NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

SPRÁVA O KYBERNETICKEJ BEZPEČNOSTI

v Slovenskej republike v roku 2022

NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

SPRÁVA O KYBERNETICKEJ BEZPEČNOSTI

v Slovenskej republike
v roku 2022

OBSAH

1 ÚVOD

Rok 2022 nám ukázal, že kybernetická vojna sa stala esenciálnou súčasťou našej spoločnosti. Kybernetické útoky nie sú výmyslom technologických nadšencov. Sú aktívne využívané vo vojenských konfliktoch, napríklad vo vojne Ruska proti Ukrajine, spravodajských hrách aj v kriminálnych aktivitách.

Správa o kybernetickej bezpečnosti v Slovenskej republike v roku 2022 ilustruje stav v tejto oblasti z globálneho a národného pohľadu. Venuje sa najvýznamnejším udalostiam a hrozbám a na základe získaných dát sa pokúša zhodnotiť aktivity a výsledky relevantných subjektov.

Údaje pochádzajú z činnosti Národného centra kybernetickej bezpečnosti SK-CERT, Kompetenčného a certifikačného centra kybernetickej bezpečnosti (KCCKB) a iných relevantných subjektov, najmä pri sektorovom pohľade na problematiku. Pokrývajú aj globálne trendy za rok 2022, pohľad na hrozby a incidenty v slovenskom kybernetickom priestore či informácie o vzdelávaní a aktivitách v tejto oblasti.

Minulý rok bol príznačný najmä začiatkom vojny Ruska proti Ukrajine. Kybernetické útoky, spojené s touto vojnou, neboli izolované len na územie okupovanej Ukrajiny, ale zasiahli viaceré štáty a to najmä tie, ktoré aktívne vojensky a humanitárne podporovali Ukrajinu. Rok 2022 nám naplno ukázal, že dobré vyhodnocovanie a riadenie rizík, dôsledná implementácia bezpečnostných opatrení a vzájomná spolupráca je cestou k úspechu.

2 PREHĽAD HROZIEB A INCIDENTOV ZA ROK 2022

Globálny kybernetický priestor v roku 2022 bol najvýznamnejšie ovplyvnený vojnou Ruska proti Ukrajine. Okrem použitia konvenčných zbraní vo fyzickom svete priniesla aj spustenie kybernetických operácií – už pred vypuknutím vojny.

2.1 Vojna Ruska proti Ukrajine

Pred konfliktom ruská strana vykonávala kybernetické ofenzívne operácie, ktoré mali spôsobiť narušenie fungovania služieb a funkcií štátnych organizácií a kritickej infraštruktúry. Po vypuknutí konfliktu sa väčšina existujúcich hackerských skupín v regióne pridala na niektorú zo zapojených strán, zvyšok si však zachoval svoje štandardné operačné modely.

Počas vojny sa objavili aj nové komunitné hackerské hnutia. Jedno z prvých bola iniciatíva skupiny KILLNET, ktorá založila komunitné hnutie LEGION. Ide o unikátne zoskupenia, ktoré si vymieňajú informácie, know-how, zdieľanie skriptov, programov a licencií k programom.

Rôznorodé skupiny ľudí sa postupne transformovali do organizovaných skupín s hierarchickým riadením a špecializáciou. Koordinovali sa cez sociálne siete, najmä na komunikačnej platforme Telegram, čo prispelo aj k zapojeniu sympatizujúcej verejnosti do útokov.

Komunitné hnutia sa zameriavali na hackerské útoky na rôzne ciele nielen na Ukrajine, ale aj v krajinách, ktoré aktívne a verejne podporovali Ukrajinu humanitárne alebo vojensky. Išlo najmä o členské krajiny EÚ a NATO, vrátane Slovenskej republiky.

Najpočetnejšou aktivitou hackerských skupín a komunitných hnutí boli DDoS útoky, ktoré mali za cieľ spôsobiť zneprístupnenie webových stránok a služieb. Voľba cieľov DDoS útokov bola naviazaná na udalosti v reálnom svete ako darovanie vojenského materiálu alebo otvorená kritika Ruska. Voľba cieľov DDoS útokov však nebola vždy najsofistikovanejšia. Útočníci sa prevažne sústredili na webové stránky štátnych organizácií (v niektorých prípadoch aj súkromných spoločností), ktorých nedostupnosť mala skôr reputačné následky než praktické dôsledky na fungovanie štátu a občanov. Postupom času však bolo možné vidieť nárast sofistikovanosti výberu cieľov, taktiky, techník a nástrojov používaných útočníkom. V niektorých prípadoch DDoS útoky slúžili ako zastierací manéver pre iné typy útokov, napríklad pokusov o prienik alebo úspešných prienikov do systémov.

2.2 Všeobecné globálne trendy

Na fungovanie jednotlivcov a organizácií má stále najväčšie dôsledky infekcia ransomvérom. V tejto oblasti pokračuje aktivita profesionálnych gangov poskytujúcich ransomvér ako službu.

Vstupný vektor do systémov je vo väčšine prípadov **únik alebo získanie prihlasovacích údajov** do RDP alebo VPN niektorého zo zamestnancov spoločností (naďalej podporované trendom prechodu na home office) alebo **zneužitie zraniteľností** zariadení alebo systémov voľne dostupných z internetu.

Inovácie ransomvérového škodlivého kódu sú majoritne vo forme **vylepšovania používaných funkcionalít** (napr. zvýšenie rýchlosti šifrovania, lepšie maskovanie exfiltrácie dát).

V boji proti ransomvéru významne **pomohli úniky komunikácie Conti ransomware** zo začiatku roka 2022, ktoré poukázali na modus operandi útočníkov (napr. štruktúra hierarchie, používané procesy a postupy). Úspešné **gangy menia svoje mená**, aby zmiatli bezpečnostné zložky.

Ransomvérový útok je zvyčajne vykonávaný ručne a útočník pri mapovaní systému obete môže získať prístupy aj ku systémom dodávateľov (v niekoľkých prípadoch aj lepšie zabezpečených), čo môže prerásť do útokov na dodávateľský reťazec.

Najvýznamnejším vstupným vektorom do siete spoločnosti je naďalej **phishing** v rôznych formách. Obeti príde správa so žiadosťou o overenie hesla, ktorá ju presmeruje na webstránku pod kontrolou útočníka. Pri cielených útokoch (spearphishing) môže webstránka vyzerať ako presná kópia prihlasovacieho webu, na ktorý je obeť zvyknutá, alebo sa na ňu môže podobať. Na zvýšenie podobnosti útočníci zneužívali napr. jednoduchý nástroj na tvorbu phishingu „Logo Kit", ktorý prihlasovaciu obrazovku personalizoval na základe e-mailovej adresy obete (preberal logo domény extrahovanej z e-mailovej adresy obete). Novšou témou bolo v roku 2022 využívanie **decentralizovaných/zdieľaných sietí** na hostovanie phishingového obsahu – napr. IPFS siete. Útočníci tento prístup začali využívať aj vďaka tomu, že provideri cloudových úložísk začali ponúkať IPFS služby.

Na obchádzanie bezpečnostných prvkov sú naďalej zneužívané skracovače URL adries. **Skracovače** je síce možné zablokovať bezpečnostnými prvkami (automatickým odstraňovaním e-mailového obsahu), ale sú natoľko populárne a využívané, že tento spôsob zabezpečenia firmy nepreferujú a v procesoch riešenia incidentov sa zameriavajú na blokovanie a nahlasovanie konkrétnych URL.

Útočníci zneužívali aktuálne geopolitické dianie ako naratívy phishingových kampaní podobne ako v minulosti. Zneužívali sa majoritne témy utečencov a téma vojny Ruska proti Ukrajine.

V tematike sociálneho inžinierstva vyšla do popredia technológia deep fake. Do povedomia spoločnosti sa dostala po vytvorení falošného videa prezidenta Zelenského, v ktorom vyzýval na vojenskú kapituláciu.

Vo vojne Ruska proti Ukrajine bolo sociálne inžinierstvo využívané aj ako metóda na získanie podkladov pre technickú analýzu a bojové operácie (napr. ukrajinské agentky pod zámienkou ponúkania sexuálnych služieb od ruských vojakov požadovali zaslanie fotiek, ktoré boli následne lokalizované a využité na precízne raketové útoky).

Významnou zmenou v oblasti sociálneho inžinierstva bolo novembrové sprístupnenie modelu ChatGPT, ktoré kyberzločinci začali zneužívať na tvorbu phishingových e-mailov. Naďalej sa využíva aj SEO optimalizácia phishingových stránok, ktorou sa útočníci snažia dostať do popredia vyhľadávacích nástrojov ako google.com a duckduckgo.com (tzv. SEO poisoning). Zneužívané bolo aj platenie reklám, ktoré webové stránky s phishingovým alebo škodlivým obsahom posunú na popredné miesto daného vyhľadávača. Počas malwaretrisement kampaní útočníci zneužili identitu populárnych nástrojov a platforiem, ako napr. prehliadač Brave, torrentový klient uTorrent alebo hudobný hosting Audacity.

Okrem vstupných vektorov, medzi ktoré patrí phishing, miskonfigurácie a zraniteľnosti do povedomia vstúpilo aj vytváranie škodlivých **programátorských knižníc** s podobnými menami, ako majú legitímne (tzv. library typosquatting).

Vysoké množstvo krádeží účtov na rôznych platformách bolo zrealizovaných cez tzv. **password spraying**. Primárnym problémom zostáva, že používatelia **nezapínajú dvoj- alebo viacfaktorovú autentifikáciu**. Okrem zraniteľností, ktoré môžu byť použité na obídenie dvoj- a viacfaktorovej autentifikácie, zostáva hrozbou aj bombardovanie výziev na potvrdenie prístupu (tzv. MFA bombing). Tento prístup spočíva v opakovanom zasielaný výziev o potvrdenie dvojfaktorovej autentifikácie. Útočník sa spolieha na nepozornosť, vyčerpanosť alebo jednoduchý preklik zo strany obete alebo obeť spamuje, kým nepodľahne nátlaku.

Microsoft uprostred roka zmenil základné nastavenia svojich Office produktov tak, aby nepovoľovali makrá. Útočníkov táto zmena donútila prejsť na iné formáty – LNK, ISO a RAR. Inovatívny útok vykonala napr. APT skupina Gamaredon, ktorá počas infekcie zariadenia obete **prepísala vzor nového dokumentu v MS Word (Normal.dotm)** tak, aby každý ďalší vytvorený dokument na počítači obete šíril rovnaký malvér.

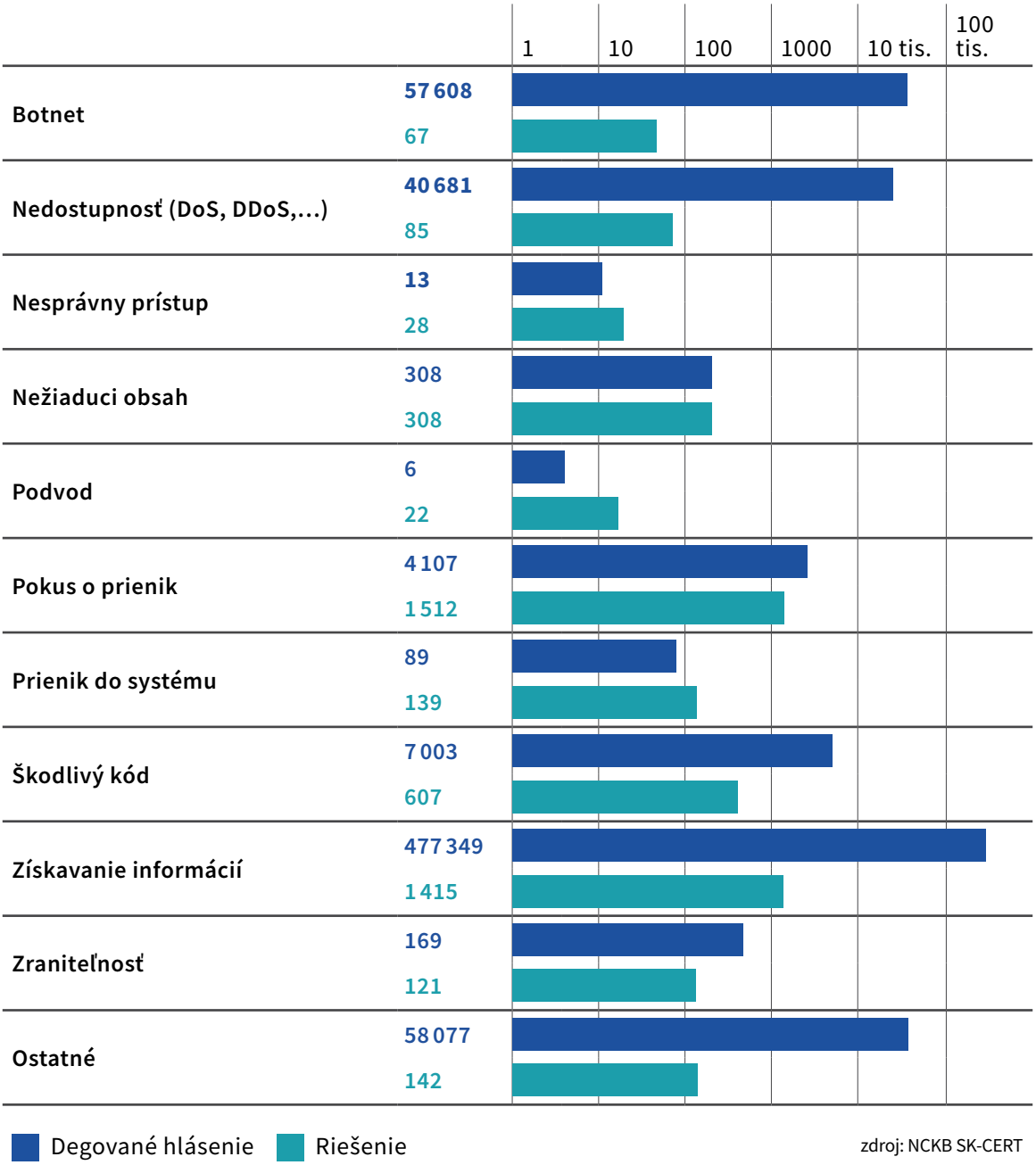
Za najzávažnejšie zraniteľnosti sa dajú v roku 2022 považovať tie, ktoré boli útočníkmi aktívne zneužívané. Medzi tieto zraniteľnosti patria napríklad Log4Shell/Log4j (CVE-2021-44228), zraniteľnosť Google Chrome (CVE-2022-0609), ProxyNotShell (CVE-2022-41040 a CVE-2022-41082) zraniteľnosti umožňujúce vzdialené vykonanie kódu v Microsoft Exchange a Zimbra (CVE-2022-27925 a CVE-2022-41352) a zraniteľnosť Adobe Commerce (CVE-2022-24086).

2.3 Štatistický prehľad incidentov za rok 2022

Národné centrum kybernetickej bezpečnosti SK-CERT ako špecializovaný útvar úradu aj v roku 2022 pokračoval v monitorovaní slovenského kybernetického priestoru. Zbieral, analyzoval a vyhodnocoval získané informácie a prijímal hlásenia o kybernetických bezpečnostných incidentoch.

Na základe získaných informácií, ktoré pochádzajú z vlastnej detekcie, povinných hlásení od PZS a poskytovateľov digitálnych služieb, dobrovoľných hlásení od slovenských firiem, súkromných osôb a partnerov a partnerských organizácií, možno vytvoriť ucelený pohľad na množstvo detegovaných, hlásených a riešených incidentov za rok 2022 podľa typu incidentu.

Množstvo detegovaných, hlásených a riešených incidentov za rok 2021 podľa typu incidentu



zdroj: NCKB SK-CERT

Do grafického zobrazenia štatistík nie sú zahrnuté incidenty, resp. bezpečnostné udalosti v kategórii Nežiaduci obsah, ktoré boli detegované na základe signatúr na bezpečnostných prvkoch. Týchto potencionálnych incidentov, resp. bezpečnostných udalostí bolo za rok 2022 celkovo 48 887 103.

V časovom pohľade bolo najviac incidentov detegovaných a hlásených v mesiaci máj. Najviac riešených incidentov bolo riešených v mesiaci december.

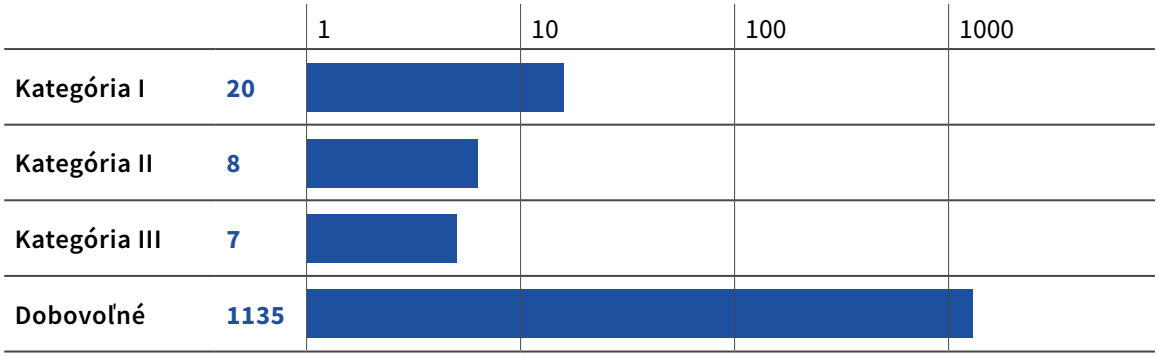
Incidenty z časového hľadiska – rok 2022

zdroj: NCKB SK-CERT

PZS a poskytovatelia digitálnych služieb sú zo zákona povinní hlásiť každý závažný kybernetický bezpečnostný incident. V roku 2022 sme zaznamenali medziročný nárast hlásení o 28 %, avšak išlo hlavne o nárast v oblasti dobrovoľných hlásení kybernetických bezpečnostných incidentov. Považujeme za nevyhnutné, aby sa PZS a poskytovatelia digitálnych služieb viac zameriavali na túto zákonnú povinnosť, pretože plnenie tejto povinnosti stále považujeme za nedostatočnú a to hlavne v najviac zraniteľných sektoroch.

Nedostatky sú viditeľné aj v nesprávnej alebo chýbajúcej klasifikácii kybernetických bezpečnostných incidentov podľa zákona. Problémy s hlásením kybernetických bezpečnostných incidentov vyplývajú najmä zo snáh povinných subjektov vyhnúť sa povinnostiam zo zákona či si tieto povinnosti zjednodušiť, ale aj nedostatočným či neexistujúcim monitoringom, zanedbanými alebo neexistujúcimi procesmi či absolútnou absenciou riadenia kybernetickej bezpečnosti v organizácii, resp. ignorovaním tejto témy.

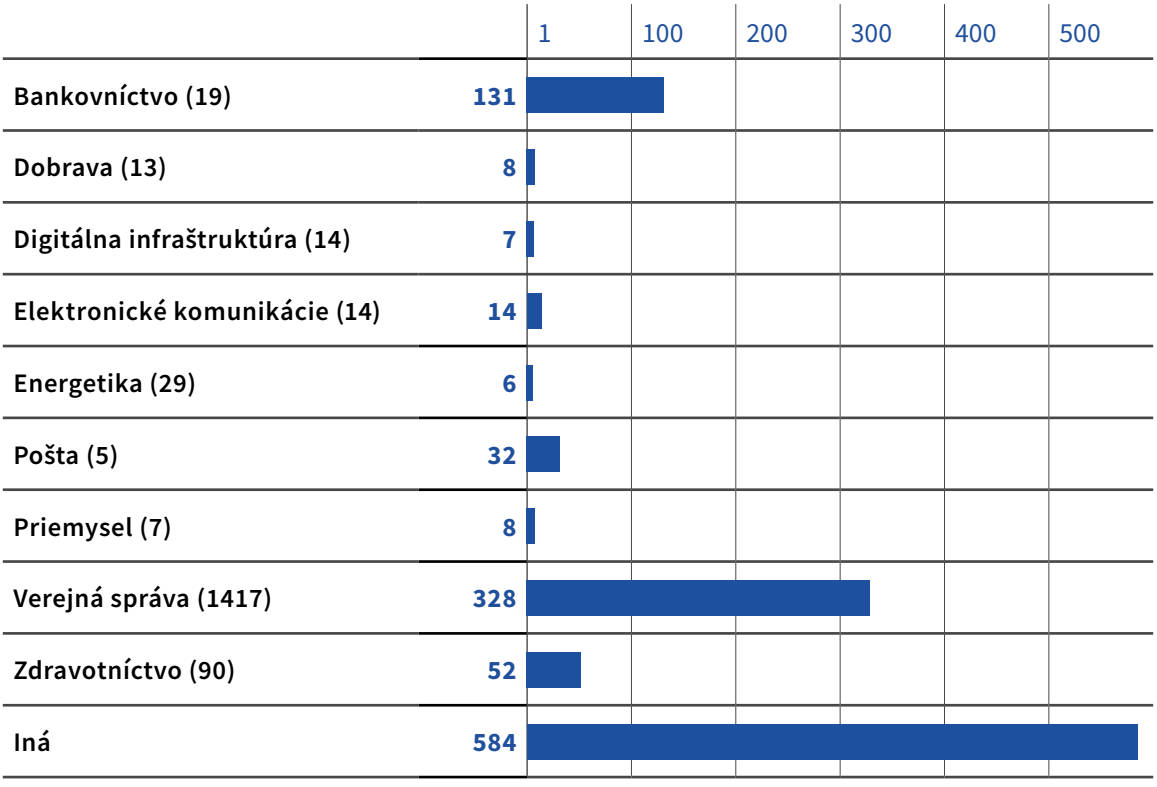
Počet hlásených kybernetických bezpečnostných incidentov podľa zákona – rok 2022



zdroj: NCKB SK-CERT

Najviac povinných a dobrovoľných hlásení v rámci sektorov bolo evidovaných v sektore Verejná správa. V niektorých sektoroch (Infraštruktúra finančných trhov, Voda a atmosféra), Národné centrum kybernetickej bezpečnosti SK-CERT neevidovalo žiadne hlásenie. Kategória „Iné“ zahŕňa dobrovoľné hlásenia od subjektov (firmy, občania), ktoré neboli zaradené do žiadneho zo sektorov podľa zákona. V zátvorke je uvedený počet identifikovaných PZS v sektore.

