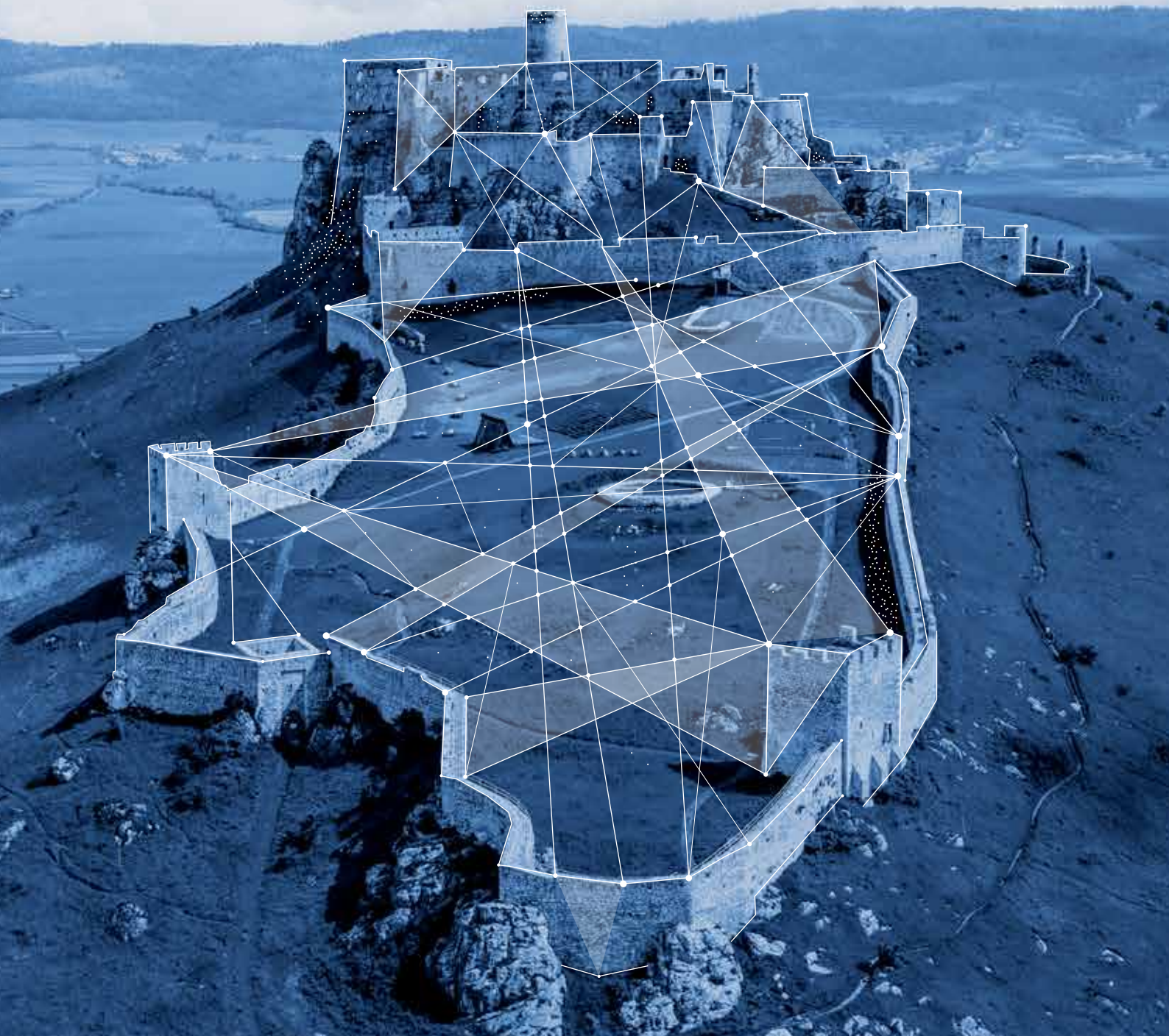
NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SPRÁVA O KYBERNETICKEJ BEZPEČNOSTI

