstránka, ktorej cieľom je pomôcť obetiam ransomvéru získať ich zašifrované dáta späť bez nutnosti platiť zločincom.

Tento projekt je podporený z Európskeho sociálneho fondu.