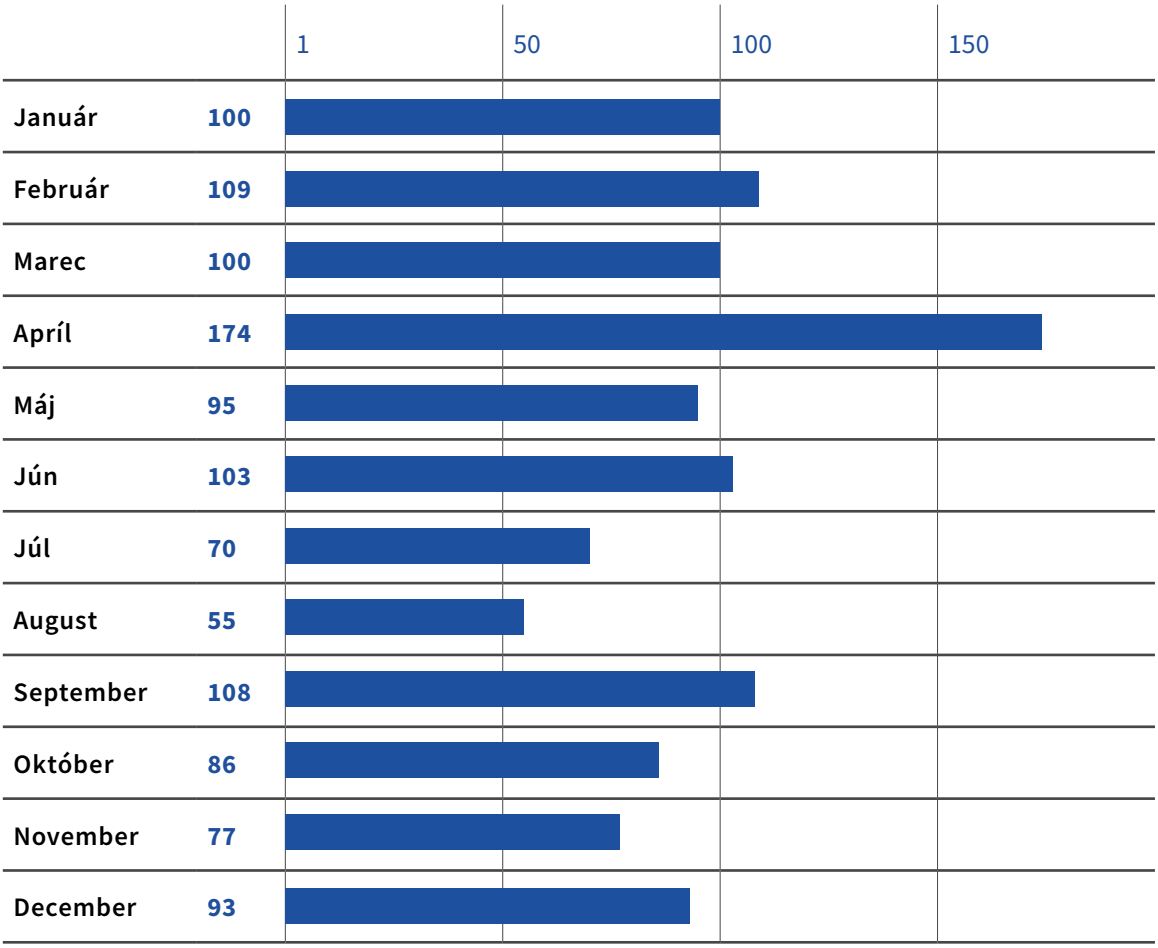
Hlásenia kybernetických bezpečnostných incidentov v sektoroch – rok 2022



zdroj: NCKB SK-CERT

Z časového hľadiska bolo najviac incidentov hlásených v mesiaci apríl.

Hlásenia kybernetických bezpečnostných incidentov v sektoroch – rok 2022



zdroj: NCKB SK-CERT

2.4 Najvýznamnejšie hrozby v Slovenskej republike za rok 2022

2.4.1 SOCIÁLNE INŽINIERSTVO

Počas celého roka pretrvávali phishingové kampane (e-mailové, telefonické aj SMS) imitujúce finančné, e-mailové, webhostingové a ISP služby. Časté bolo aj zneužívanie značiek globálnych dodávateľských spoločnosti (vrátane poštových služieb). Útoky boli na rôznej úrovni sofistikovanosti až po úroveň, na ktorej hodnoverne kopírovali spôsob aj dizajn komunikácie spoločnosti, ktorej meno zneužívajú. Útok je o to úspešnejší ak sa útočníkovi podarí získať prístup do pracovného e-mailového účtu osoby s významným postavením a tento prístup následne zneužije na ďalšie útoky (typ útoku „Business e-mail compromise“).

Phishingové útoky boli naďalej zneužívané na získanie prihlasovacích a iných citlivých údajov a na šírenie škodlivého kódu. Významnou zmenou bolo, že útočníci využívajúci škodlivé makrá v MS Office prílohách e-mailov prešli po zmene základných konfigurácií zo strany Microsoftu (vypnutie makier) na alternatívne formy príloh (napr. LNK, ISO a RAR).

V septembri boli zaznamenané prvé hlásenia telefonických a e-mailových phishingových kampaní zneužívajúcich identitu orgánov činných v trestnom konaní, Interpolu a Europolu. Väčšina hláse-

ných telefonických kampaní bola vedená v anglickom jazyku, obete boli kontaktované opakovane a forma komunikácie bola každým kontaktom agresívnejšia. E-mailové kampane boli nízkej kvality (e-maily boli nekvalitne spracované) a obsahovali „oficiálne vyzerajúci“ dokument MS Word.

Aj v roku 2022 sa niektorí útočníci zameriavali na podvodné konanie na inzertných portáloch. Spôsob útoku sa nezmenil – predajca bol oslovený útočníkom, ktorý mu pod zámienkou objednania prepravy podhodil škodlivú URL adresu, do ktorej následne obeť vpísala údaje z platobnej karty.

Zaznamenané boli aj rôzne pyramídové koncepty súvisiace s investíciami do kryptomien. Podvodná schéma má za cieľ vylákať od obete čo najviac finančných prostriedkov a aby pôsobila dôveryhodne, útočník na začiatku obeti aj reálne vypláca províziu, resp. výnos, v istom bode s tým však prestane, pričom obeť zväčša stále investuje. Tieto koncepty majú masívnu reklamu, napríklad aj na sociálnych sieťach.

2.4.2 NEDOSTUPNOSŤ SLUŽBY, DDOS ÚTOKY

Vo všeobecnosti možno rozlíšiť nedostupnosť spôsobenú následkom útoku a nedostupnosť spôsobenú následkom neočakávaného javu alebo prevádzkovej udalosti. Z pohľadu kybernetického priestoru SR bola najčastejšia nedostupnosť služby spôsobená z prevádzkových dôvodov – problémy po aktualizácii, rôzne nehody, miskonfigurácie a neadekvátna odpoveď administrátorov na zvýšenú návštevnosť webu, ktorá bola interpretovaná ako DDoS útok.

Významnú pozíciu mali aj DDoS útoky súvisiace s vojnou Ruska proti Ukrajine. Vo februári boli zaznamenané aktivistické DDoS útoky na niektoré slovenské médiá. Na útoky boli väčšinou používané voľne šírené nástroje, ale šírili sa aj webstránky, ktoré DDoS vykonávali cez prehliadač ich návštevníkov (aj bez ich vedomia).

V apríli boli zaznamenané rozsiahle DDoS útoky na členské štáty NATO, ktoré realizovali komunitné hackerské skupiny LEGION a KILLNET. Ďalšie útoky KILLNET boli zaznamenané v júni a v októbri, k niektorým sa priznala skupina Anonymous Russia. Vo väčšine prípadov sa jednotlivé skupiny k DDoS útokom verejne priznali.

Väčšina útokov bola realizovaná z IP adries patriacich anonymizačnej službe TOR, VPN službám, open proxy službám a z kompromitovaných zariadení, ktoré boli súčasťou infraštruktúry nástrojov na DDoS, ktoré sú na čiernom trhu prenajímané ako služba.

Najviditeľnejšie v slovenskom kybernetickom priestore boli DDoS útoky zamerané na zneprístupnenie rôznych webových stránok a služieb rôznych verejných inštitúcií (ministerstvá), ale aj súkromných spoločností (banky, letiská, dopravné spoločnosti). Tieto útoky boli koordinované a smerovali aj na iné členské štáty EÚ a NATO a ich verejné inštitúcie alebo iné dôležité ciele. Útoky boli často odpoveďou na vyhlásenia verejných predstaviteľov alebo na schválenie konkrétnych sankcií uvalených proti Rusku.

2.4.3 ŠKODLIVÝ KÓD

V máji, júni a novembri bol zaznamenaný nárast aktivity malvéru Emotet. Aktivita sa prejavovala v hlásených phishingových kampaniach a z informácií od zahraničných partnerov.

V októbri, novembri a decembri bolo zaznamenaných viacero kampaní, ktoré šírili malvér SystemBC (väčšinou vedie k infekcii ransomvérom). Podobne boli počas roka 2022 zaznamenané aktivity ďalších malvérov, napríklad Trickbot, Ursnif, Systembc, Hajime, Mirai, Expiro Gazavat, IcexLoader a iné, vrátane ransomvéru (HIVE, Venus, PLAY, Lockbit, Bozq a mig21 a iné).

Najčastejším vektorom infekcie škodlivým kódom bolo úspešné sociálne inžinierstvo, zlá bezpečnostná politika (používanie súkromných zariadení na pracovné účely, používanie služobných kont na súkromné účely a pod.), navštevovanie kompromitovaných webových stránok, inštalácia nelegálneho softvéru a zneužitie existujúcich zraniteľností na zariadeniach dostupných z internetu.

2.4.4 ZRANITEĽNOSTI A POKUSY O PRIENIK DO SYSTÉMU

Najčastejším vstupným vektorom do systémov obetí sú naďalej phishingové útoky, resp. nepozornosť zamestnancov vo forme vyplnenia prihlasovacích formulárov na phishingových weboch. Naďalej kritické sú aj nesprávne konfigurácie zariadení – otvorené RDP, FTP a dostupné rozhrania na prihlasovanie, ktoré útočníci identifikujú neustávajúcim skenovaním.

Zverejnené návody na zneužitie zraniteľností sú behom pár hodín objektom skenovania zo strany útočníkov. V priebehu roka boli (na základe informácií dostupných z verejných zdrojov) vykonané adresné varovania, ktoré obsahovali informácie o nesprávne nakonfigurovaných zariadeniach, o potenciálnych únikoch dát a zraniteľnostiach (napr. medializované zraniteľnosti MS Exchange, QNAP NAS, Fortinet a Zimbra). Na prieniky do systému sú naďalej zneužívané brute-force útoky ako password spraying. Viacero incidentov bolo spôsobených nesprávnou politikou používania hesiel, napr. opakovaným používaním hesiel, ktoré sú už (často roky) kompromitované alebo zanechaním pôvodného hesla z výroby.

Organizácie používajú desiatky rôznych technológií a ich udržiavanie je pre počtom menší tím časovo náročné. Absencia politiky aktualizácií často spôsobuje stret záujmov – dostupnosť služieb počas prevádzkových hodín a pracovný čas zamestnanca, čo vedie k nutnému používaniu dlhodobo neaktualizovaných technológií. Absencia manažmentu aktív spôsobuje, že zmenou zamestnanca spravujúceho IT sa na menej používané technológie zabudne a nie sú naďalej udržiavané a aktualizované.

2.4.5 ÚNIKY DÁT

Vlastnou aktivitou Národné centrum kybernetickej bezpečnosti SK-CERT identifikovalo viacero kompromitovaných e-mailových účtov a RDP prístupov, ktoré boli ponúkané na predaj na hackerských fórach (obete boli adresne varované). Rozšírená bola aj spolupráca s bankovým sektorom, ktorý bol pravidelne informovaný o potencionálnych kompromitáciách platobných kariet. Jedným z identifikovaných únikov bola databáza platobných kariet, ktorú zdieľal hackerský obchod BidenCash zadarmo ako súčasť svojho marketingu.

3 SEKTOROVÝ POHĽAD

Hlavným zdrojom dát pre zhodnotenie pohľadu na jednotlivé sektory netvoria len výsledky auditných správ, ale aj zhodnotenie aktivít jednotlivých ústredných orgánov. Je možné konštatovať, že stav kybernetickej bezpečnosti sa výrazne líši v závislosti od sektora.

Sektor „**Bankovníctvo**“ kontinuálne vykazuje veľmi dobré výsledky v oblasti kybernetickej bezpečnosti. K tejto téme jednotliví PZS pristupujú zodpovedne nielen pri implementovaní bezpečnostných požiadaviek, ale aj pri komunikácii s NBÚ. V prípade riešenia incidentov, ale aj iných problémov reagujú operatívne a veľmi rýchlo. Zástupcovia PZS v tomto sektore sú aktívni aj pri budovaní bezpečnostnej komunity.

V sektore „**Zdravotníctvo**“ sa postupne zlepšuje vnímanie témy kybernetickej bezpečnosti. Napomáha tomu zlepšujúci sa stav aktivít ústredného orgánu. Postupné uvedomenie si zodpovednosti nielen za dáta, ale aj za zabezpečenie funkčnosti systémov a služieb, od ktorých závisia ľudské životy, postupne zlepšuje stav kybernetickej bezpečnosti v tomto sektore.

Sektor „**Energetika**“ má najvýraznejší rozdiel medzi podsektormi aj v samotných podsektoroch. Podsektor „**Plynárenstvo**“ je na tom z hľadiska auditných výsledkov najlepšie spomedzi všetkých sektorov a podsektorov. V prípade podsektora „**Elektroenergetika**“ sú prítomné výrazné rozdiely medzi jednotlivými PZS. Naopak, v podsektore „**Tepelná energetika**“ pretrvávajú extrémne zlé výsledky auditov napriek skutočnosti, že ide o dôležitý podsektor, ktorého fungovanie má veľmi veľký vplyv na bežný život občanov a to najmä v zimnom období. Obmedzenie alebo výpadok služieb môže zásadne ovplyvniť životy a zdravie občanov.

Pri sektoroch „**Infraštruktúra finančných trhov**“, „**Priemysel**“ a „**Pošta**“ nie je možné získať jasný prehľad o stave kybernetickej bezpečnosti. Ústredné orgány zodpovedné za tieto sektory neuviedli konkrétne informácie o stave kybernetickej bezpečnosti v týchto sektoroch a takisto v týchto sektoroch nie je odovzdaných dostatok auditných správ, aby sa z nich dala spraviť dostatočne anonymizovaná štatistická vzorka.

Pri sektore „**Verejná správa**“, podsektor „**Informačné systémy verejnej správy**“, v ktorom sa nachádza najväčší počet PZS sa situácia v oblasti kybernetickej bezpečnosti dlhodobo nemení. Stále tu možno pozorovať až kritické zanedbávanie bezpečnosti. Najmä samosprávy a menší prevádzkovatelia si dostatočne neuvedomujú dôležitosť témy kybernetickej bezpečnosti, k problematike pristupujú povrchne a zameriavajú sa skôr na formálne aktivity (napríklad kupovanie generickej dokumentácie).

Takisto sa často snažia preniesť zodpovednosť za riešenie tejto problematiky na externé spoločnosti, vrátane zodpovedností, ktoré prináležia len štatutárovi spoločnosti a sú teda neprenosné. Celkové riadenie kybernetickej bezpečnosti pri PZS v tomto sektore často chýba, je chaotické alebo čiastkové. Tieto zistenia však nie sú príznačné len pre samosprávy alebo malých prevádzkovateľov , ale aj pre niektorých veľkých PZS v tomto podsektore, vrátane štátnych inštitúcií.

3.1 Najčastejšie nálezy auditu

Z auditných správ, ktoré odovzdali PZS za rok 2022 možno konštatovať nasledujúce najčastejšie nálezy auditu (bez rozdielu sektora):

3.1.1 RIADENIE BEZPEČNOSTI

- Neexistujúca stratégia KB a nedostatočná podpora najvyššieho vedenia
- Neurčený Manažér KB, prípadne neformálna rola
- Nie je definovaná štruktúra riadenia, výkonu a kontroly v oblasti kybernetickej bezpečnosti
- Nie sú definované kontrolné manažérske mechanizmy
- Nie je zaručená nezávislosť riadenia bezpečnosti od riadenia IT
- Závažné nedostatky v oblasti riadenia aktív, hrozieb a rizík
- Nie je stanovená zodpovednosť za identifikáciu a evidenciu aktív
- Nie sú stanovené pravidlá a zodpovednosti pri implementácii opatrení
- Nie je vykonaná klasifikácia informácií a kategorizácia informačných systémov
- Nedostatočná, neaktuálna alebo chýbajúca bezpečnostná dokumentácia
- Nie je zadokumentovaná bezpečnostná architektúra, resp. vymedzenie rozsahu a spôsobu plnenia bezpečnostných opatrení
- Neexistujú, alebo nie sú aktualizované smernice obsahujúce požiadavky fyzickej bezpečnosti
- Pravidlá popísané v politikách nie sú zavedené do praxe (nízka vyspelosť procesov)
- Nie je vykonaná analýza funkčných dopadov
- Nie sú definované špecifické postupy HR vo vzťahu ku kybernetickej bezpečnosti
- Nie sú definované postupy na zaradenie osôb do bezpečnostných rolí, ich kompetencie a právomoci
- Zodpovednosti v oblasti bezpečnosti nie sú súčasťou pracovných zmlúv
- Nie je sformalizovaná zásada najnižších privilégií
- Nie je sformalizovaná zásada oddeľovania zodpovedností
- Nie sú stanovené postupy pri presune práv, povinnosti a zodpovednosti vo vzťahu ku KB na inú osobu
- Nie sú formalizované procesy pri ukončení pracovného vzťahu pre bezpečnostné roly (exit management)
- Zmluvy s dodávateľmi neobsahujú ustanovenia v oblasti kybernetickej bezpečnosti
- Nie sú určené procesy nezávislého hodnotenia, merania a preskúmavania efektivity a účinnosti prijatých opatrení
- Nie je vytvorený auditný program, ktorý by zahŕňal IT a bezpečnostné kontrolné mechanizmy
- Chýba vzdelávanie v oblasti informačnej bezpečnosti a ochrany údajov

3.1.2 VÝKON BEZPEČNOSTI

- Nie sú uchovávané prevádzkové záznamy
- Nie je implementovaný nástroj na monitorovanie udalostí
- Chýbajúca topológia, segmentácia, zoznamy portov
- Nedostatočné riešenie šifrovej ochrany informácií
- Neexistuje záložná komunikačná trasa pre konektivitu
- Nie je implementovaná politika riadenia prístupov
- Nie je formálne definovaný proces riešenia a hlásenia bezpečnostných incidentov
- Neexistencia procesov riadenia kontinuity činností
- Nie sú testované havarijné plány a plány kontinuity
- Nie sú vypracované plány zálohovania a požiadavky na zálohovanie
- Nejasné a neformálne postupy zálohovania
- Nie je vykonávané testovanie obnovy záloh
- Vzdialený prístup do nie je zabezpečený (týka sa zamestnancov aj dodávateľov)
- Nie je implementované riešenie pre automatické overovanie bezpečnosti zariadení tretích strán
- Nie sú určené procesy bezpečného vývoja a obstarávania systémov (SSDLC)

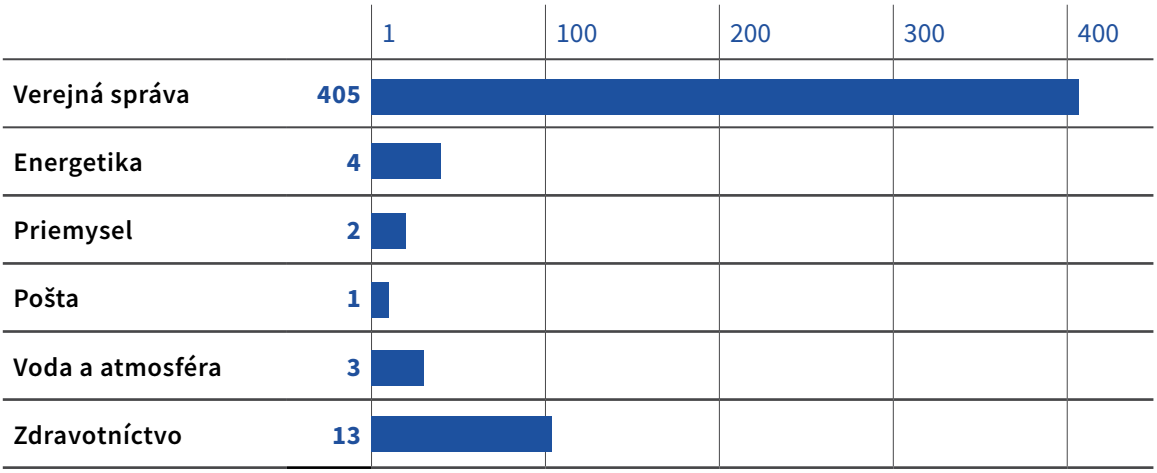
3.2 Samohodnotenia

Mieru implementácie zákonných požiadaviek v oblasti kybernetickej bezpečnosti je možné overiť aj tzv. samohodnotením manažérom kybernetickej bezpečnosti. Samohodnotenie plne nahrádza potrebu auditu kybernetickej bezpečnosti, pričom PZS ho môže vykonať len pre siete a informačné systémy v kategórii I. a II. v období od 1. augusta 2021 do 31. decembra 2023.