v Slovenskej republike v roku 2023



NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

SPRÁVA O KYBERNETICKEJ BEZPEČNOSTI

v Slovenskej republike
v roku 2023

OBSAH

1. Prehľad hrozieb za rok 2023

1.1 Globálne trendy

Dianie v kybernetickom priestore v roku 2023 ovplyvňovalo viacero faktorov. Kybernetický rozmer vojny Ruska proti Ukrajine bol stále prítomný, pričom sofistikovanosť a intenzita kybernetických útokov značne neklesla.

V tomto vojenskom konflikte ide stále o významný prvok ovplyvňujúci boje, spravodajskú činnosť a kybernetickú bezpečnosť oboch strán. Skúsenosti z konfliktu v oblasti kybernetickej bezpečnosti a obrany budú v budúcnosti cenným poučením nielen pre bojujúce strany.

Geopolitické súperenie štátov v kybernetickom priestore sa symptomaticky odzrkadlilo v špionážnych aktivitách viacerých APT skupín podporovaných štátmi. Spojené štáty americké aj Veľká Británia opakovane obvinili Rusko a Čínu z týchto škodlivých aktivít.

Naďalej aktívne boli aj iránske a severokórejské štátom podporované skupiny. Októbrový útok teroristickej skupiny Hamas na izraelské civilné ciele a následná odveta Izraela boli ďalšími z prípadov, keď sa kinetické akcie takmer okamžite preniesli aj do kybernetického priestoru.

Priamo zapojení aktéri alebo spriaznené skupiny v nadväznosti na agresiu uskutočnili viaceré DDoS kampane a iné škodlivé aktivity voči izraelským aj palestínskym cieľom.

Kyberkriminálne aktivity boli takisto významným prvkom, ktorý ovplyvňoval dianie v kyberpriestore a predovšetkým ransomvérové útoky naďalej prekonávali minulé rekordy – počtom zasiahnutých obetí aj finančných škôd.

1.1.1 ZNEPRÍSTUPNENIE SLUŽIEB

Znefunkčnenie služieb pomocou DDoS útokov bolo ďalej populárnou formou škodlivej aktivity medzi útočníkmi s rôznou mierou znalostí a sofistikovanosti.

Medzi najčastejšie ciele tejto techniky patrili inštitúcie EÚ a NATO, spomedzi sektorov kritická infraštruktúra, banky a veľké spoločnosti. V porovnaní s predošlými rokmi bol v roku 2023 zaznamenaný výrazný nárast intenzity DDoS útokov. Bol spozorovaný aj nový typ DDoS útoku, ktorý aktívne zneužíval zraniteľnosť formou HTTP/2 Rapid Reset techniky.

Medzi aktérmi, ktorí najčastejšie využívali DDoS útoky, boli hacktivistické skupiny zapojené do vojny Ruska proti Ukrajine Útoky boli o ich primárnou agendou (vzhľadom na ich relatívnu jednoduchosť oproti pokusom o prienik do infraštruktúry). Ich aktivity kopírovali vývoj konfliktu na Ukrajine. Z ruskej strany boli tieto aktivity cielené na infraštruktúru štátov, najmä na tie podporujúce Ukrajinu, pričom na opačnej strane ciele zahŕňali najmä ruské inštitúcie.

Medzi najaktívnejšie hacktivistické skupiny patrili Anonymous Russia, DDoSia, NoName057(16), National Hackers Russia, Killnet, Revil, Anonymous Sudan. Tieto zoskupenia

sa k aktivitám pri propagácii svojej činnosti aktívne hlásili na sociálnych sieťach – predovšetkým Telegrame.