NBÚ má na svojom webovom sídle zverejnený formulár samohodnotenia, ktorý je tvorený sériou otázok za účelom zistenia úrovne kybernetickej bezpečnosti u PZS .

K 31. 12. 2022 bolo NBÚ doručených 428 samohodnotení, pričom výrazne majoritné zastúpenie patril sektoru Verejná správa s počtom 405 samohodnotení.

Počet hlásených kybernetických bezpečnostných incidentov podľa zákona – rok 2022



zdroj: Doručené samohodnotenia 2022, NBÚ

3.3 Sankcie

V zmysle zákona č. 69/2018 o kybernetickej bezpečnosti je úrad oprávnený uložiť pokutu, ak PZS poruší svoje povinnosti, ktoré mu z tohto zákona vyplývajú. V roku 2022 vykonal úrad viacero kontrol plnenia zákonných povinností prevádzkovateľmi základnej služby. Úrad uložil pokutu dvom subjektom v celkovej výške 26 000 eur.

3.4 Bankovníctvo

Ústredný orgán: Ministerstvo financií Slovenskej republiky (MF SR)

Počet PZS : 19

Počet PZS s povinnosťou auditu v roku 2022: 18
(možné splniť aj samohodnotením podľa §34a ods. 2 ZoKB)

Počet odovzdaných auditných správ: 13

Počet odovzdaných samohodnotení: 0

Podsektory: žiadne

3.4.1 ZHODNOTENIE STAVU KYBERNETICKEJ BEZPEČNOSTI ZA ROK 2022 ÚSTREDNÝM ORGÁNOM

3.4.1.1 Hrozby

Za najvýznamnejšie hrozby v roku 2022 považuje MF SR pokročilé pretrvávajúce hrozby (APT), ransomvérové útoky, rastúce útoky na internet vecí (IoT), bezpečnostné hrozby v cloude (v súvislosti s rastúcim počtom organizácií, ktoré presúvajú svoje údaje a aplikácie do cloudu) a útoky sociálneho inžinierstva.

3.4.1.2 Aktivity

MF SR ako ústredný orgán v zmysle zákona č. 45/2011 o kritickej infraštruktúre zrealizoval v priebehu roka 2022 kontrolu u prevádzkovateľov prvku sektora Financie v zmysle § 9 „Povinnosti prevádzkovateľa“. Pri kontrolnej činnosti boli u niektorých subjektov identifikované nedostatky, na nápravu ktorých boli vyzvané, zároveň MF SR poskytlo odporúčania na zefektívnenie procesov v oblasti ochrany prvku pred narušením alebo zničením, dopracovanie bezpečnostnej dokumentácie, vykonanie súvisiacich auditov a iné v súlade s platnou legislatívou. MF SR začalo budovať Security operations center (SOC) ako oddelenie ministerstva, pričom v decembri 2022 sa SOC MF SR stal členom medzinárodného združenia TF CSIRT pod štatútom „Listed team“.

3.4.1.3 Plánované aktivity

MF SR plánuje plošne rozvinúť mechanizmus vzdelávania svojich pracovníkov v boji proti kybernetickým hrozbám (e- learningový portál LMS, interné vzdelávanie pracovníkov). Takisto plánuje akreditovať Oddelenie bezpečnostného monitoringu SOC v medzinárodnom združení TF CSIRT. Plánuje zorganizovať stretnutie so zástupcami sektorových organizácií MF SR na tému zlepšenia poskytovaných služieb v kybernetickej bezpečnosti, pričom prvotne ako pilotný projekt bude chcieť naštartovať výmenu relevantných informácií o kybernetických útokoch a zasielanie relevantných varovaní.

3.4.2 VÝSLEDKY AUDITOV PZS V SEKTORE BANKOVNÍCTVO

Národnému bezpečnostnému úradu bolo k 31.12.2022 doručených celkovo 13 auditných správ zo sektora Bankovníctvo (bez zmeny oproti roku 2021). Nie všetci prevádzkovatelia ale musia vykonať audit, pretože v prípadoch podľa zákona stačí doručenie samohodnotenia, ktoré nie sú v tejto štatistike zahrnuté. Na základe štatistiky súladu s auditnými požiadavkami, v sektore Bankovníctvo je priemerná percentuálna miera súladu nasledujúca:

Priemerná percentuálna miera súladu (rok 2022)

SÚLAD	77 %
ČIASTOČNÝ SÚLAD	6 %
NESÚLAD	8 %
NEAPLIKOVATEĽNÉ	3 %
OVERENÉ NA INOM MIESTE	5 %

zdroj: Doručené audity 2022, NBÚ

Pri pohľade na jednotlivých PZS v sektore Bankovníctvo je vysoká miera súladu s auditnými požiadavkami kontinuálna naprieč všetkými prevádzkovateľmi. Najvyššiu mieru súladu dosiahol PZS, ktorý z 226 auditovaných požiadaviek dosiahol súlad v 218 požiadavkách a čiastočný súlad v 8 požiadavkách. Na druhej strane, najnižšia miera súladu bola identifikovaná u PZS , ktorý z 264 auditovaných požiadaviek dosiahol súlad v 66 požiadavkách a nesúlad v 153 požiadavkách (15 požiadaviek bolo neaplikovateľných, 12 overených na inom mieste).

3.4.3 NAJČASTEJŠIE AUDITNÉ ZISTENIA

Medzi najčastejšie auditné zistenia v sektore Bankovníctvo patria:

- nie je zdokumentované vymedzenie rozsahu a spôsobu plnenia všetkých bezpečnostných opatrení,
- nie sú stanovené postupy pri presune práv, povinnosti a zodpovednosti vo vzťahu ku kybernetickej bezpečnosti na inú osobu,
- vstupno-výstupné body sú identifikované len v príslušnej dokumentácii k jednotlivým projektom, pričom celkový zoznam neexistuje,
- nie sú implementované kontroly zariadení tretích strán.

3.5 Sektor Doprava

Ústredný orgán: Ministerstvo dopravy Slovenskej republiky (MD SR)

Počet PZS : 13

Počet PZS s povinnosťou auditu v roku 2022: 13
(možné splniť aj samohodnotením podľa §34a ods. 2 ZoKB)

Počet odovzdaných auditných správ: 9

Počet odovzdaných samohodnotení: 0

Podsektory: Cestná doprava, Letecká doprava, Vodná doprava, Železničná doprava

3.5.1 ZHODNOTENIE STAVU KYBERNETICKEJ BEZPEČNOSTI ZA ROK 2022 ZO STRANY ÚSTREDNÉHO ORGÁNU

3.5.1.1 Hrozby

MD SR za najzávažnejšie hrozby identifikovalo najmä nedostatok odborných personálnych kapacít pre oblasť bezpečnosti, hrozby sociálneho inžinierstva, hrozby v súvislosti so zvýšeným počtom rôznych typov útokov súvisiacich s vojenským konfliktom na Ukrajine a morálnu opotrebovanosť hardvéru a softvéru.

3.5.1.2 Aktivity

MD SR vykonalo analýzu potrieb a požiadaviek sektorov doprava, pošta, elektronické komunikácie, ktorých je gestorom. Na základe analýzy boli zaktualizované sektorové kritériá. Sú východiskom pre prípravu podkladov na vypracovanie návrhu sektorových vyhlášok, ktoré zadefinujú sektorové bezpečnostné opatrenia pre jednotlivé sektory. Na základe analýzy sektorových kritérií v súvislosti aj s NIS 2 MD SR identifikovalo požiadavky, ktoré následne budú upravené v sektorových vyhláškach v rámci transpozície požiadaviek NIS 2.

3.5.1.3 Plánované aktivity

MD SR plánuje transponovať požiadavky NIS 2 do národnej legislatívy SR s určením kompetencií medzi dotknutými sektormi, vrátane prípravy sektorových vyhlášok pre sektor dopravy, sektor pošty a sektor elektronických komunikácií.

3.5.2 VÝSLEDKY AUDITOV PZS V SEKTORE DOPRAVA

Národnému bezpečnostnému úradu bolo k 31.12.2022 doručených celkovo 9 auditných správ zo sektora Doprava. Nie všetci prevádzkovatelia ale musia vykonať audit, nakoľko v prípadoch podľa zákona stačí doručenie samohodnotenia, ktoré nie sú v tejto štatistike zahrnuté. Na základe štatistiky súladu s auditnými požiadavkami, v sektore Doprava je priemerná percentuálna miera súladu nasledujúca:

Priemerná percentuálna miera súladu (rok 2022)

SÚLAD	46 %
ČIASTOČNÝ SÚLAD	17 %
NESÚLAD	28 %
NEAPLIKOVATEĽNÉ	3 %
OVERENÉ NA INOM MIESTE	5%

zdroj: Doručené audity 2022, NBÚ

V sektore Doprava je priemerná miera súladu pod 50 %. Najvyššiu mieru súladu dosiahol PZS , ktorý z 266 auditných požiadaviek dosiahol súlad v 205 požiadavkách, čiastočný súlad v 17 požiadavkách a nesúlad v 14 požiadavkách (15 požiadaviek bolo neaplikovateľných a 15 overených na inom mieste).

Najnižšiu mieru súladu dosiahol PZS, ktorý z 261 auditných požiadaviek dosiahol súlad v 20 požiadavkách, čiastočný súlad v 68 požiadavkách a nesúlad v 156 požiadavkách (5 požiadaviek bolo neaplikovateľných, 12 overených na inom mieste).

3.5.3 NAJČASTEJŠIE AUDITNÉ ZISTENIA

Medzi najčastejšie auditné zistenia v sektore Doprava patria:

- nie sú dostatočne definované role a zodpovednosti v oblasti kybernetickej bezpečnosti,
- manažér kybernetickej bezpečnosti nie je menovaný,
- nie sú definované kontrolné mechanizmy v oblasti riadenia kybernetickej bezpečnosti,
- zmluvy s dodávateľmi neobsahujú všetky povinné náležitosti vyplývajúce z Vyhlášky 362 a nie sú v centrálnej evidencii,
- nie je definovaná a implementovaná politika riadenia prístupov.

3.6 Digitálna infraštruktúra

Ústredný orgán: Národný bezpečnostný úrad (NBÚ)

Počet PZS: 14

Počet PZS s povinnosťou auditu v roku 2022: 14
(možné splniť aj samohodnotením podľa §34a ods. 2 ZoKB)

Počet odovzdaných auditných správ: 11

Počet odovzdaných samohodnotení: 0

Podsektory: žiadne

3.6.1 ZHODNOTENIE STAVU KYBERNETICKEJ BEZPEČNOSTI ZA ROK 2022 ZO STRANY ÚSTREDNÉHO ORGÁNU

3.6.1.1 Hrozby

NBÚ identifikoval v sektore Digitálna infraštruktúra ako najvýznamnejšie hrozby, ktoré sa najčastejšie vyskytujú v rámci slovenského kybernetického priestoru – útoky využívajúce sociálne inžinierstvo (najmä phishing a vishing), šírenie škodlivého kódu a zneužívanie zraniteľností.

Pre sektor Digitálna infraštruktúra je ďalej významnou hrozbou zneužívanie kompromitovanej infraštruktúry PZS na vykonávanie iných útokov (riadenie botnetových sietí, DoS útoky, šírenie phishingu, šírenie škodlivého kódu).

3.6.1.2 Aktivity

V sektore Digitálna infraštruktúra NBÚ vykonáva viacero aktivít, z ktorých najvýznamnejšou je najmä koordinácia riešenia kybernetických bezpečnostných incidentov. Takisto vykonáva preventívne aktivity v podobe včasných varovaní a zasielania relevantných informácií PZS v sektore a taktiež poskytuje pravidelné odborné konzultácie jednotlivým PZS podľa potreby.

3.6.1.3 Plánované aktivity

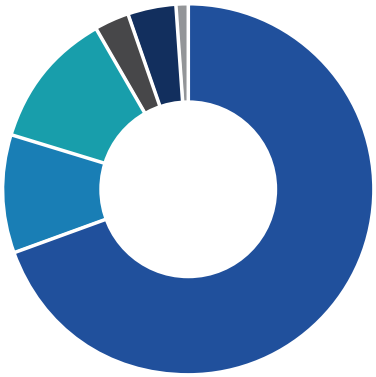
NBÚ plánuje kontinuálne pokračovať v už existujúcich aktivitách a postupne zlepšovať služby poskytované PZS. NBÚ pravidelne prehodnocuje situáciu v sektore Digitálna infraštruktúra a v prípade potreby bude pružne reagovať.

3.6.2 VÝSLEDKY AUDITOV PZS V SEKTORE DIGITÁLNA INFRAŠTRUKTÚRA

Národnému bezpečnostnému úradu bolo k 31.12.2022 doručených celkovo 11 auditných správ zo sektora Digitálna infraštruktúra. Nie všetci prevádzkovatelia ale musia vykonať audit. V prípadoch podľa zákona stačí doručenie samohodnotenia, ktoré nie sú v tejto štatistike zahrnuté. Na základe štatistiky súladu s auditnými požiadavkami, v sektore Digitálna infraštruktúra je priemerná percentuálna miera súladu nasledujúca:

Pri pohľade na jednotlivých PZS v sektore Digitálna infraštruktúra je viac ako polovičná miera súladu s auditnými požiadavkami kontinuálna u väčšiny prevádzkovateľov, čo sa prejavilo aj na celkovej miere súladu v sektore. Najvyššiu mieru súladu dosiahol PZS, ktorý zo 162 auditných požiadaviek dosiahol súlad v 157 požiadavkách, čiastočný súlad v 3 požiadavkách a v žiadnej z požiadaviek nemal nesúlad (ostatné požiadavky boli neaplikovateľné).

Na druhej strane, najnižšia miera súladu bola identifikovaná u PZS , ktorý z 273 auditných požiadaviek dosiahol súlad v 94 požiadavkách, čiastočný súlad v 28 požiadavkách a nesúlad v 117 požiadavkách (13 požiadaviek bolo neaplikovateľných, 21 overených na inom mieste).



Priemerná percentuálna miera súladu (rok 2022)

SÚLAD	69 %
ČIASTOČNÝ SÚLAD	10 %
NESÚLAD	12 %
NEAPLIKOVATEĽNÉ	3 %
OVERENÉ NA INOM MIESTE	4 %
NEVYHODNOTENÉ	1 %

zdroj: Doručené audity 2022, NBÚ

3.6.3 NAJČASTEJŠIE AUDITNÉ ZISTENIA

Medzi najčastejšie auditné zistenia v sektore Digitálna infraštruktúra patria:

- nie sú definované postupy na zaradenie osôb do bezpečnostných rolí s jasne stanovenými kompetenciami a právomocami,
- nevykonáva sa pravidelná analýza rizík,
- nie sú identifikované požiadavky na zabezpečenie kontinuity riadenia kybernetickej bezpečnosti,
- nie sú vypracované plány zálohovania,
- testovanie havarijných plánov sa nevykonáva.

3.7 Elektronické komunikácie

Ústredný orgán: Ministerstvo dopravy Slovenskej republiky (MD SR)

Počet PZS : 11

Počet PZS s povinnosťou auditu v roku 2022: 11
(možné splniť aj samohodnotením podľa §34a ods. 2 ZoKB)

Počet odovzdaných auditných správ: 9

Počet odovzdaných samohodnotení: 0

Podsektory: Satelitná komunikácia, Siete a služby pevných a mobilných elektronických komunikácií

3.7.1 ZHODNOTENIE STAVU KYBERNETICKEJ BEZPEČNOSTI ZA ROK 2022 ZO STRANY ÚSTREDNÉHO ORGÁNU

3.7.1.1 Hrozby

Ústredný orgán poskytol zhodnotenie hrozieb len v rámci sektora Doprava.

3.7.1.2 Aktivity

MD SR vykonalo analýzu potrieb a požiadaviek sektorov doprava, pošta, elektronické komunikácie, ktorým je gestorom. Na základe analýzy boli zaktualizované sektorové kritériá, ktoré sú východiskom pre prípravu podkladov na vypracovanie návrhu sektorových vyhlášok, ktoré zadefinujú sektorové bezpečnostné opatrenia pre jednotlivé sektory. Na základe analýzy sektorových kritérií v súvislosti aj s NIS 2 MD SR identifikovalo požiadavky, ktoré následne budú upravené v sektorových vyhláškach v rámci transpozície požiadaviek NIS 2.

3.7.1.3 Plánované aktivity

MD SR plánuje transponovať požiadavky NIS 2 do národnej legislatívy SR s určením kompetencií medzi dotknutými sektormi, vrátane prípravy sektorových vyhlášok pre sektor dopravy, sektor pošty a sektor elektronických komunikácií.

3.7.2 VÝSLEDKY AUDITOV PZS V SEKTORE ELEKTRONICKÉ KOMUNIKÁCIE

Národnému bezpečnostnému úradu bolo k 31.12.2022 doručených celkovo 9 auditných správ zo sektora Elektronické komunikácie. Nie všetci prevádzkovatelia ale musia vykonať audit. V prípadoch podľa zákona stačí doručenie samohodnotenia, ktoré nie sú v tejto štatistike zahrnuté. Na základe štatistiky súladu s auditnými požiadavkami, v sektore Elektronické komunikácie je priemerná percentuálna miera súladu nasledujúca:

Priemerná percentuálna miera súladu (rok 2022)

SÚLAD	73 %
ČIASTOČNÝ SÚLAD	9 %
NESÚLAD	13 %
NEAPLIKOVATEĽNÉ	2 %
OVERENÉ NA INOM MIESTE	3 %

zdroj: Doručené audity 2022, NBÚ

Pri pohľade na jednotlivých PZS v sektore Elektronické komunikácie je viac ako polovičná miera súladu s auditnými požiadavkami kontinuálna naprieč všetkými prevádzkovateľmi. Najvyššiu mieru súladu dosiahol PZS, ktorý dosiahol 100 % mieru súladu vo všetkých 199 auditovaných požiadavkách.

Na druhej strane, najnižšiu mieru súladu dosiahol PZS, ktorý z 266 auditovaných požiadaviek dosiahol súlad v 13 požiadavkách, čiastočný súlad v 44 požiadavkách a nesúlad v 189 požiadavkách (7 požiadaviek bolo neaplikovateľných, 13 overených na inom mieste).