Pri tomto type incidentu je potrebné rozlišovať medzi nedostupnosťou služby, ktorá je spôsobená priamym zavinením aktéra a nepredvídateľnou udalosťou. Práve pri zneprístupnení služieb sa veľmi často stáva, že je spôsobená nepredvídateľnou udalosťou – nevydarenou aktualizáciou, výpadkom prúdu a podobne..

1.1.2 RANSOMVÉR

Rok 2023 sa vyznačoval nárastom v oblasti ransomvérových útokov. Výrazný vplyv mal na fungovanie inštitúcií, firiem aj jednotlivcov.

V tejto oblasti prevláda aktivita profesionálnych gangov poskytujúcich ransomvér ako službu (RaaS). Ransomvérové gangy pokračovali vo vylepšovaní svojich postupov a nástrojov napríklad pomocou zrýchleného zašifrovania dát a zefektívnenie postupov pre exfiltráciu dát.

Možnosti vykonávať ransomvérové útoky sa rozširujú, čo je spôsobené napríklad nárastom poskytovateľov RaaS. Úniky zdrojových kódov známych ransomvérových skupín spôsobujú, že si noví aktéri vedia už overené nástroje ľahko modifikovať a prevziať. Pomáhajú aj úniky návodov na ransomvérový útok, ktoré umožňujú útočníkovi zvyšovať svoju efektivitu.

Primárnymi vektormi pri prienikoch do systémov a zariadení sú aj naďalej úniky prihlasovacích údajov (priamo do infraštruktúry, do služieb alebo do VPN), získavanie prístupových údajov metódami sociálneho inžinierstva, výskyt bezpečnostných zraniteľností a nesprávnej konfigurácie systémov, ale aj nasadenie škodlivého kódu phishingovými aktivitami.

Úspech zaznamenali aj bezpečnostné zložky, ktoré vďaka medzinárodnej spolupráci rozložili niekoľko kyberzločineckých skupín, napr. LockerGoga, MegaCortex, HIVE a Dharma ransomware.

1.1.3 PHISHING

Motiváciu útočníkov vykonávať phishingové aktivity možno rozdeliť na dve kategórie.

Prvá spočíva v získavaní citlivých údajov, ktoré sú následne predávané tretím stranám.

Druhou kategóriou je vykonávanie phishingovej aktivity s cieľom šírenia malvéru, ktorý však v konečnom dôsledku môže slúžiť aj na zber citlivých údajov.

Phishingové kampane boli naďalej najpopulárnejšou a najúspešnejšou metódou na získavanie citlivých údajov. Bol pozorovaný výrazný nárast amatérskych škodlivých aktérov. Nárast pravdepodobne spôsobilo to, že je jednoduché získať phishingové nástroje, ktoré sú vyvíjané a následne predávané alebo poskytované útočníkom ako služba (Phishing as a Service). Niektoré z nich sú dokonca voľne dostupné na internete a vie sa k nim dostať prakticky každý.

Najrozšírenejšími kampaňami sú naďalej tie, ktoré zneužívajú identitu bankových a finančných inštitúcií, poštových a doručovateľských služieb, populárnych online služieb, exponovaných používateľov sociálnych sietí (napríklad politikov).

Boli zaznamenané aj aktivity, ktoré využívali témy geopoliticky relevantných udalostí, napríklad vojna na Ukrajine alebo konflikt v Izraeli.

Útočníci na maskovanie svojej činnosti a obchádzanie bezpečnostných prvkov často využívajú skracovače URL adries a viacnásobné presmerovania.

V roku 2023 pokračovali aj malwaretisement kampane a šírili sa trojanizované verzie frekventovane používaných softvérov. Hlavým problémom bol aj naďalej zvyk ľudí automaticky klikať na reklamy, ktoré sa nachádzajú medzi prvými výsledkami v internetových vyhľadávačoch.

SEO optimalizácia webových stránok bola často využívaným nástrojom útočníkov. Funguje na princípe optimalizácie technickej konfigurácie webovej stránky, relevantnosti obsahu a popularity odkazov. Umožňuje ľahší prienik falošných verzií webových stránok na popredné miesta vo vyhľadávačoch. Útočníci využívali aj možnosť platenej reklamy.