3.7.3 NAJČASTEJŠIE AUDITNÉ ZISTENIA

Medzi najčastejšie auditné zistenia v sektore Elektronické komunikácie patria:

- požiadavky kybernetickej bezpečnosti počas celého životného cyklu informácií a IS nie sú zohľadnené,
- nie sú definované špecifické postupy personalistiky vo vzťahu ku kybernetickej bezpečnosti,
- zmluvy s dodávateľmi neobsahujú ustanovenia v oblasti kybernetickej bezpečnosti,
- neboli predložené formalizované pravidlá práce v zabezpečenom priestore PZS,
- požiadavky na zálohovanie nie sú formalizované, dokumentácia zálohovania nie je zo strany PZS centrálne evidovaná.

3.8 Energetika

Ústredný orgán: Ministerstvo hospodárstva Slovenskej republiky (MH SR)

Počet PZS: 29

Počet PZS s povinnosťou auditu v roku 2022: 28
(možné splniť aj samohodnotením podľa §34a ods. 2 ZoKB)

Počet odovzdaných auditných správ: 20

Počet odovzdaných samohodnotení: 4

Podsektory: Baníctvo, Elektroenergetika, Plynárenstvo,
Ropa a ropné produkty, Tepelná energetika

3. 8. 1 ZHODNOTENIE STAVU KYBERNETICKEJ BEZPEČNOSTI ZA ROK 2022 ZO STRANY ÚSTREDNÉHO ORGÁNU

3.8.1.1 Hrozby

Podľa vyjadrenia ústredného orgánu v roku 2022 MH SR neriešilo žiadne hrozby v sektoroch ani podsektoroch.

3.8.1.2 Aktivity

V spolupráci s ostatnými ústrednými orgánmi MH SR pripomienkovalo Stratégiu kybernetickej obrany SR a vyhlášku NBÚ, ktorou sa určujú znalostné štandardy v oblasti kybernetickej bezpečnosti.

Zástupca MH SR sa zúčastňoval na viacerých pracovných skupinách súvisiacich s kybernetickou bezpečnosťou. Nad rámec §9 ods. 1 písm. c) zákona č. 69/2018 o kybernetickej bezpečnosti nevykonávali žiadne činnosti.

3.8.1.3 Plánované aktivity

Pre plnohodnotnú koordináciu v oblasti kybernetickej bezpečnosti v sektoroch a podsektoroch, za ktoré je podľa zákona MH SR zodpovedné, plánuje MH SR vytvoriť pracovné miesto pre koordináciu kybernetickej bezpečnosti v sektoroch a podsektoroch, resp. pre komunikáciu a koordináciu kybernetickej bezpečnosti s PZS .

3. 8. 2 VÝSLEDKY AUDITOV PZS V SEKTORE ENERGETIKA

Národnému bezpečnostnému úradu bolo k 31.12.2022 doručených celkovo 20 auditných správ zo sektora Energetika. Nie všetci prevádzkovatelia ale musia vykonať audit. V prípadoch podľa zákona stačí doručenie samohodnotenia, ktoré nie sú v tejto štatistike zahrnuté. Na základe štatistiky súladu s auditnými požiadavkami, v sektore Energetika je priemerná percentuálna miera súladu nasledujúca:

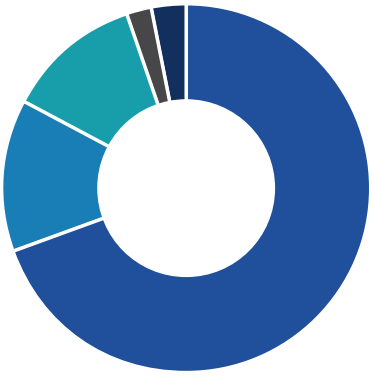
Priemerná percentuálna miera súladu (rok 2022)

SÚLAD	57 %
ČIASTOČNÝ SÚLAD	19 %
NESÚLAD	21 %
NEAPLIKOVATEĽNÉ	2 %
OVERENÉ NA INOM MIESTE	2 %

zdroj: Doručené audity 2022, NBÚ

V sektore Energetika sú prítomné veľké rozdiely naprieč sektormi.

V podsektore Elektroenergetika je evidovaná miera súladu skoro 70 %, v prípade podsektora Plynárenstvo takmer 90 %. V sektore Tepelná energetika je priemerná miera súladu pod 1 %.



Elektrotechnika – priemerná percentuálna miera súladu (rok 2022)

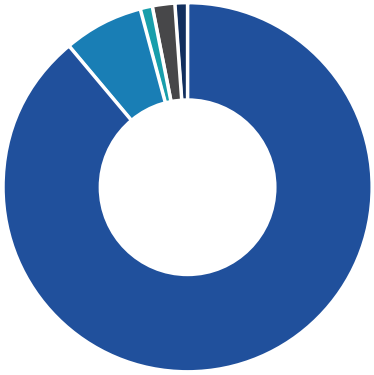
SÚLAD	69 %
ČIASTOČNÝ SÚLAD	13 %
NESÚLAD	12 %
NEAPLIKOVATEĽNÉ	2 %
OVERENÉ NA INOM MIESTE	3 %

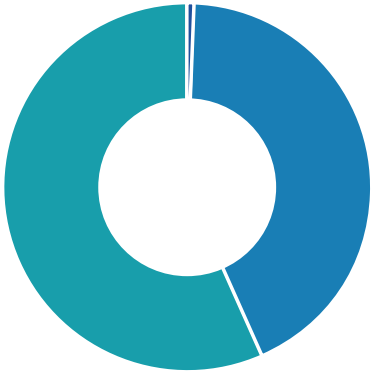
zdroj: Doručené audity 2022, NBÚ

Plynárenstvo – priemerná percentuálna miera súladu (rok 2022)

SÚLAD	88 %
ČIASTOČNÝ SÚLAD	7 %
NESÚLAD	1 %
NEAPLIKOVATEĽNÉ	2 %
OVERENÉ NA INOM MIESTE	1 %

zdroj: Doručené audity 2022, NBÚ





Tepelná energerika – priemerná percentuálna miera súladu (rok 2022)

SÚLAD	0,8 %
ČIASTOČNÝ SÚLAD	42,8 %
NESÚLAD	56,4 %

zdroj: Doručené audity 2022, NBÚ

V prípade podsektora Tepelná energetika dvaja z prevádzkovateľov dosiahli nulovú mieru súladu s auditovanými požiadavkami.

3. 8. 3 NAJČASTEJŠIE AUDITNÉ ZISTENIA

Medzi najčastejšie auditné zistenia v sektore Energetika patria:

- zoznam kontrolných aktivít v spoločnosti nie je definovaný,
- spoločnosť nemala vytvorený auditný program, ktorý by zahŕňal IT a bezpečnostné kontrolné mechanizmy,
- nebola vykonaná analýza funkčných vplyvov,
- procesy pri uskutočnení pracovného vzťahu pre bezpečnostné roly nie sú formalizované,
- nie sú aplikované kontroly technických prostriedkov proti škodlivému kódu pri vzdialenom prístupe pre dodávateľské koncové stanice.

3.9 Infraštruktúra finančných trhov

Ústredný orgán: Ministerstvo financií Slovenskej republiky (MF SR)

Počet PZS: 1

Počet PZS s povinnosťou auditu v roku 2022: 1
(možné splniť aj samohodnotením podľa §34a ods. 2 ZoKB)

Počet odovzdaných auditných správ: 1

Počet odovzdaných samohodnotení: 0

Podsektory: žiadne

3.9.1 ZHODNOTENIE STAVU KYBERNETICKEJ BEZPEČNOSTI ZA ROK 2022 ZO STRANY ÚSTREDNÉHO ORGÁNU

Ústredný orgán poslal rovnaké zhodnotenie ako pre sektor Bankovníctvo.

3.9.2 VÝSLEDKY AUDITOV PZS V SEKTORE INFRAŠTRUKTÚRA FINANČNÝCH TRHOV

Pre nemožnosť vytvoriť anonymizovanú štatistickú vzorku z jedného prevádzkovateľa neuvádzame výsledok jeho auditu v tejto správe.

3.10 Pošta

Ústredný orgán: Ministerstvo dopravy a výstavby Slovenskej republiky (MD SR)

Počet PZS: 5

Počet PZS s povinnosťou auditu v roku 2022: 3
(možné splniť aj samohodnotením podľa §34a ods. 2 ZoKB)

Počet odovzdaných auditných správ: 1

Počet odovzdaných samohodnotení: 1

Podsektory: Poskytovanie poštových služieb, poštový platobný styk a obstarávateľská činnosť

3.10.1 ZHODNOTENIE STAVU KYBERNETICKEJ BEZPEČNOSTI ZA ROK 2022 ZO STRANY ÚSTREDNÉHO ORGÁNU

3.10.1.1 Hrozby

Ústredný orgán poskytol zhodnotenie hrozieb len v sektore Doprava.

3.10.1.2 Aktivity

MD SR vykonalo analýzu potrieb a požiadaviek sektorov doprava, pošta, elektronické komunikácie, ktorých je gestorom. Na základe analýzy boli zaktualizované sektorové kritériá.

Sú východiskom pre prípravu podkladov na vypracovanie návrhu sektorových vyhlášok, ktoré zadefinujú sektorové bezpečnostné opatrenia pre jednotlivé sektory. Na základe analýzy sek-

torových kritérií aj v súvislosti s NIS 2 ministerstvo identifikovalo požiadavky, ktoré následne budú upravené v sektorových vyhláškach pri transpozícii požiadaviek NIS 2.

3.10.1.3 Plánované aktivity

MD SR plánuje transponovať požiadavky NIS 2 do národnej legislatívy SR s určením kompetencií medzi dotknutými sektormi, vrátane prípravy sektorových vyhlášok pre sektor dopravy, sektor pošty a sektor elektronických komunikácií.

3.10.2 VÝSLEDKY AUDITOV PZS V SEKTORE POŠTA

V sektore Pošta bola odovzdaná iba jedna auditná správa, preto nie je možné vytvoriť anonymizované zhodnotenie výsledkov auditov v sektore.

3.11 Priemysel

Ústredný orgán: Ministerstvo hospodárstva Slovenskej republiky (MH SR)

Počet PZS: 7

Počet PZS s povinnosťou auditu v roku 2022: 7
(možné splniť aj samohodnotením podľa §34a ods. 2 ZoKB)

Počet odovzdaných auditných správ: 2

Počet odovzdaných samohodnotení: 2

Podsektory: Farmaceutický priemysel, Hutnícky priemysel, Chemický priemysel, Inteligentný priemysel

3.11.1 ZHODNOTENIE STAVU KYBERNETICKEJ BEZPEČNOSTI ZA ROK 2022 ZO STRANY ÚSTREDNÉHO ORGÁNU

3.11.1.1 Hrozby

Podľa vyjadrenia ústredného orgánu v roku 2022 MH SR neriešilo žiadne hrozby v sektoroch ani podsektoroch.

3.11.1.2 Aktivity

V spolupráci s ostatnými ústrednými orgánmi MH SR pripomienkovalo Stratégiu kybernetickej obrany SR a Vyhlášku NBÚ, ktorou sa určujú znalostné štandardy v oblasti kybernetickej bezpečnosti.

Zástupca MH SR sa zúčastňoval na viacerých pracovných skupinách súvisiacich s kybernetickou bezpečnosťou. Nad rámec §9 ods. 1 písm. c) zákona č. 69/2018 o kybernetickej bezpečnosti nevykonávali žiadne činnosti.

3.11.1.3 Plánované aktivity

Pre plnohodnotnú koordináciu v oblasti kybernetickej bezpečnosti v sektoroch a podsektoroch, za ktoré je podľa zákona MH SR zodpovedné, plánuje vytvoriť pracovné miesto pre koordináciu kybernetickej bezpečnosti v sektoroch a podsektoroch, resp. pre komunikáciu a koordináciu kybernetickej bezpečnosti s PZS.

3.11.2 Výsledky auditov PZS v sektore Priemysel

V sektore Priemysel boli odovzdané iba dve auditné správy, preto nie je možné vytvoriť dostatočne anonymizované zhodnotenie výsledkov auditov v sektore.

3.12 Voda a atmosféra

Ústredný orgán: Ministerstvo životného prostredia Slovenskej republiky (MŽP SR)

Počet PZS: 20

Počet PZS s povinnosťou auditu v roku 2022: 20 (možné splniť aj samohodnotením podľa §34a ods. 2 ZoKB)

Počet odovzdaných auditných správ: 11

Počet odovzdaných samohodnotení: 3

Podsektory: Meteorologická služba, Vodné stavby, Zabezpečovanie pitnej vody

3.12.1 ZHODNOTENIE STAVU KYBERNETICKEJ BEZPEČNOSTI ZA ROK 2022 ZO STRANY ÚSTREDNÉHO ORGÁNU

3.12.1.1 Hrozby

MŽP SR vníma ako najzávažnejšie hrozby bezprecedentný útok na samostatnú, priamo susediacu krajinu, dezinformácie, rastúci trend phishingových kampaní, distribuované útoky formou odmietnutia služby a energetickú krízu.

3.12.1.2 Aktivity

MŽP SR zameralo svoju činnosť najmä na samotné ministerstvo. Podalo žiadosť o poskytnutie nenávratného finančného príspevku so zameraním na rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v podsektore VS so špecifickým cieľom zvýšenia kybernetickej bezpečnosti v spoločnosti, prioritná os č. 7. Informačná spoločnosť.

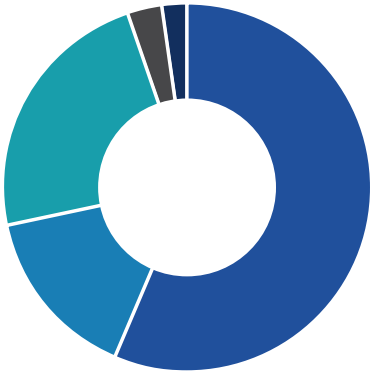
Realizovalo školenia s cieľom zvyšovania úrovne bezpečnostného povedomia. Komunikovalo záujem o spoluprácu pri realizácii projektu Investície č. 6 Posilnenie preventívnych opatrení, zvýšenie rýchlosti detekcie a riešenia incidentov (ITVS), Komponent 17, Plán obnovy a odolnosti zameranej na posilnenie kybernetickej bezpečnosti.

3.12.1.3 Plánované aktivity

V budúcnosti chce MŽP SR inicializovať memorandum o spolupráci pri realizácii projektu Investície č. 6 Posilnenie preventívnych opatrení, zvýšenie rýchlosti detekcie a riešenia incidentov (ITVS), Komponent 17, Plán obnovy a odolnosti zameranej na posilnenie kybernetickej bezpečnosti, ktorý bol prezentovaný zástupcami sekcie kybernetickej bezpečnosti MIRRI. Ďalej chce prehlbovať spoluprácu s KCCKB, SK-CERT a vládnou jednotkou pre riešenie počítačových incidentov v Slovenskej republike CSIRT.SK.

3.12.2 VÝSLEDKY AUDITOV PZS V SEKTORE VODA A ATMOSFÉRA

Národnému bezpečnostnému úradu bolo k 31.12.2022 doručených celkovo 11 auditných správ zo sektora Voda a atmosféra. Nie všetci prevádzkovatelia ale musia vykonať audit. V prípadoch podľa zákona stačí doručenie samohodnotenia, ktoré nie sú v tejto štatistike zahrnuté. Na základe štatistiky súladu s auditnými požiadavkami, v sektore Voda a atmosféra je priemerná percentuálna miera súladu nasledujúca:



Priemerná percentuálna miera súladu (rok 2022)

SÚLAD	56 %
ČIASTOČNÝ SÚLAD	15 %
NESÚLAD	23 %
NEAPLIKOVATEĽNÉ	3 %
OVERENÉ NA INOM MIESTE	2 %

zdroj: Doručené audity 2022, NBÚ

Pri pohľade na jednotlivých PZS v sektore Voda a atmosféra je viac ako polovičná miera súladu s auditnými požiadavkami kontinuálna u väčšiny prevádzkovateľov. Najvyššiu mieru súladu dosiahol PZS , ktorý z 266 auditných požiadaviek dosiahol súlad v 200 požiadavkách, čiastočný súlad v 16 požiadavkách a v 19 nesúlad (16 požiadaviek bolo neaplikovateľných a 15 overených na inom mieste).

Na druhej strane, najnižšia miera súladu bola identifikovaná u PZS , ktorý zo 171 auditných požiadaviek dosiahol súlad v 63 požiadavkách, čiastočný súlad v 58 požiadavkách a nesúlad v 46 požiadavkách (4 požiadavky boli neaplikovateľné).

3.12.3 NAJČASTEJŠIE AUDITNÉ ZISTENIA

Medzi najčastejšie auditné zistenia v sektore Voda a atmosféra patria:

- obsah bezpečnostnej dokumentácie nie je v mnohých prípadoch plne implementovaný alebo nezobrazuje reálny stav vykonávaných činností,
- nie sú implementované princípy najnižších privilégií a oddeľovania právomocí,
- pravidlá popísané v politike nie sú zavedené v praxi,
- nie je implementovaný centrálny nástroj na monitorovanie udalostí v sieti a nie sú zaznamenávané prevádzkové záznamy,
- nie je pripravený komunikačný plán na plnenie havarijných plánov a havarijné plány ako aj plány obnovy nie sú testované.

3.13 Verejná správa

Ústredný orgán:
Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (MIRRI SR)
Ministerstvo obrany Slovenskej republiky (MO SR)
Ministerstvo vnútra Slovenskej republiky (MV SR)
Národný bezpečnostný úrad (NBÚ)

Počet PZS: 1417

Počet PZS s povinnosťou auditu v roku 2022: 1416 (možné splniť aj samohodnotením podľa §34a ods. 2 ZoKB)

Počet odovzdaných auditných správ: 99

Počet odovzdaných samohodnotení: 405

Podsektory: Bezpečnosť, Informačné systémy verejnej správy, Obrana, Utajované skutočnosti

3. 13. 1 ZHODNOTENIE STAVU KYBERNETICKEJ BEZPEČNOSTI ZA ROK 2022 ZO STRANY ÚSTREDNÉHO ORGÁNU

3.13.1.1 Ministerstvo obrany Slovenskej republiky – Obrana

3.13.1.1.1 Hrozby

V hodnotenom období bolo v podmienkach informačnej a komunikačnej infraštruktúry Ministerstva obrany Slovenskej republiky, Ozbrojených síl Slovenskej republiky aj inštitúcií a organizácií zriadených v ich pôsobnosti zaznamenaných množstvo kybernetických bezpečnostných incidentov.

Vo všeobecnosti je možné konštatovať, že išlo o štandardné počítačové bezpečnostné incidenty, ktoré svojim rozsahom a charakterom nevybočujú z radu zaznamenaných kybernetických kampaní voči členským krajinám NATO a EÚ v kontexte aktuálnej geopolitickej situácie.

Za najzávažnejšie kybernetické bezpečnostné incidenty zaznamenané v roku 2022 považujeme snahy o prieniky do informačnej a komunikačnej infraštruktúry rezortu obrany, ale aj bezpečnostné kybernetické incidenty spôsobené tzv. „vnútornou hrozbou“. Za významné z geopolitického hľadiska, avšak s menej významným vplyvom na samotnú kybernetickú bezpečnosť rezortu obrany, považujeme DDoS útoky voči nami monitorovaným informačným a komunikačným infraštruktúram.

Oproti minulosti bol vlani výrazný nárast počtu a sofistikovanosť phisingových a scamových kampaní. V tejto súvislosti bolo v hodnotnom období prešetrovaných viac ako 1 000 mailov.

3.13.1.1.2 Aktivity

Na úseku kybernetickej bezpečnosti rezort obrany spolupracuje s ostatnými ústrednými orgánmi a prevádzkovateľmi základných služieb pri plnení úloh vyplývajúcich zo zákona č. 69/2018 o kybernetickej bezpečnosti. V tejto súvislosti má rezort obrany uzatvorené dohody o spolupráci na úseku kybernetickej bezpečnosti a kybernetickej obrany s viacerými štátnymi a medzinárodnými inštitúciami, ktorým poskytuje rôzne foriem služieb.

Vo všeobecnosti ide okrem iného o monitorovanie informačnej a komunikačnej infraštruktúry, asistenciu a riešenie kybernetických bezpečnostných incidentov, zasielanie bezpečnostných varovaní, vykonávanie a zabezpečovanie výcviku a vzdelávania, či účasť na cvičeniach kybernetickej obrany.

Osobitnou úlohou v hodnotenom období bola participácia na zabezpečovaní auditu kybernetickej bezpečnosti v podmienkach Vzdušných síl Ozbrojených síl Slovenskej republiky a Ústrednej vojenskej nemocnice v Ružomberku – fakultná nemocnica.

V súvislosti so zmenou bezpečnostného prostredia z dôvodu vypuknutia ozbrojeného konfliktu na Ukrajine rezort obrany plnil mimoriadne úlohy na úseku kybernetickej bezpečnosti stanovené Bezpečnostnou radou Slovenskej republiky. Tieto úlohy boli plnené v úzkej súčinnosti s Národným bezpečnostným úradom a Slovenskou informačnou službou.

3.13.1.1.3 Plánované aktivity

Okrem bežných činnosti vyplývajúcich z národnej legislatívy bude nosnou aktivitou rezortu obrany na úseku kybernetickej bezpečnosti plnenie úloh stanovených Akčným plánom pre implementáciu kybernetickej obrany Slovenskej republiky. Cieľom bude celkové posilnenie a zefektívnenie procesov riadenia a výkonu kybernetickej bezpečnosti v podmienkach rezortu obrany.

3.13.1.2 Ministerstvo vnútra Slovenskej republiky – bezpečnosť

3.13.1.2.1 Hrozby

MV SR v podsektore bezpečnosť zaregistrovalo zvýšené aktivity, hrozby a nebezpečné činnosti v oblasti kybernetickej bezpečnosti zamerané na infraštruktúru a informačné systémy ministerstva. Po vypuknutí konfliktu na Ukrajine a najmä po politickom odsúdení tejto agresie a na to nadväzujúcich reštrikcií voči Rusku zaznamenali zvýšený počet ponúk na kybernetické útoky na vládne inštitúcie Slovenskej republiky medzi nimi aj na ministerstvo, kritickú infraštruktúru a strategické podniky.

V nadväznosti na to zaznamenali zvýšenie útokov na infraštruktúru, a to najmä phishing a DDoS útoky, ktoré však nemožno jednoznačne spájať s konfliktom na Ukrajine, ale skôr s vývojom v tejto oblasti. Nemožno opomenúť narastajúci počet phishingových útokov na zamestnancov ministerstva, ktorých úroveň a sofistikovanosť má stúpajúcu tendenciu.

3.13.1.2.2 Aktivity

MV SR zvýšilo monitoring kybernetického priestoru v rezorte vrátane nelegálnych webov, sociálnych sietí, a komunikačných platforiem, kde sa zameralo na činnosť hackerských skupín. Pri preventívnych aktivitách reflektovalo na aktuálne bezpečnostné varovania, zraniteľnosti a bulletiny a ich nasadzovanie a odstraňovanie v infraštruktúre.

V priebehu roka sa zameralo na zvyšovanie kybernetického povedomia zamestnancov ministerstva formou kybernetických cvičení, vzdelávacími aktivitami a rozširovaním komunikačných kanálov na nahlasovanie kybernetických incidentov. Zriadili telefonickú podporu pre riešenie a nahlasovanie kybernetických bezpečnostných incidentov pre zamestnancov rezortu, ktorá je im k dispozícii nepretržite. Ministerstvo odštartovalo druhú fázu budovania technických spôsobilostí zameraných na tzv. Security Operations Center (SOC) zaoberajúci sa riešením bezpečnostných incidentov, monitoringom a dohľadom nad infraštruktúrou a informačnými systémami ministerstva. Nadviazali aj na spoluprácu s ostatnými ústrednými orgánmi a vybudovali si vzájomné komunikačné kanály pre okamžitú výmenu informácií.

3.13.1.2.3 Plánované aktivity

MV SR ako ústredný orgán plánuje v roku 2023 dobudovať technické spôsobilosti zamerané na jednotku SOC s postupnou implementáciou logovacieho a monitorovacieho systému SIEM za účelom identifikácie a riešenia kybernetických bezpečnostných incidentov.

Za dôležitý aspekt kybernetickej bezpečnosti ministerstvo považuje aj školenia bezpečnostných administrátorov a zvyšovanie bezpečnostného povedomia a vedomostí zamestnancov rezortu na pravidelnej báze. V neposlednom rade plánujeme aj implementovanie nástrojov na ochranu dát, dátových prenosov a komunikácie voči externým hrozbám a ich prípadnému zneužitiu.

3.13.1.3 Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky – Verejná správa

3.13.1.3.1 Hrozby

Vládnou jednotkou CSIRT boli vlani identifikované viaceré druhy hrozieb. Významným faktorom bolo najmä vypuknutie vojenského konfliktu na Ukrajine a s tým súvisiace kybernetické útoky rôznych skupín, ktoré smerovali aj na subjekty verejnej správy.

Jednotka zaznamenala mierny nárast nahlásených kybernetických bezpečnostných incidentov, v porovnaní s predchádzajúcim rokom približne o 20 %. V porovnaní s dlhodobým priemerom (roky 2014 až 2021) sa významne zvýšil počet prienikov do systémov (roku 2022 evidovaných spolu 56).

Viac ako dvojnásobne narástol oproti dlhodobému priemeru aj počet zaznamenaných kybernetických bezpečnostných incidentov spôsobených škodlivým kódom. Za hlavné faktory vzniku incidentov možno označiť dlhodobé nedostatky identifikované v podsektore verejnej správy – nedostatočne implementované procesy pre včasné odhaľovanie zraniteľností a nasadzovanie opravných aktualizácií; nedostatočný alebo úplne absentujúci bezpečnostný monitoring; zanedbané vzdelávanie a tréning zamestnancov a s tým spojené zvýšené nebezpečenstvá spôsobené útokmi, ktoré využívajú metódy sociálneho inžinierstva.

Okrem toho boli zachytené kampane cielené na kybernetický priestor Slovenskej republiky, aj svetové kampane prekladané do slovenčiny.

3.13.1.3.2 Aktivity

Ministerstvo v spolupráci s NASES vytvorilo bezpečnostné dohľadové centrum ako základ pre centrálny bezpečnostný monitoring vládnej siete Govnet (NASES), prvých subjektov verejnej správy a riešenie kybernetických bezpečnostných incidentov.

Okrem toho boli vybavené špecializované laboratóriá na penetračné testovania, forenznú a malvérovú analýzu. Za účelom odhaľovania zraniteľností boli v priebehu roka systémom Achilles pravidelne skenované IP adresy dostupné z internetu. Mesačne bolo skenovaných 165 organizácií, ktoré sa zapojili do využívania služby tzv. vulnerability assessmentu.

MIRRI SR aktualizovalo a doplnilo zverejnené metodické usmernenia a vzory bezpečnostnej dokumentácie pre subjekty verejnej správy, ktoré implementujú minimálne bezpečnostné opatrenia v súlade s požiadavkami zákona č. 69/2018 o kybernetickej bezpečnosti, zákona č. 95/2019 o informačných technológiách vo verejnej správe a ich vykonávacími predpismi.

Okrem plnenia úloh z uznesení vlády úspešne uzavrela dopytové výzvy Rozvoj governance informačnej a kybernetickej bezpečnosti v podsektore verejnej správy a v zdravotníckych zariadeniach, ktorých cieľom bolo podporiť PZS a orgánom riadenia na zvýšenie miery súladu s legislatívnymi požiadavkami, ktoré sú na nich kladené, a to najmä inventarizácia aktív, spracovanie bezpečnostnej dokumentácie, analýza rizík, implementácia log manažment systému a bezpečnostného dohľadového centra ako služby.

Z viac ako 120 žiadateľov o nenávratné finančné príspevky za spolu 20 miliónov eur tvorili takmer polovicu mestá a samosprávne kraje. MIRRI SR distribuovalo informáciu pre mestá a obce o metodických materiáloch, ktorými podporujeme tvorbu bezpečnostnej dokumentácie aj s metodikou analýzy rizík, ktorú vydal NBÚ.

Vládna jednotka CSIRT počas roku 2022 zároveň preškolila viac ako 500 zamestnancov VS v oblasti KIB.

MIRRI SR tiež vytvorí centrálny portál pre kybernetickú bezpečnosť a pripraví jednotný metodický rámec, ktorý bude zahŕňať doplnenie a aktualizáciu vzorovej dokumentácie pre povinné osoby; pracovná skupina pre legislatívu sa zameria na možnosti zjednodušenia legislatívnych požiadaviek v oblasti kybernetickej a informačnej bezpečnosti.

3.13.2 VÝSLEDKY AUDITOV PZS V SEKTORE VEREJNÁ SPRÁVA

Národnému bezpečnostnému úradu bolo k 31.12.2022 doručených celkovo 99 auditných správ zo sektora Verejná správa. Nie všetci prevádzkovatelia ale musia vykonať audit. V prípadoch podľa zákona stačí doručenie samohodnotenia, ktoré nie sú v tejto štatistike zahrnuté. Na základe štatistiky súladu s auditnými požiadavkami, v sektore Verejná správa je priemerná percentuálna miera súladu nasledujúca:

Priemerná percentuálna miera súladu (rok 2022)

SÚLAD	37 %
ČIASTOČNÝ SÚLAD	17 %
NESÚLAD	36 %
NEAPLIKOVATEĽNÉ	5 %
OVERENÉ NA INOM MIESTE	4 %

zdroj: Doručené audity 2022, NBÚ

V sektore Verejná správa je možné identifikovať najmenšiu priemernú mieru súladu (a naopak najvyššiu priemernú mieru nesúladu zo všetkých sektorov – s výnimkou podsektora Tepelná energetika, kde však je významne menej identifikovaných prevádzkovateľov).

Najvyššiu mieru súladu dosiahol PZS , ktorý z 233 auditných požiadaviek dosiahol súlad v 230 požiadavkách, čiastočný súlad v 2 požiadavkách a v žiadnej z požiadaviek nemal nesúlad (1 požiadavka bola neaplikovateľná).

Na druhej strane, najnižšia miera súladu bola identifikovaná u PZS , ktorý zo 179 auditných požiadaviek dosiahol súlad v 5 požiadavkách, čiastočný súlad v 61 požiadavkách a nesúlad v 109 požiadavkách (4 požiadavky boli neaplikovateľné).

3.13.3 NAJČASTEJŠIE AUDITNÉ ZISTENIA

Medzi najčastejšie auditné zistenia v sektore Verejná správa patria:

- nebol preukázaný systém riadenia kybernetickej bezpečnosti,
- bezpečnostná stratégia kybernetickej bezpečnosti ani ďalšia bezpečnostná dokumentácia nebola predložená,
- manažér kybernetickej bezpečnosti nie je formálne menovaný, je v konflikte záujmov a má nevhodne kumulované zodpovednosti,
- analýza rizík nie je zakotvená ako proces v interných predpisoch ani metodicky popísaná, nevykonáva sa,
- v organizácii sa nachádzajú vysoko privilegované účty, ktoré sú spoločné a nemajú definovaných vlastníkov a účel,
- v organizácii neexistuje definícia závažného kybernetického bezpečnostného incidentu, organizácia nevypracovala postupy a nemá dostatočné schopnosti na detekciu, zvládanie a poučenie sa z prípadných incidentov.

3.14 Zdravotníctvo

Ústredný orgán: Ministerstvo zdravotníctva Slovenskej republiky (MZ SR)

Počet PZS: 90

Počet PZS s povinnosťou auditu v roku 2022: 85
(možné splniť aj samohodnotením podľa §34a ods. 2 ZoKB)

Počet odovzdaných auditných správ: 61

Počet odovzdaných samohodnotení: 13

Podsektory: Zdravotnícke zariadenia (vrátane nemocníc a súkromných kliník)

3.14.1 Zhodnotenie stavu kybernetickej bezpečnosti za rok 2022 zo strany ústredného orgánu

3.14.1.1 Hrozby

Vzhľadom na citlivosť zdravotníckych dát je sektor zdravotníctva čoraz častejšie vystavený kybernetickým hrozbám a incidentom ohrozujúcich bezpečnostný atribút dát, kontinuitu a kvalitu zdravotnej starostlivosti. Zdravotnícke zariadenia disponujú zastaranými informačno-komunikačnými technológiami a zdravotníckym personálom s nedostatočným povedomím v oblasti kybernetickej bezpečnosti.

Za najzávažnejšie hrozby v sektore zdravotníctva možno považovať nedostatočnú podporu najvyššieho vedenia organizácie a s tým súvisiaci nedostatok adekvátne vyčlenených finančných prostriedkov potrebných na navyšovanie a rozvoj úrovne kybernetickej bezpečnosti; absentujúcu komplexnosť IT systémov z titulu používania množstva rôznych nástrojov a riešení; nesprávne chápanú zdieľanú zodpovednosť za bezpečnosť v prípade používania cloudových riešení; vendor lock-in a IoT zariadenia obsahujúce početné a ľahko zneužiteľné zraniteľnosti.

Budovaním odolnosti voči kybernetickým hrozbám prostredníctvom správnych bezpečnostných opatrení a iných osvedčených postupov či zlepšením detekcie incidentov a reakcie na ne sa však tento sektor dá ochrániť.

3.14.1.2 Aktivity

Ústredný orgán pre sektor zdravotníctva v zmysle ustanovenia § 9 ods. 1 písm. c) zákona č. 69/2018 o kybernetickej bezpečnosti aktívne spolupracuje s jednotkami, ktoré v rozsahu svojej pôsobnosti zodpovedajú za riešenie kybernetických bezpečnostných incidentov a vykonávajú preventívne služby a reaktívne služby.

Ministerstvo zdravotníctva Slovenskej republiky usmerňuje organizácie v jeho zakladateľskej, zriaďovateľskej a akcionárskej pôsobnosti v oblasti kybernetickej bezpečnosti.

Bezpečnostný výbor Ministerstva zdravotníctva Slovenskej republiky pre oblasť informačnej a kybernetickej bezpečnosti v postavení poradného orgánu ministra rokoval a rozhodoval o otázkach smerujúcich k eliminácií a riešeniu následkov spôsobených kybernetickými incidentmi v sektore zdravotníctva.

Za účelom včasnej a efektívnej reakcie na kybernetické útoky sa realizuje projekt implementácie centrálneho nástroja na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov zabezpečujúceho bezpečnostný dohľad nad sieťami a informačnými systémami zaznamenávaním prevádzky týchto sietí a informačných systémov.

V zmysle projektu Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v podsektore vernej správy je účinná zmluva o poskytnutí nenávratného finančného príspevku s cieľom navýšenia kybernetickej bezpečnosti v sektore zdravotníctva.

3.14.1.3 Plánované aktivity

Ústredný orgán pre sektor zdravotníctva s cieľom zníženia rozsahu škody spôsobenej zneužitím konkrétnej zraniteľnosti konkrétnou hrozbou vypracuje postupy riešenia bezpečnostných incidentov pre najčastejšie sa vyskytujúce bezpečnostné hrozby vznikajúce pri poskytovaní zdravotnej starostlivosti.

V súvislosti s transpozíciou Smernice Európskeho parlamentu a Rady (EÚ) 2022/2555 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2) Ministerstvo zdravotníctva začne komunikáciu s Národným bezpečnostným úradom pri definovaní typov subjektov v sektore zdravotníctva v kontexte prípravy novely zákona č. 69/2018 o kybernetickej bezpečnosti.

3.14.2 VÝSLEDKY AUDITOV PZS V SEKTORE ZDRAVOTNÍCTVO

Národnému bezpečnostnému úradu bolo k 31.12.2022 doručených celkovo 61 auditných správ zo sektora Zdravotníctvo. Nie všetci prevádzkovatelia ale musia vykonať audit. V prípadoch podľa zákona stačí doručenie samohodnotenia, ktoré nie sú v tejto štatistike zahrnuté. Na základe štatistiky súladu s auditnými požiadavkami, v sektore Zdravotníctvo je priemerná percentuálna miera súladu nasledujúca:

Priemerná percentuálna miera súladu (rok 2022)

SÚLAD	42 %
ČIASTOČNÝ SÚLAD	15 %
NESÚLAD	35 %
NEAPLIKOVATEĽNÉ	4 %
OVERENÉ NA INOM MIESTE	4 %

zdroj: Doručené audity 2022, NBÚ

V sektore Zdravotníctvo je menej ako polovičná miera súladu s auditnými požiadavkami kontinuálna naprieč všetkými prevádzkovateľmi a zároveň vysoká miera nesúladu.

Najvyššiu mieru súladu dosiahol PZS , ktorý z 266 auditných požiadaviek dosiahol súlad v 202 požiadavkách, čiastočný súlad v 16 požiadavkách a v 21 nesúlad (13 požiadaviek bolo neaplikovateľných a 14 overených na inom mieste).

Na druhej strane, najnižšia miera súladu bola identifikovaná u PZS , ktorý z 266 auditovaných požiadaviek dosiahol súlad v 6 požiadavkách, čiastočný súlad v 23 požiadavkách a nesúlad v 210 požiadavkách (15 požiadaviek bolo neaplikovateľných a 12 overených na inom mieste).

3.14.3 NAJČASTEJŠIE AUDITNÉ ZISTENIA

Medzi najčastejšie auditné zistenia v sektore Zdravotníctvo patria:

- u PZS nie je definovaná štruktúra riadenia, výkonu a kontroly v oblasti kybernetickej bezpečnosti,
- nie sú stanovené pravidlá a zodpovednosti pri implementácii opatrení vyplývajúcich z analýzy rizík, nie je stanovená zodpovednosť za identifikáciu a evidenciu aktív,
- PZS nedostatočne rieši šifrovú ochranu informácií,
- väčšina procesov v oblasti šifrovania a managementu kľúčov nie je formalizovaná,
- vzdialený prístup do interných sietí a IS nie je zabezpečený.

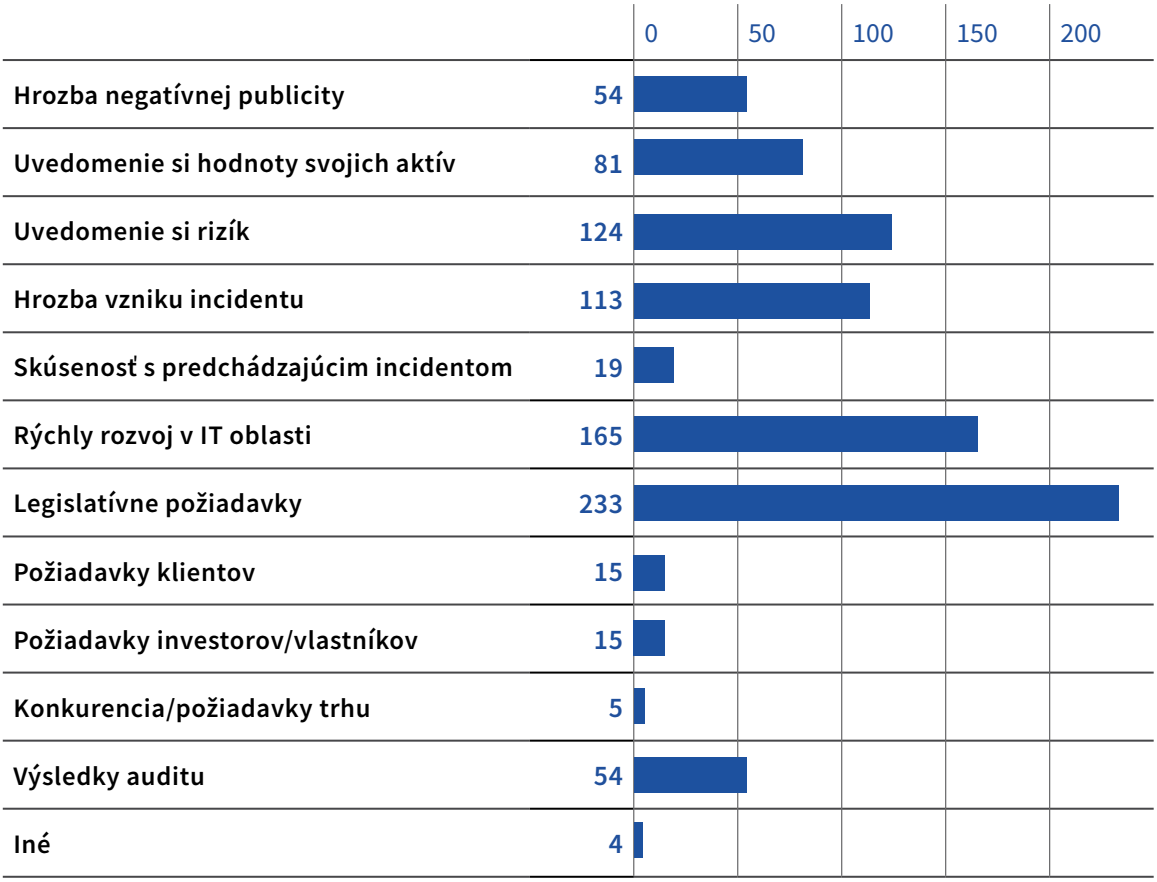
3.15 Prieskum stavu kybernetickej bezpečnosti u PZS

Národné centrum kybernetickej bezpečnosti SK-CERT vykonalo medzi PZS prieskum zameraný na stav kybernetickej bezpečnosti za rok 2022. Prieskum bol vykonaný na dobrovoľnej báze, pričom dáta poskytlo celkovo 270 prevádzkovateľov naprieč sektormi. Otázky v prieskume boli postavené tak, aby bolo možné vyhodnotiť viaceré aspekty riadenia, financovania a rozvoja kybernetickej bezpečnosti u regulovaných subjektov.