1.1.4 ÚTOKY ZNEUŽÍVAJÚCE NEPOZORNOSŤ A NEDOSTATOČNÉ ZABEZPEČENIE

V minulom roku boli opäť zaznamenané prípady súvisiace s nedostatkami bezpečného prístupu k informačným technológiám na strane používateľov aj správcov informačných systémov.

Zaraďujeme sem najmä nesprávnu konfiguráciu a nedostatočné zabezpečenie systémov s nedostatočnou kybernetickou hygienou a najlepšou bezpečnostnou praxou.

Nedostatky sa objavovali vo forme veľkého počtu zariadení a služieb (napríklad sieťové úložiská, IP kamery, služby vzdialeného prístupu) voľne dostupných z internetu, slabých hesiel, opakovaného používania rovnakých hesiel medzi rôznymi službami a neimplementovanej dvojfaktorovej autentifikácie.

Medzi ďalšie zaznamenané trendy patrí výskyt podvodných knižníc. Majú podobne znejúce názvy ako ich legitímne náprotivky (tzv. library typosquatting). Ich cieľom je šírenie škodlivého kódu, pričom benefitujú na preklepoch alebo nepozornosti programátorov. V prípade používania produktu v iných službách tak hrozí infikovanie celého dodávateľského reťazca.

1.1.5 ZRANITEĽNOSTI

Z globálneho hľadiska narástol počet odhalených a zverejnených zraniteľností. Celkové riziko a relevantnosť zraniteľnosti sa okrem objektívneho zhodnotenia závažnosti prostredníctvom metriky CVSS posudzuje aj podľa dostupnosti dôkazu zneužiteľnosti zraniteľnosti (tzv. proof of concept) a skutočnosti či je zraniteľnosť aktívne zneužívaná útočníkmi.

Oproti roku 2022, kedy dominovalo niekoľko veľkých a viditeľných zraniteľností, v roku 2023 bolo odhalených viacero kritických zraniteľností s veľkým dosahom a vplyvom, ktorým sa jednotlivo nedostalo toľko mediálnej pozornosti.

V roku 2023 boli celosvetovo najzávažnejšie útoky zneužívajúce zraniteľnosti v produktoch Forta GoAnywhere (CVE-2023-0669), Barracuda Email Security Gateway (CVE-2023-2868), Progress Software Moveit Transfer (CVE-2023-34362), MS Windows a Office riešeniach (CVE-2023-23397, CVE-2023-36884, CVE-22336584), WebP/Libwebp (CVE-2023-4863), Cisco XE (CVE-2023-20198), VMware ESXi (CVE-2023-20867), Apple iOS a iPad iOS (CVE-2023-41992, CVE-2023-41993), Attlasian Confluence (CVE-2023-22515) a Citrix NetScaler a Netscaler Gateway (CVE-2023-4966).

Uvedené zraniteľnosti umožňovali útočníkom od získania neoprávneného prístupu k citlivým údajom, cez neoprávnený prístup do systému až po vykonanie škodlivého kódu s následkom úplného narušenia dôvernosti, integrity a dostupnosti zraniteľných systémov.

1.1.5 NEGATÍVNY VPLYV AI MODELOV NA KYBERNETICKÚ BEZPEČNOSŤ

Nárast popularity nástrojov umelej inteligencie (AI) a sprístupnenie jazykových modelov ako sú napríklad ChatGPT, MS Copilot alebo Grok otvorili nové možnosti útočníkom a dodali im širokú škálu nástrojov na zefektívnenie ich činností. Umožňujú im napríklad generovať kvalitnejšie preklady a texty phishingových e-mailov alebo automatizáciu rôznych činností vykonávaných počas celého životného cyklu phisingovej kampane, nielen generovania obsahu v rôznych jazykoch. Vyššia sofistikovanosť útokov bola taktiež spôsobená využívaním vlastných generatívnych modelov priamo určených pre škodlivých aktérov – ako napríklad WormGPT, ktorý neobsahuje bezpečnostné obmedzenia ani poistky voči zneužitiu na nelegálne účely.