3.15.1 FAKTORY OVPLYVŇUJÚCE ZVYŠOVANIE ÚROVNE KYBERNETICKEJ BEZPEČNOSTI

Z pohľadu PZS bez rozdielu sektora medzi faktormi, ktoré ovplyvňujú zvyšovanie úrovne kybernetickej bezpečnosti v organizácii, prevládajú legislatívne požiadavky, za ktorými nasleduje rýchly rozvoj v IT oblasti a uvedomenie si rizík (PZS mohli označiť viacero možností).

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



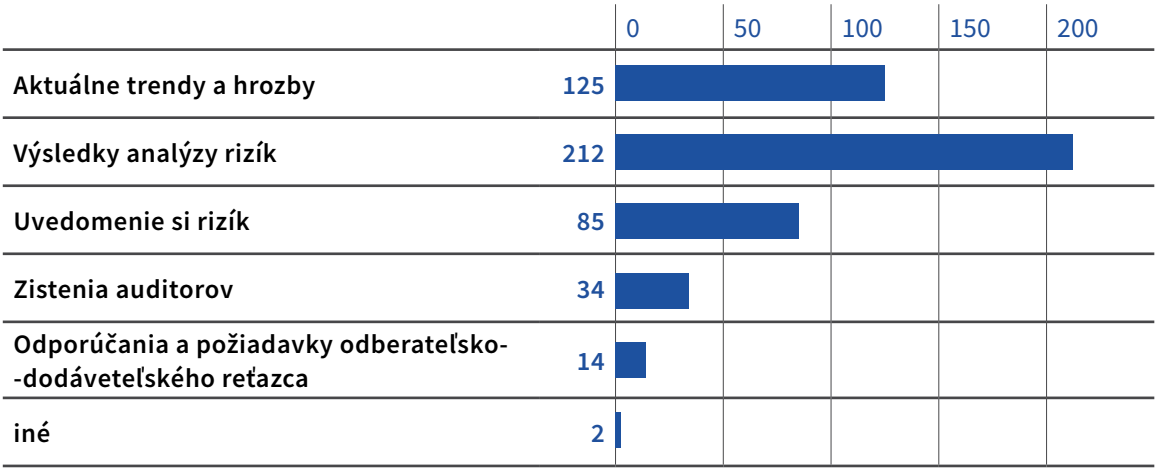
zdroj: Prieskum názorov PZS za rok 2022, NCKB SK-CERT, marec 2022

Ak sa na otázku pozrieme z pohľadu sektorov, nájdeme mierne odlišný pohľad v sektore Doprava, kde najvýznamnejším faktorom zvyšovania úrovne kybernetickej bezpečnosti je výsledok auditu, v sektoroch Elektronické komunikácie a Digitálna infraštruktúra je to hrozba vzniku incidentu, pri sektore Energetika uvedomenie si hodnoty vlastných aktív a v sektore Zdravotníctvo je najvýznamnejším faktorom uvedomenie si rizík a hrozba vzniku incidentu.

3. 15. 2 IDENTIFIKÁCIA PRIORÍT A SMEROVANIA PRE OBLASŤ KYBERNETICKEJ BEZPEČNOSTI

PZS definujú svoje priority a smerovania v oblasti kybernetickej bezpečnosti najmä na základe analýzy rizík, aktuálnych trendov a hrozieb a výsledkov auditov.

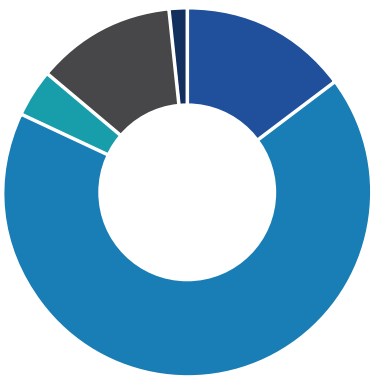
Aké sú faktory, ktoré majú vo vašej organizácii najvyšší vplyv na zvyšovanie úrovne kybernetickej bezpečnosti?



zdroj: Prieskum názorov PZS za rok 2022, NCKB SK-CERT, marec 2022

3. 15. 3 VNÍMANIE AKTIVÍT ÚSTREDNÉHO ORGÁNU

Aktivity jednotlivých ústredných orgánov (orgán zodpovedný za sektor podľa zákona o kybernetickej bezpečnosti) väčšina PZS vníma veľmi dobre až uspokojivo. Až 12,2 % prevádzkovateľov však nevníma žiadne aktivity alebo pôsobenie Ústredného orgánu (najmä v sektore Verejná správa).



Ako vnímate aktivity a pôsobonie Ústredného orgánu podľa zákona 69/2018 Z. z. o kybernetickej bezpečnosti, ktorý je zodpovedný za váš sektor?

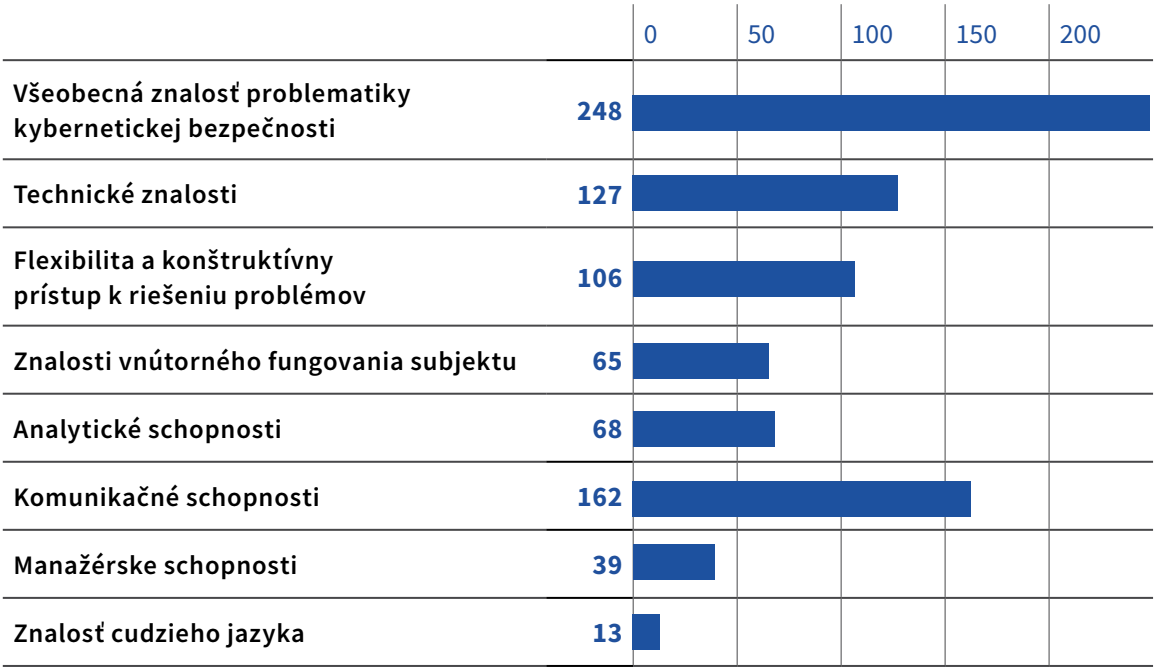
VEĽMI DOBRE	14,8 %
USPOKOJIVO	67,4 %
NIE SOM VÔBEC SPOKOJNÝ S AKTIVITAMI A PÔSOBENÍM ÚSTREDNÉHO ORGÁNU	4,1 %
NEVNÍMAM ŽIADNE AKTIVITY, ALEBO PÔSOBENIE ÚSTREDNÉHO ORGÁNU	12,2 %
INÉ	1,5 %

zdroj: Prieskum názorov PZS za rok 2022, NCKB SK-CERT, marec 2022

3. 15. 4 SKÚSENOSTI A ZNALOSTI PRACOVNÍKOV

PZS si u svojich pracovníkov najviac cenia všeobecnú znalosť problematiky kybernetickej bezpečnosti, komunikačné schopnosti a technické znalosti. Miernym špecifikom je sektor Digitálna infraštruktúra, kde sú najviac cenené analytické schopnosti a sektor Voda a atmosféra, v ktorom si prevádzkovatelia najviac cenia flexibilitu a konštruktívny prístup k riešeniu problémov (PZS mohli označiť viacero možností).

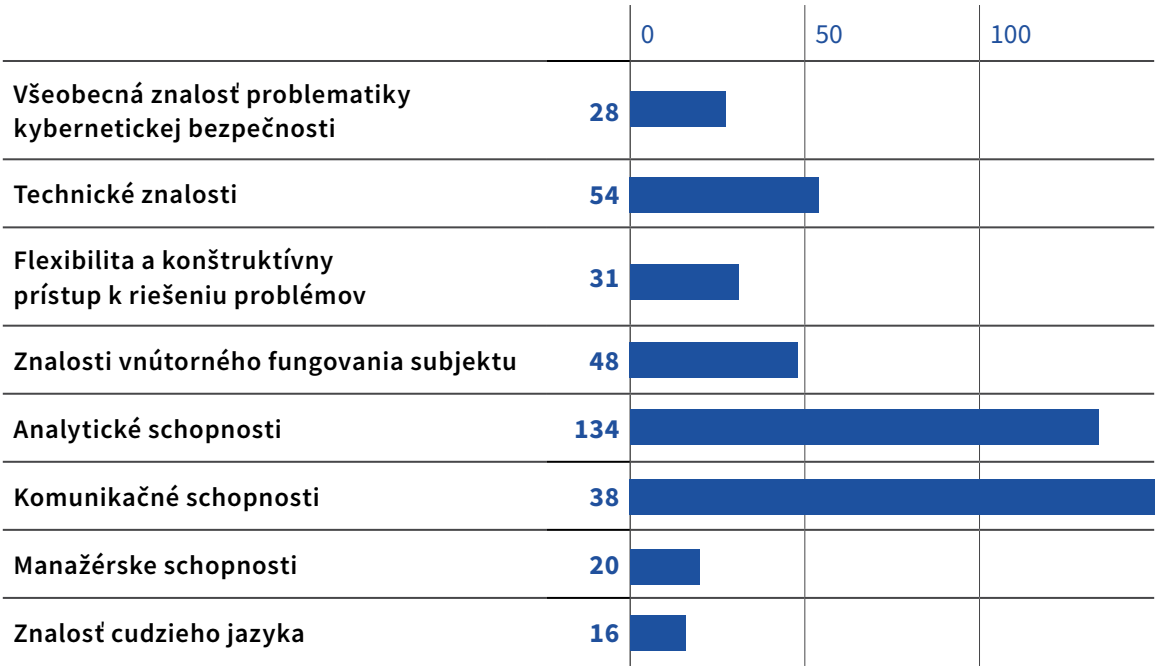
Ktoré znalosti a skúsenosti pracovníkov kybernetickej bezpečnosti si najviac ceníte?



zdroj: Prieskum názorov PZS za rok 2022, NCKB SK-CERT, marec 2022

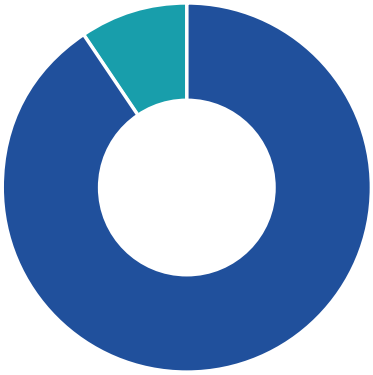
Za najviac nedostatkové znalosti a schopnosti prevádzkovatelia považujú analytické schopnosti, technické znalosti a znalosti vnútorného fungovania subjektu (PZS mohli označiť viacero možností).

Ktoré znalosti a skúsenosti pracovníkov kybernetickej bezpečnosti považujete momentálne najviac za nedostatkové?



zdroj: Prieskum názorov PZS za rok 2022, NCKB SK-CERT, marec 2022

Väčšina z oslovených PZS poskytuje svojim zamestnancom možnosti na zvyšovanie povedomia v oblasti kybernetickej bezpečnosti a takisto u väčšiny z nich je takéto vzdelávanie povinné.



Poskytujete svojim zamestnancom možnosti na zvyšovanie povedomia v oblasti kybernetickej bezpečnosti?

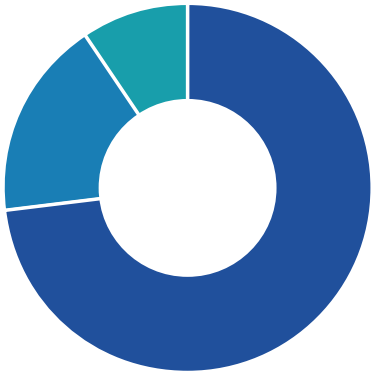
ÁNO	90,7 %
NIE	9,3 %

zdroj: Prieskum názorov PZS za rok 2022, NCKB SK-CERT, marec 2022

Je takéto vzdelávanie pre vašich zamestnancov povinné alebo dobrovoľné?

SÚLAD	73,3 %
ČIASTOČNÝ SÚLAD	17,4 %
NESÚLAD	9,3 %

zdroj: Prieskum názorov PZS za rok 2022, NCKB SK-CERT, marec 2022



3. 15. 5 RIADENIE KYBERNETICKEJ BEZPEČNOSTI

Implementáciu bezpečnostných opatrení nad rámec zákona vykonáva 25 % opýtaných prevádzkovateľov a ide zväčša o prevádzkovateľov v sektore Bankovníctvo (regulácia vo finančnom sektore) a v sektore Verejná správa (zákon č. 95/2019 o informačných technológiách vo verejnej správe).

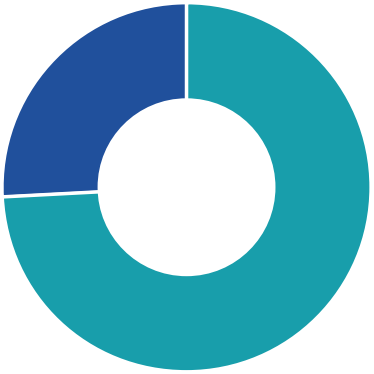
Viacero prevádzkovateľov uviedlo, že implementujú opatrenia podľa zákona č. 18/2018 o ochrane osobných údajov (resp. podľa nariadenia GDPR). Niektorí prevádzkovatelia pri tejto otázke odpovedali, že sa riadia medzinárodnými štandardami (ktoré však nie sú právne záväzné).

Implementujete bezpečnostné opatrenia nad rámec zákonných povinností?

ÁNO	25 %
NIE	75 %

zdroj: Prieskum názorov PZS za rok 2022, NCKB SK-CERT, marec 2022

Oslovení prevádzkovatelia vo väčšine vykonávajú pravidelné posúdenie prijatých bezpečnostných opatrení z vlastnej iniciatívy.



Vykonávate pravidelné posúdenie efektívnosti prijatých bezpečnostných opatrení z vlastnej iniciatívy?

ÁNO	74,4 %
NIE	25,6 %

zdroj: Prieskum názorov PZS za rok 2022, NCKB SK-CERT, marec 2022

Z prevádzkovateľov základných služieb, ktorí boli oslovení, má takmer 62 % vypracované plány kontinuity činnosti organizácie, avšak len 12 % z nich vykonáva pravidelný test a overuje jeho využiteľnosť aspoň raz za rok.

Najvýraznejší rozdiel medzi existenciou plánov kontinuity činnosti a ich pravidelným testovaním je v sektore Verejná správa, kde iba 8,6 % subjektov, ktoré majú vypracované plány kontinuity činnosti, ich aj pravidelne testuje. Naopak v sektore Digitálna infraštruktúra skoro 67 % opýtaných subjektov svoje plány pravidelne testuje.

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

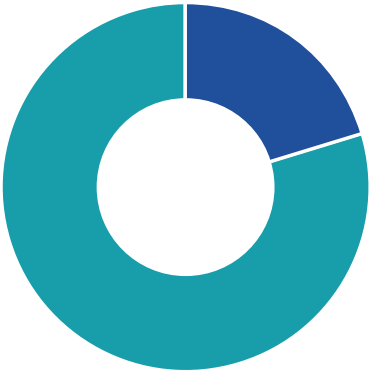
ÁNO	38,2 %
NIE	61,8 %

zdroj: Prieskum názorov PZS za rok 2022, NCKB SK-CERT, marec 2022

Vykonávate test BCM, pri ktorom overujete jeho využiteľnosť, aspoň raz za rok?

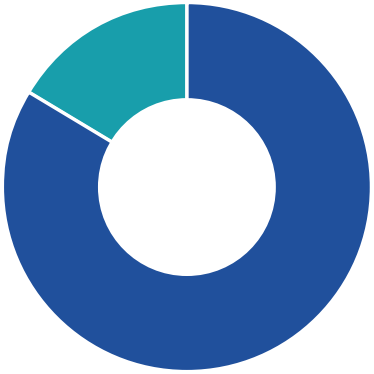
ÁNO	12,6 %
NIE	87,4 %

zdroj: Prieskum názorov PZS za rok 2022, NCKB SK-CERT, marec 2022



3.15.6 FINANCOVANIE

Pre viac ako 83 % oslovených prevádzkovateľov je rozpočet na kybernetickú bezpečnosť súčasťou rozpočtu na IT. Rozpočet na kybernetickú bezpečnosť je u väčšiny prevádzkovateľov flexibilný, teda mení sa podľa potreby.



Je rozpočet na kybernetickú bezpečnosť súčasťou rozpočtu na IT?

ÁNO	83,7 %
NIE	16,3 %

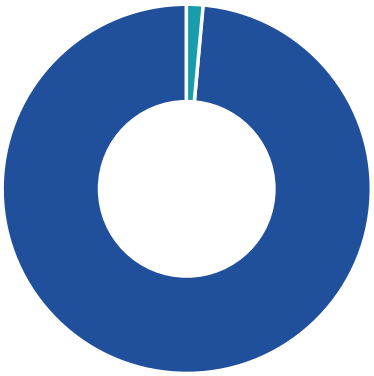
zdroj: Prieskum názorov PZS za rok 2022, NCKB SK-CERT, marec 2022

Ako máte stanovený ročný rozpočet na kybernetickú bezpečnosť?

JE FIXNÝ	12,6 %
MENÍ SA PODĽA POTREBY	87,4 %

zdroj: Prieskum názorov PZS za rok 2022, NCKB SK-CERT, marec 2022

PZS typicky nevyčleňujú osobitné prostriedky na výnimočné situácie – iba 1,5 % opýtaných má vyčlenené finančné prostriedky na pokrytie BCM.

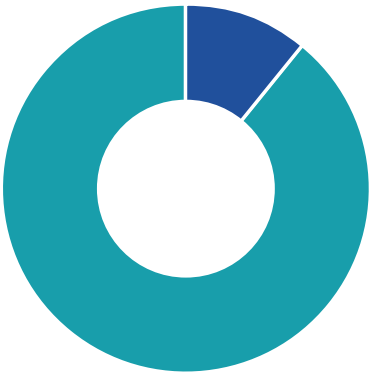


Máte osobitne určený rozpočet na BCM (výnimočné situácie)?

ÁNO	1,5 %
NIE	98,5 %

zdroj: Prieskum názorov PZS za rok 2022, NCKB SK-CERT, marec 2022

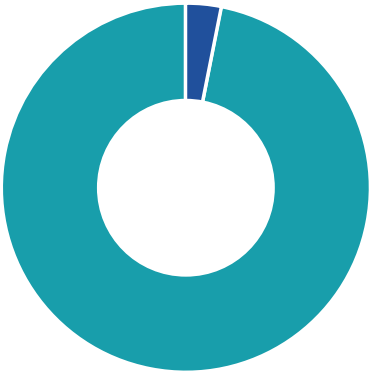
V oblasti poistenia oslovení PZS príliš nevyužívajú možnosti poistenia či už svojich aktív alebo poistenie vo vzťahu ku kybernetickej bezpečnosti (čo môže byť ovplyvnené trhovou ponukou takéhoto typu poistenia).



Máte uzatvorené poistenie svojich informačných aktív?

ÁNO	11,1 %
NIE	88,9 %

zdroj: Prieskum názorov PZS za rok 2022, NCKB SK-CERT, marec 2022



Máte uzatvorené poistenie vo vzťahu ku kybernetickej bezpečnosti?

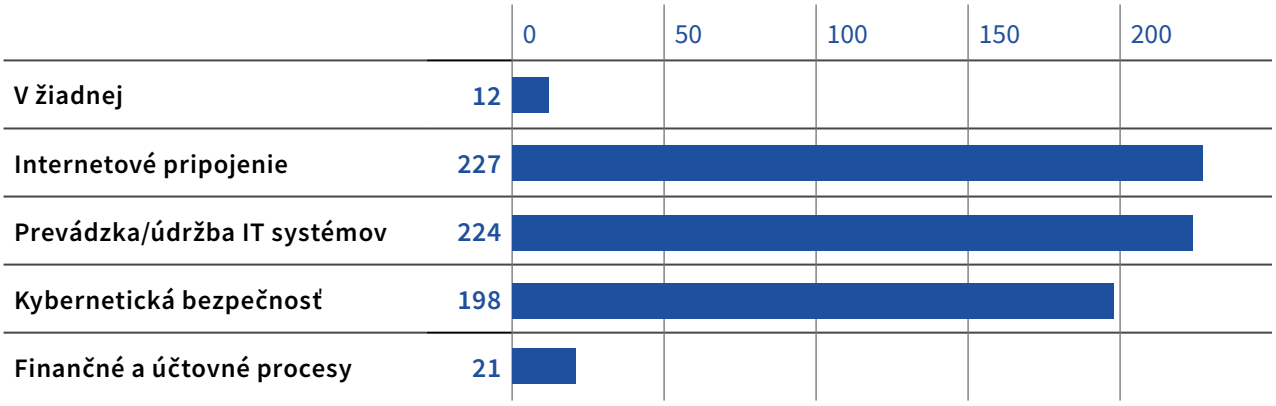
ÁNO	3,3 %
NIE	96,7 %

zdroj: Prieskum názorov PZS za rok 2022, NCKB SK-CERT, marec 2022

4.15.7 SLUŽBY

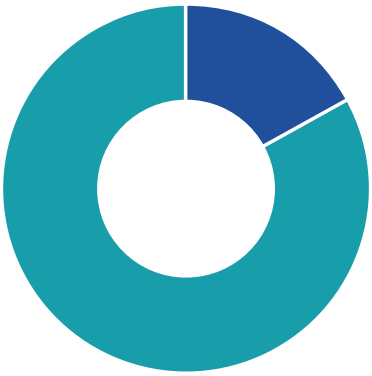
Oslovení PZS pri externých službách najviac využívajú internetové pripojenie, prevádzku/údržbu IT systémov a kybernetickú bezpečnosť.

V akých oblastiach využívate externé zdroje/procesy (outsourcing)?



zdroj: Prieskum názorov PZS za rok 2022, NCKB SK-CERT, marec 2022

Manažované služby bezpečnosti (Managed Security Services) využíva 17 % opýtaných prevádzkovateľov, pričom pri väčšine prevádzkovateľov ide najmä o služby v oblasti kybernetickej bezpečnosti.



Využívate na procesy kybernetickej bezpečnosti služby poskytovateľov MSS (Managed Security Services), resp. spoločnosti, ktoré ponúkajú niektoré oblasti kybernetickej bezpečnosti ako službu?

ÁNO	**17 %**
NIE	**83 %**

zdroj: Prieskum názorov PZS za rok 2022, NCKB SK-CERT, marec 2022

4 VZDELÁVANIE V OBLASTI KYBERNETICKEJ BEZPEČNOSTI

4.1 Vzdelávanie na základných a stredných školách

Oproti roku 2021 sa vo vzdelávaní na základných a stredných školách v podstate nič nezmenilo. Tento stav je podčiarknutý aj stavom plnenia úloh, ktoré v oblasti vzdelávania vyplývajú z Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025. Opäť musíme konštatovať, že vzdelávanie a šírenie povedomia o kybernetickej bezpečnosti nie je na základných školách vôbec koncepčne riešené.

Vzdelávanie v tejto oblasti by malo podliehať najnovším technologickým trendom a poznatkom. V sylabách Ministerstva školstva, vedy, výskumu a športu Slovenskej republiky sa výučba kybernetickej bezpečnosti vyskytuje len veľmi okrajovo na hodinách informatiky.

Ak si uvedomíme rozsah problematiky kybernetickej bezpečnosti a porovnáme ho so skutočnou hodinovou dotáciou informatiky na jednotlivých školách, kde sa žiaci majú učiť nielen bezpečnosti, ale najmä digitálnej gramotnosti, môžeme konštatovať tento stav za absolútne nepostačujúci.

Kybernetická bezpečnosť je prierezovou témou, a preto možno očakávať výučbu v tejto oblasti aj na iných predmetoch ako informatika, čo sa však takisto nedeje. Takýmto prístupom k výučbe minimálne základov kybernetickej bezpečnosti sa prehlbujú problémy, ktoré následne spôsobujú vyššiu mieru obetí kybernetických útokov, ale aj nedostatočný počet expertov na problematiku kybernetickej bezpečnosti.

Absolútne nedostačujúci záujem o uchopenie problematiky kybernetickej bezpečnosti vo vzdelávaní kompetentným orgánom musia teda suplovať len nadšení učitelia, občianske združenia a niekoľko jednotlivcov. Tí však nedokážu dostatočne pokryť spoločenskú potrebu.

Chýbajúce učebné pomôcky, ktoré takisto vznikajú len vďaka nadšeniu jednotlivcov a občianskych združení, nedostatočná časová dotácia a takisto aj nedostatok pedagógov v oblasti kybernetickej bezpečnosti budú rokmi viesť k stagnácii a prehĺbeniu problémov, ktoré môžu spôsobiť neodstrániteľný deficit povedomia o kybernetickej bezpečnosti.

4.2 Vzdelávanie na vysokých školách

V roku 2021 NBÚ s KCCKB vykonali na relevantných vysokých školách prieskum, ktorý odzrkadľoval stav vysokoškolského vzdelávania v oblasti kybernetickej bezpečnosti na Slovensku.

Prieskum bol zameraný najmä na zisťovanie aktuálneho stavu v oblasti existencie akreditovaných študijných programov, odborov alebo predmetov. Za rok 2022 možno konštatovať, že situácia sa v tejto oblasti nezmenila a relevantný vysoké školy, ktoré indikovali existenciu programu, odboru alebo predmetu si svoju akreditáciu udržali.

Akreditácia programu, odboru alebo predmetu je dlhodobý proces a výsledky snáh iných vysokých škôl, ktoré sa začali so snahami o akreditáciu nedávno, budú viditeľné v nasledujúcich rokoch.

Možno však konštatovať, že vzdelávanie expertov na vysokých školách napreduje lepšie ako všeobecné vzdelávanie o kybernetickej bezpečnosti na nižších stupňoch vzdelania. Relevantné vysoké školy pochopili dôležitosť vzdelávania odborníkov. Môžu však narážať na viacero problémov, napríklad na nezáujem študentov študovať kybernetickú bezpečnosť, nakoľko uprednostňujú iné študijné smery.

Napriek postupnému zlepšovaniu úrovne vzdelávania v oblasti kybernetickej bezpečnosti na vysokých školách však tieto stále nedokážu pokryť potreby trhu práce v dostatočnom počte absolventov.

4.3 Vzdelávanie dospelých

Vzdelávanie dospelých v kybernetickej bezpečnosti patrí aj do gescie KCCKB ako príspevkovej organizácie NBÚ. Vzdelávanie dospelých je jednou z možností, ako začať pokrývať potreby trhu práce v oblasti kybernetickej bezpečnosti.

Nosnou témou počas roku 2022 bola príprava novej sady špecializačných kurzov a workshopov pre existujúcich aj budúcich manažérov kybernetickej bezpečnosti.

Za uvedené obdobie sa KCCKB podarilo najmä:
- vydať aktualizovanú Vzdelávaciu schému v kybernetickej bezpečnosti
- aktualizovať viacero existujúcich kurzov kybernetickej bezpečnosti
- do portfólia školení zaradiť nový typ praktickej vzdelávacej aktivity – workshop
- otvoriť nové školenia (verejné a neverejné termíny):
  - riadenie rizík v KB (1 dňový kurz + 1 dňový workshop)
  - klasifikácia informácií a kategorizácia sietí a IS (1 dňový kurz + 1 dňový workshop)
  - riadenie informačnej bezpečnosti podľa ISO/IEC 27001
- realizovať aktivity v rámci zvyšovania bezpečnostného podvedomia:
  - účasť na odborných konferenciách kybernetickej bezpečnosti (EPI, ITAPA)
  - participácia na komunikačných aktivitách pre odbornú a laickú verejnosť na web stránke a sociálnych sieťach KCCKB

Za rok 2022 KCCKB realizovalo celkovo **5 kurzov** „Prehľad KB“, **20 kurzov** „Manažér KB“ a **12 špecializačných kurzov** a workshopov. Celkovo sa na týchto aktivitách zúčastnilo **473 účastníkov**.

Priestor pre ďalšie zlepšenia v roku 2023 KCCKB vidí opätovne najmä v dosiahnutí dohody o spolupráci vo vzdelávaní s ďalšími subjektami verejnej správy, menovite MIRRI a orgánmi samosprávy.

5 VYHODNOTENIE PLNENIA AKČNÉHO PLÁNU REALIZÁCIE NÁRODNEJ STRATÉGIE KYBERNETICKEJ BEZPEČNOSTI NA ROKY 2021 AŽ 2025

Pre účely vyhodnocovania Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025 bol NBÚ zriadený Monitorovací výbor pre implementáciu akčného plánu.

Tento výbor je nezávislým poradným orgánom riaditeľa úradu. Jeho úlohou je monitorovať a koordinovať implementáciu úloh, ktoré vyplývajú z Akčného plánu. Predsedom výboru je príslušník úradu, členmi výboru sú zástupcovia všetkých subjektov, ktoré majú v akčnom pláne minimálne jednu úlohu.

Jednou z úloh monitorovacieho výboru je každoročne pripraviť odpočet plnenia úloh akčného plánu. Tvorí sa vždy za predchádzajúci rok. Odpočet za rok 2022 obsahuje aj odpočet úloh z roku 2021, ktoré doposiaľ neboli splnené.

Stav plnenia jednotlivých úloh je rozdelený na:

- **splnené** – úloha je splnená v súlade s merateľnými ukazovateľmi,
- **priebežne plnené** – úlohy s časovým horizontom „priebežne“, pričom pri takýchto úlohách je uvedený spôsob priebežného plnenia úloh,
- **plní sa** – subjekt úlohu ešte nesplnil, ale indikuje, že na nej pracuje a má v pláne ju dokončiť,
- **nesplnené** – subjekt úlohu nesplnil a ani neuviedol, či na nej pracuje alebo má v pláne ju dokončiť,
- **neodpočtované** – zodpovedný subjekt k úlohe nezaslal odpočet.

Plnenie úloh akčného plánu napreduje len v niektorých oblastiach. Veľa úloh viacerých subjektov sú v stave rozpracovania. Najhoršou oblasťou plnenia úloh je vzdelávanie. Subjekt s najviac úlohami v tejto oblasti – Ministerstvo školstva, vedy, výskumu a športu, indikovalo takmer všetky úlohy ako nesplnené bez indikácie, ako naozaj na tom jednotlivé úlohy sú.

Ide o jednu z najdôležitejších oblastí v oblasti kybernetickej bezpečnosti a zodpovedný subjekt mu neprikladá adekvátnu dôležitosť a meškaním jednotlivých úloh sa vzďaľuje splneniu strategických cieľov, ktoré boli identifikované v Národnej stratégii kybernetickej bezpečnosti na roky 2021 až 2025.

Odpočet plnenia akčného plánu spolu s podrobným popisom stavu plnenia jednotlivých úloh sa nachádza v prílohe tejto správy.

6 AKTIVITY A OPATRENIA

NBÚ aj v roku 2022 potvrdil svoje smerovanie v budovaní bezpečnostného prostredia, ktoré zodpovedá princípom prijatých v Stratégii Európskej únie pre bezpečnostnú úniu na obdobie rokov 2020 až 2025 a Stratégie kybernetickej bezpečnosti EÚ v digitálnej dekáde.

Prioritami naďalej zostávajú zvyšovanie odolnosti kybernetickej infraštruktúry, kybernetickej bezpečnosti a nastavovanie procesov na zaistenie bezpečnosti ako aj vo fyzickom, tak aj v digitálnom prostredí.

Pokiaľ ide o rozvoj medzinárodných vzťahov úradu tie príslušníci rozvíjali v rámci medzinárodného zastúpenia Slovenskej republiky, kde sa zúčastňovali a podieľali na tvorbe bezpečnostných politík na pôde EÚ a NATO a takisto rozvíjali rôzne medzinárodné aktivity, bilaterálne vzťahy a regionálnu spoluprácu

6.1 Národná legislatíva

V roku 2022 úrad legislatívnymi zmenami v **zákone č. 69/2018 Z. z. o kybernetickej bezpečnosti** reagoval na narastajúci počet aktérov na dezinformačnej scéne v kybernetickom priestore. Zákonom č. 55/2022 o niektorých opatreniach prijatých v súvislosti so situáciou na Ukrajine sa ustanovila povinnosť úradu rozhodnúť o blokovaní škodlivého obsahu alebo škodlivej aktivity smerujúcej do/z kybernetického priestoru SR a zabezpečiť aj samotné vykonanie blokovania (s prechodným obmedzením do 30. 06. 2022).

Zákonom č. 231/2022, ktorým sa mení a dopĺňa zákon č. 69/2018, sa predĺžila táto lehota do 30. 09. 2022. V máji 2022 bol predložený do medzirezortného pripomienkového konania návrh zákona, ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z., ktorého cieľom bolo reflektovať na niektoré otázky aplikačnej praxe v súvislosti s výkonom blokovania, zodpovednosti, procesného postupu pri vydávaní rozhodnutia a jeho realizácii a úprava zverejňovania rozhodnutí na webovom sídle úradu. V novembri 2022 bol vládny návrh zákona predložený na rokovanie Národnej rady Slovenskej republiky (I. čítanie), avšak do ďalšieho čítania zákon neprešiel.

Ďalej úrad v roku 2022 zrealizoval legislatívny proces dvoch vykonávacích predpisov zákona č. 69/2018. Pôvodný **návrh novely vyhlášky Národného bezpečnostného úradu č. 436/2019 o audite kybernetickej bezpečnosti a znalostnom štandarde audítora** sa v priebehu legislatívneho procesu transformoval na návrh novej vyhlášky o audite kybernetickej bezpečnosti s cieľom aktualizovať pravidlá výkonu auditu kybernetickej bezpečnosti, jeho časový rozsah trvania, periodicitu a stanovenie náležitosti záverečnej správy o výsledkoch auditu. Nová vyhláška Národného bezpečnostného úradu č. 493/2022 o audite kybernetickej bezpečnosti nadobudla účinnosť 1. januára 2023.

Vyhláška Národného bezpečnostného úradu č. 492/2022, ktorou sa ustanovujú znalostné štandardy v oblasti kybernetickej bezpečnosti má za cieľ určiť minimálne odborné znalosti pre jednotlivých používateľov sietí a informačných systémov vykonávajúcich činnosti a úlohy v oblasti kybernetickej bezpečnosti.

Znalostné štandardy rovnako tvoria rámec pre vytvorenie vzdelávacích programov na vzdelávacích inštitúciách, čím sa vypĺňa priestor nielen pre budovanie kvalitného bezpečnostného povedomia v oblasti kybernetickej bezpečnosti, ale aj pre zvyšovanie kvality vzdelávacích procesov. Uvedené následne ovplyvní aj kvalitu pracovníkov vykonávajúcich činnosti v oblasti kybernetickej bezpečnosti v štátnych a v súkromných organizáciách. Zavedenie a definovanie znalostných štandardov a ich aplikovanie v oblasti kybernetickej bezpečnosti je základným prvkom budovania stabilného a predvídateľného bezpečnostného prostredia. Aj táto vyhláška nadobudla účinnosť 1. januára 2023.

6.2 Európska únia

Príslušníci úradu sa zúčastňovali na pravidelných zasadnutiach **Bezpečnostného výboru Rady EÚ (CSC), Skupiny expertov Európskej komisie pre bezpečnostnú politiku (ComSEG) a Bezpečnostného výboru Európskej služby pre vonkajšiu činnosť (EEAS).**

Na pôde Rady EÚ v roku 2022 naďalej pokračovala revízia bezpečnostných pravidiel s cieľom odstrániť nedostatky identifikované v aplikačnej praxi a zvýšiť komfort pre adresátov týchto pravidiel. V uvedených pracovných formátoch sa úrad aktívne zapájal do prípravy bezpečnostných noriem tak, aby bola zvýšená úroveň ochrany utajovaných skutočností a pokračoval aktívnym zapojením v procese revízie bezpečnostných pravidiel.

V oblasti ochrany utajovaných skutočností bolo na pôde EÚ najdiskutovanejšou témou pripravované nariadenie EK o spoločných jednotných pravidlách ochrany utajovaných skutočností EÚ pre všetky inštitúcie, orgány a agentúry EÚ. Členské štáty sa zhodujú, že (právny) základ všetkých bezpečnostných pravidiel EÚ je stanovený Radou platnými dokumentami.

Na pravidelnom zasadaní Bezpečnostného výboru Európskej služby pre vonkajšiu činnosť (SC EEAS) sa EEAS v rámci ich činnosti venovali revízii programu bezpečnostného povedomia a zintenzívnenia školenia personálu o možných kybernetických rizikách. V tejto súvislosti pripravuje príručku, ktorá má pomôcť nielen nováčikom pri práci s EUCI. Zamestnanci EEAS prispeli k budovaniu odolnosti a bezpečnostného povedomia na zahraničných delegáciách EÚ pomocou školení, workshopov a podporných programov.

Úrad mal pravidelné a aktívne zastúpenie na rokovaniach **Horizontálnej pracovnej skupiny pre kybernetické záležitosti (HWPCI)** počas francúzskeho a českého predsedníctva v Rade EÚ.

V legislatívnej oblasti bol rok 2022 dôležitým míľnikom pre posilnenie kybernetickej bezpečnosti EÚ, keďže bola prijatá smernica stanovujúca pravidlá na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti Únie (Smernica NIS 2). Hlavnou úlohou úradu v tejto súvislosti bude jej transpozícia do národnej legislatívy.

Ďalším dôležitým a nadväzujúcim krokom bolo predstavenie návrhu právneho aktu o kybernetickej odolnosti, ktorý stanoví požiadavky kybernetickej bezpečnosti pre produkty s digitálnymi prvkami. Rozhodujúcou úlohou v tomto smere bude jednoznačné nastavenie pravidiel zabezpečenia vysokej úrovne kybernetickej bezpečnosti EÚ s víziou stanovenia štandardov aj pre zvyšok sveta.

Rokovania HWPCI sa zaoberali aj negociovaním nelegislatívnych dokumentov. Za najdôležitejšie z nich a na ktorých forme sa podieľalo aj NBÚ možno považovať Strategický kompas, Závery Rady EÚ o kybernetickom postoji únie, Závery Rady o bezpečnosti dodávateľského reťazca IKT a návrh novej politiky kybernetickej obrany predstavenej v tzv. obrannom balíku EK. Oblasť kybernetickej diplomacie bola vo veľkej miere ovplyvnená udalosťami u východného partnera EÚ.

Rokovania HWPCI sa preto sústredili aj na formulovanie textov vyhlásení vysokého predstaviteľa EÚ o odsúdení kybernetických útokov ruských aktérov na Ukrajinu, ktoré predchádzali a naďalej pretrvávali počas invázie Ruska na Ukrajinu. V tejto súvislosti sa niekoľkokrát otvorila otázka revízie súboru nástrojov kybernetickej diplomacie (CDT).

Na hlavnom **Bezpečnostnom výbore pre Vesmírne programy EÚ** v Agentúre Európskej únie pre vesmírny program (EUSPA) boli hlavným bodom diskusie vypracovanie Bezpečnostných pokynov pre jednotlivé programy (PSI).

Rozsiahle dokumenty boli pripravované v jednotlivých podporných pracovných skupinách, či už ide o Pracovnú skupinu pre bezpečnosť programu Galileo, GOVSATCOM, Copernicus alebo Egnos. V súvislosti s programom GOVSATCOM boli vytvorené nové iniciatívy EK, ide o ad hoc skupinu EuroQCI (Quantum Communication Infrastructure), ktorá sa podieľa na diskusii o prierezovej téme kvantovej komunikačnej infraštruktúry. Má byť využitá v súvislosti s programom GOVSATCOM a má zabezpečiť vysokú mieru šifrovania, odolnosti a v konečnom dôsledku aj bezpečnosti, keďže táto sieť má byť prispôsobená aj na prenos utajovaných skutočností.

Medzi kľúčové priority **Skupiny pre spoluprácu** aj naďalej patrí implementácia Smernice Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Európskej únii (smernica NIS), a s tým súvisiaca aplikácia jednotlivých nástrojov.

V roku 2022 k tejto úlohe pribudli aj ďalšie dôležité témy ako „Hodnotenie rizika a rizikové scenáre“

čo vyplýva aj z úlohy pre Skupinu pre spoluprácu a adresne zo Záverov Rady pre rozvoj pozície EÚ ku kybernetickej bezpečnosti, „Krízové riadenie“, „Organizácia a potencionálne oblasti spolupráce v budúcnosti v Skupine pre spoluprácu“ a „Koordinované zverejňovanie zraniteľnosti“.

ENISA realizovala cestovnú mapu potrieb pre cvičenia pre oblasť kybernetickej bezpečnosti a štáty si zdieľali svoje skúsenosti pokiaľ išlo o najzávažnejšie incidenty a hrozby v oblasti kybernetickej bezpečnosti, ktoré ich počas roka zasiahli (dominoval opäť ransomvér).

V roku 2022 pôsobil úrad a SK-CERT vo viacerých **Work Streamoch** Skupiny pre spoluprácu:

Work Stream 3 – Skupina zameraná na notifikačné povinnosti PZS. Skupina v rámci svojej činnosti sa venovala zlepšeniu jednotlivých nástrojov, ktoré slúžia k notifikačným povinnostiam pre členské krajiny. Zároveň sa ČŠ venovali príprave „Výročnej správy“, ktorá obsahovala priame vstupy od členských štátov, ktoré si tak splnili svoje informačné a notifikačné povinnosti. Finálna správa je vždy schválená Skupinou pre spoluprácu a úrad ju pripomienkuje a zasiela svoje vstupy.

Work Stream 7 – Skupina pre riešenie kybernetických bezpečnostných incidentov veľkého rozsahu. Na úrovni tejto skupiny sa pokračovalo v príprave operačných procedúr pri riešení závažných incidentov s medzinárodným presahom a zástupcovia úradu na nich aktívne participujú.

Work Stream 10 – Skupina pre Digitálnu infraštruktúru. V rámci platformy sa v roku 2022 ČŠ venovali príslušným orgánom a ich povinnosti definovať a dodržiavať spoločný prístup k implementačným požiadavkám pre poskytovateľov digitálnych služieb (PDS). Zámerom smernice NIS bolo definovať maximálny harmonizačný rámec pre PDS, ktorí budú podliehať jurisdikcii jediného kompetentného orgánu (príslušného orgánu v krajine hlavného sídla v EÚ) pre všetky ich činnosti v Únii.

Work Stream 5G – Skupina zabezpečenie a ochranu 5G sietí. Na úrovni EK úrad aktívne pôsobil v pracovnej skupine pre problematiku kybernetickej bezpečnosti v sieťach piatej generácie (5G). EK uverejnila súbor odporúčaných opatrení na zmiernenie rizík súvisiacich s výstavbou a prevádzkou 5G sietí, tzv. 5G Toolbox. Aplikácia týchto opatrení sa preniesla aj na národnú úroveň najmä v podobe aplikačnej praxe.

Work Stream 12 – Skupina pre sektor zdravotníctva. Experti, ktorí pracujú v uvedenej pracovnej skupine sa museli vysporiadať s aktuálnymi problémami, ktoré so sebou priniesla pandémia COVID-19 v oblasti kybernetickej bezpečnosti práve v sektore zdravotníctva. Súčasne aktívne pracujú na návrhu dokumentu o implementácii smernice NIS (sektorové pravidlá a odporúčania, pokiaľ ide o nastavenie kybernetických bezpečnostný opatrení v danom segmente) v sektore zdravotníctva, ktorý nadobúda reálnu podobou. Ďalším zámerom tejto platformy je zvýšenie opatrení v rámci kybernetickej bezpečnosti subjektov, ktoré spadajú do oblasti zdravotníctva.

Nová pracovná platforma **Work stream 15** – Skupina pre bezpečnosť dodávateľských reťazcov, kde aj úrad potvrdil svoje členstvo pri jej sformovaní sa zameriavala počas roka 2022 na posilnenie bezpečnosti dodávateľského reťazca IKT a tiež k prvým krokom k riešeniu hrozieb neželaných strategických závislostí v dodávateľských reťazcoch IKT.

Počas roka nabrala na vážnosti aj komunita **EU CyberNet** zainteresovaných subjektov, ktorá združuje národné orgány a inštitúcie pôsobiace v oblasti kybernetickej bezpečnosti, expertné skupiny pre danú oblasť, think-thanky a akademické inštitúcie so sídlom v členských štátoch EÚ. EU CyberNet organizovala počas roka množstvo workshopov a konferencií, ktoré boli venované aktuálnym témam kybernetickej bezpečnosti, pričom príslušníci si zvyšovali svoju odbornosť a poznatky aktívnou účasťou na týchto aktivitách a budovali kapacity úradu.

6.3 NATO

Chod Organizácie Severoatlantickej zmluvy (NATO) bol vo veľkej miere ovplyvnený geopolitickým dianím, a to najmä situáciou na Ukrajine – jedného z hlavných partnerov NATO s kandidátskymi ašpiráciami na vstup.

Kybernetické útoky na Ukrajinu vykonávané ruskými aktérmi, ktoré predchádzali samotnej nevyprovokovanej invázii a stále trvajú, boli zo strany generálneho tajomníka NATO Jensa Stoltenberga jednoznačne odsúdené verejnými vyhláseniami.

Výbor kybernetickej obrany (CDC) sa v značnej miere zaoberal poskytnutím pomoci vojnou zasiahnutému partnerovi, ako aj urýchlením jeho vstupu do Centra výnimočnosti kybernetickej obrany v Talline. Vojna na Ukrajine priniesla aj isté ponaučenia z nekoordinovaného postupu pri poskytovaní pomoci

a júlový madridský samit v tejto súvislosti priniesol dohodu spojencov na zriadení virtuálnej jednotky rýchlej kybernetickej odozvy, ktorá by dobrovoľne združovala kybernetických expertov spolupracujúcich pri reakciách na závažné škodlivé kybernetické aktivity.

V uplynulom roku sa konalo historicky prvé zasadnutie národných kybernetických koordinátorov na pôde Severoatlantickej rady (NAC). Hlavnou témou diskusie boli národné príspevky kybernetickej obrany do celkovej aliančnej zostavy síl pre odstrašenie a obranu v reakcii na dianie na vojnu na Ukrajine. Za Slovenskú republiku sa na rokovaní zúčastnil riaditeľ SK-CERT.

Naďalej prebiehali rokovania Bezpečnostného výboru NATO (SC) vo všetkých svojich formátoch – vo formáte bezpečnostných politík, bezpečnosti komunikačných a informačných systémov (CISS) a na najvyššej úrovni – úroveň riaditeľov bezpečnostných úradov ČŠ. Tento rok bol z pohľadu ochrany utajovaných skutočností NATO v znamení pokračovania v rozsiahlej revízii bezpečnostných pravidiel NATO.

Úrad sa zúčastnil aj na zasadaní expertnej skupiny špecialistov z členských štátov na oblasť priemyselnej bezpečnosti (Capability Team) a počas októbrového zasadnutia predostreli Bezpečnostnému úradu NATO (NOS) a delegátom svoje návrhy na zmenu Smernice o utajovaných projektoch a priemyselnej bezpečnosti. Formát bezpečnosti komunikačných a informačných systémov v rámci NATO SC sa venoval dvom hlavným dokumentom, Smernici o kybernetickej bezpečnosti a NATO Stratégii o umelej inteligencii (AI). Počas októbrového zasadania na najvyššom formáte (Principals level) bol predostretý účastníkom program na rok 2023, ktorý bol rozšírený o 2 nové podporné dokumenty.

Prvý z nich sa bude zaoberať tele-prácou a druhý adresuje Zahraničné vlastníctvo, kontrola a vplyv na firmy zúčastňujúce sa NATO kontraktov (FOCI).

6.4 Regionálna spolupráca

Na základe rotácie predsedníctva krajín, ktoré sú členmi Stredoeurópskej platformy pre kybernetickú bezpečnosť (CECSP) NBÚ v zastúpení Slovenskej republiky v roku 2022 predsedal tejto platforme. V platforme sú svojimi expertmi zastúpené krajiny Vyšehradskej štvorky (Česká republika, Maďarsko, Poľsko, Slovenská republika) a Rakúsko. Úrad zorganizoval partnermi vysokohodnotené pracovné stretnutie vo fyzickom formáte, ktoré bolo 12. septembra v Bratislave.

Predmetom samotných rokovaní boli aktuálne témy, ktoré na úrovni EÚ rezonovali počas celého roka 2022 a súčasne sa partneri v rámci týchto tém snažili nájsť spoločné prieniky a vzájomnú podporu. Medzi tie najdôležitejšie témy patrili: „Nové výzvy, ktoré si vyžadujú adaptívny, koordinovaný a inovatívny prístup k transpozícii smernice NIS 2.0 a „Koordinované oznamovanie zraniteľnosti“.

Slovenská republika sa zviditeľnila aj prezentáciou venovanou téme umiestnenia kompetenčného centra v systéme regulácie kybernetickej bezpečnosti Slovenskej republiky a predstavili sme náš koncept pre komunitu kybernetickej bezpečnosti v Slovenskej republike. Komplexnú a ucelenú štúdiu, ktorá sa týkala auditu kybernetickej bezpečnosti na Slovensku prezentoval zástupca KCCKB. Experti si vymenili vzájomné poznatky a uviedli príklady dobrej praxe pokiaľ ide o prípravný proces transpozície smernice NIS 2.0.

6.5 Bilaterálne vzťahy

Úrad rozvíjal bilaterálne vzťahy na dennodennej báze naprieč všetkými pracovnými platformami, či už pri kontakte počas zasadnutia pracovných skupín, alebo pri ad hoc plnení úloh práve na bilaterálnej úrovni.

NBÚ podpísal medzinárodnú bilaterálnu dohodu medzi vládou Slovenskej republiky a vládou Spojených štátov amerických o bezpečnostných opatreniach na ochranu utajovaných skutočností. Nová zmluva výrazne prospieva k prehĺbeniu vzťahov a zintenzívneniu spolupráce medzi oboma krajinami.

V priebehu roka bola odštartovala komunikácia o uzatvorení zmluvy o ochrane utajovaných skutočností s Holandským kráľovstvom, čo sa vzhľadom na aplikačnú prax ukazuje ako dôležitá priorita na nadchádzajúce obdobie. Rozširovanie sféry spolupráce prebiehalo aj smerom na Východnú Áziu a počas uplynulého roka sa uskutočnili dve zahraničné návštevy z Indonézskej republiky, počas ktorej sa účastníci zaujímali o oblasť ochrany utajovaných skutočností a kybernetickej bezpečnosti.

V oboch oblastiach bola nadviazaná bližšia spolupráca s cieľom uzatvoriť medzinárodnú zmluvu

o ochrane utajovaných skutočností a tiež aj memorandum o spolupráci v oblasti kybernetickej bezpečnosti. V súvislosti s medzinárodnou spoluprácou sa uskutočnila v septembri 2022 študijná návšteva v rámci EÚ programu TAIEX, počas ktorej navštívila Slovenskú republiku delegácia zo Severného Macedónska. Príslušníci úradu pripravili viacero prezentácií a vzdelávacích aktivít najmä k vyžiadanej téme ohľadom fyzickej bezpečnosti a objektovej bezpečnosti. Koncom roka 2022 bola Bezpečnostnou radou Európskej vesmírnej agentúry (ESA) schválená bezpečnostná zmluva medzi vládou Slovenskej republiky a ESA.

6.6 Vydávanie bulletinov a varovaní

SK-CERT už od svojho začiatku pravidelne vydáva bezpečnostné bulletiny a varovania. Dokumenty obsahujú upozornenia na zraniteľnosti v rôznych systémoch a službách. Sú určené najmä pre PZS a PDS, na ich odber sa však môže prihlásiť bezplatne ktokoľvek.

Hodnotenie zraniteľností, ktoré sa nachádzajú v bulletinoch a varovaniach, sa riadi medzinárodne uznávanou metodikou CVSS 3.1, ktorá sa používa na hodnotenie zraniteľností softvérových a hardvérových produktov.

Bezpečnostné bulletiny sú vydávané každý týždeň a obsahujú zoznam zraniteľností strednej a vysokej závažnosti podľa metriky CVSS 3.1. Bezpečnostné varovania obsahujú kritické zraniteľnosti a v prípade, že majú veľký vplyv, SK-CERT vydáva varovanie aj pre zraniteľnosti s nižšou závažnosťou.

Nasledujúci prehľad uvádza počet vydávaných týždenných bezpečnostných bulletinov a bezpečnostných varovaní za rok 2022

	Celkový počet bulletinov za rok 2022	Celkový počet varovaní za rok 2022	Celkovo zraniteľností
JANUÁR	4	11	**36**
FEBRUÁR	4	28	**46**
MAREC	5	17	**47**
APRÍL	4	22	**45**
MÁJ	5	22	**53**
JÚN	4	27	**55**
JÚL	4	32	**60**
AUGUST	5	23	**46**
OKTÓBER	4	23	**50**
NOVEMBER	5	21	**59**
DECEMBER	4	22	**69**
SPOLU	**52**	**271**	**629**

6.7 Cybergame 2022

V roku 2022 zorganizoval NBÚ súťaž v oblasti kybernetickej bezpečnosti pod názvom CyberGame. Cieľom tejto kyberbezpečnostnej hry bolo zaujímavou a hravou formou priblížiť tému verejnosti, šíriť povedomie o kybernetickej bezpečnosti, hrozbách a spôsoboch ochrany svojich dôležitých dát, motivovať ľudí venovať sa tejto oblasti a hľadať či podporovať talenty.

Hra bola určená pre kohokoľvek – nadšencov, špecialistov, študentov, učiteľov, zamestnancov verejnej správy; bez rozdielu veku, pohlavia, zamestnania alebo vzdelania. Hra trvala od 1. marca do 10. mája 2022 a pre zapojenie sa stačil obyčajný notebook a voľne dostupné nástroje z internetu.

CyberGame kombinovala technické a netechnické úlohy a celkovo bolo pripravených viac ako 50 úloh. Hra bola rozdelená na 4 vetvy:

- malvérová analýza – analýza vzoriek škodlivého kódu. Cieľom bolo zistiť, ako škodlivý kód funguje a nájsť ďalšie spojitosti,
- forenzná analýza –hráči museli nájsť digitálne stopy,
- obfuskácia a kryptografia – hráči analyzovali šifrované alebo kódované informácie,
- OSINT – analýza otvorených zdrojov,

Každá vetva obsahovala niekoľko scenárov (príbehov), ktoré počas trvania hry pribúdali, pričom v každom scenári bolo niekoľko úloh, ktoré na seba logicky nadväzovali. Jednotlivé scenáre boli odstupňované podľa náročnosti. Náročnejší scenár znamenal viac bodov. Princípom hry bolo zbierať body za tzv. „vlajky“. Vyhral ten, kto získal najviac bodov. Ak hráč použil pomôcku, body sa mu zredukovali. Za dokončenie celého scenára bolo bonusové ohodnotenie.

Celkovo sa do hry registrovalo 1 242 hráčov, z čoho 600 hráčov aktívne hralo. Najmladší hráč mal 12 rokov, najstarší 62. Celkovo sa do hry zapojilo 452 študentov, 125 ženských hráčov, 37 učiteľov a 225 hráčov z verejnej správy. Celkový víťaz, najlepšia hráčka v ženskej kategórii a najlepší študent vyhrali fakultatívny zájazd do malvérového laboratória v kanadskom Montreali, ostatní súťažiaci v ostatných kategóriách vyhrali vecné ceny. CyberGame v roku 2022 získala ocenenie IT projekt roka, tzv. slovenského IT Oscara.

6.8 Činnosť KCCKB

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti je štátnou príspevkovou organizáciou s právnou subjektivitou, ktorá je na štátny rozpočet zapojená každoročne upravovaným príspevkom poskytovaným úradom v súlade s ustanovením § 21 a § 24 zákona č. 523/2004 o rozpočtových pravidlách verejnej správy.

Kompetenčné centrum od začiatku roka 2022 plní úlohu Národného koordinačného centra (NCC) v sieti európskych koordinačných centier a Európskeho centra priemyselných, technologických a výskumných kompetencií v zmysle nariadenia Európskeho parlamentu a Rady EÚ č. 2021/887.

V roku 2022 získalo KCCKB akreditáciu od Európskej komisie, ktorá potvrdzuje, že Kompetenčné centrum disponuje potrebnými kapacitami na manažovanie európskych finančných fondov. Akreditácia bola nutná podmienka na získanie financovania úloh spojených s výkonom NCC. Po úspešnom podaní európskeho projektu v programe Digitálna Európa bola koncom roka 2022 podpísaná grantová dohoda medzi Európskou komisiou a KCCKB. Finančná hodnota projektu sú 4 milióny eur s 50 % spolufinancovaním a jeho trvanie bolo stanovené na dva roky so začiatkom v novembri 2022.

Podstatnou časťou úloh Kompetenčného centra je výkon posudzovania zhody v kybernetickej bezpečnosti v zmysle nariadenia Európskeho parlamentu a Rady EU č. 2019/881 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií (Nariadenie o kybernetickej bezpečnosti) a neskôr, po jeho prijatí, aj v zmysle Nariadenia Európskeho parlamentu a Rady o kybernetickej odolnosti (The European Cyber Resilience Act – CRA).

Vzhľadom na to, že Európska komisia od roku 2020 zdržiava schválenie harmonizovaných európskych certifikačných schém, v súčasnosti ešte nie je možné požiadať Slovenskú národnú akreditačnú službu o akreditáciu na posudzovanie zhody výrobkov, procesov a služieb v oblasti kybernetickej bezpečnosti podľa osobitného predpisu a podľa normy STN EN ISO/IEC 17065 . Okrem produktov (t. j. výrobkov, pro-

cesov a služieb) je kompetenčné centrum už v súčasnosti akreditované na certifikáciu:

- audítorov a manažérov kybernetickej bezpečnosti podľa osobitného predpisu a normy STN EN ISO/IEC 17024,
- integrovaných systémov manažérstva kvality, manažérstva informačnej bezpečnosti, manažérstva IT služieb a manažérstva kontinuity činností, podľa normy STN EN ISO/IEC 17021.

Dôležitým výhľadom Kompetenčného centra je splniť požiadavky na žiadosť o zápis znaleckého ústavu do zoznamu znalcov, tlmočníkov a prekladateľov Ministerstva spravodlivosti Slovenskej republiky pre odbory a odvetvia relevantné v kybernetickej bezpečnosti.

Ministerstvo spravodlivosti Slovenskej Republiky v legislatívnom procese 2022/806 akceptovalo návrh Národného bezpečnostného úradu na rozšírenie znaleckých odvetví o nové odvetvie Kybernetická bezpečnosť. Pokiaľ bude v zmysle návrhu novelizovaná vyhláška Ministerstva spravodlivosti Slovenskej republiky č. 228/2018, ktorou sa vykonáva zákon č. 382/2004 o znalcoch, tlmočníkoch, Kompetenčné centrum má ambíciu byť prvou znaleckou organizáciou, ktorá bude vykonávať znalecké činnosti v novom znaleckom odvetví.

7 ZOZNAM SKRATIEK

CSIRT.SK – vládna jednotka CSIRT (Computer Security Incident Response Team)

KCCKB – Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

MDV SR – Ministerstvo dopravy a výstavby Slovenskej republiky

MF SR – Ministerstvo financií Slovenskej republiky

MH SR – Ministerstvo hospodárstva Slovenskej republiky

MIRRI SR – Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky

MO SR – Ministerstvo obrany Slovenskej republiky

MV SR – Ministerstvo vnútra Slovenskej republiky

MZ SR – Ministerstvo zdravotníctva Slovenskej republiky

MZVEZ SR – Ministerstvo zahraničných vecí a európskych záležitostí Slovenskej republiky

MŽP SR – Ministerstvo životného prostredia Slovenskej republiky

NCC – Národné koordinačné centrum kybernetickej bezpečnosti

NCKB SK-CERT – Národné centrum kybernetickej bezpečnosti SK-CERT

NBÚ – Národný bezpečnostný úrad

PDS – poskytovateľ digitálnej služby

PZS – prevádzkovateľ základnej služby