Najbežnejšie trendy v používaní umelej inteligencie na škodlivé účely ďalej zahŕňalo modifikovanie a generovanie škodlivého kódu pomocou AI, automatizované permutácie verzií kódu na vyhýbanie sa detekcii ako aj ďalšie otváranie dverí amatérskym útočníkom do sveta nelegálnych aktivít.

1.2 Najvýznamnejšie hrozby v Slovenskej republike za rok 2023

1.2.1 SOCIÁLNE INŽINIERSTVO

Phishingové kampane pokračovali vo využívaní sociálneho inžinierstva na efektívnejšie dosiahnutie svojho cieľa. Trendy v získavaní citlivých informácií sa s predchádzajúcim rokom príliš nelíšili.

V roku 2023 prevládalo na Slovensku napodobňovanie predovšetkým doručovateľských služieb (DHL, DPD, Slovenská pošta, Packeta a pod.), poskytovateľov internetového pripojenia, bankových a finančných inštitúcií, polície a Interpolu a taktiež impersonácia ústredných orgánov štátnej správy (napr. finančnej správy a ministerstva investícií, regionálneho rozvoj a informatizácie). Prípady boli v priebehu roka opakovane medializované zo strany štátnych orgánov aj zasiahnutých subjektov.

Pretrvávali aj podvodné aktivity, ktoré zneužívali známe online predajné platformy a fóra, pričom útočníci sa snažili vylákať od svojich obetí citlivé informácie, najmä údaje z ich platobných kariet alebo prihlasovacie údaje do internetbankingu. V tejto oblasti pretrvával aj fenomén sexuálneho vydierania (tzv. sextortion), pričom útočníci nemusia mať žiadny prístup k citlivým materiálom, ktorými obeť vydierajú.

Rok 2023 sa vyznačoval najmä kampaňami, ktoré boli založené na podvodoch s kryptomenami (rôzne služby a pyramídové koncepty súvisiace s investíciami do kryptomien). Útočník si získal dôveru obete tým, že jej prvotne vyplácal provízie, no v istom bode prestal. Podvody majú masívny PR rozmer, a to napr. prostredníctvom Telegramu a iných sociálnych sietí, ako aj organizovania fyzických stretnutí.

Ďalším typom sociálneho inžinierstva bol tzv. whaling, ktorý je napriek nižšiemu výskytu stále relevantný. Je možné sa s ním stretnúť napríklad vo forme impersonácie riaditeľa

spoločnosti so žiadosťou o stav účtu a platbu, pričom obeť je urgentne nasmerovaná odoslať finančné prostriedky domnelému nadriadenému či dodávateľovi.

Oproti predpokladom z minulého roka bolo zaznamenané minimum phishingového obsahu umiestneného na decentralizovaných peer-to-peer platformách (IPFS). Dokumenty vytvorené v balíke MS Office napriek plošnému zablokovaniu spúšťania makeir útočníci stále na šírenie škodlivého obsahu (avšak v menšej miere) – dokumenty môžu obsahovať URL škodlivé odkazy alebo útočníci používajú iné metódy, ako napríklad OLE template injeciton (počas otvárania súboru sa sťahujú časti so škodlivým obsahom do zariadenia), na ktoré nemá vypnutie makier vplyv.

Na šírenie škodlivého obsahu v kampaniach využívajú aktéri e-mailové prílohy s príponami .lnk, .iso, .rar a podobne.

Vzrástol aj počet interaktívnych foriem sociálneho inžinierstva často spojeného s phishingovými útokmi. V niektorých prípadoch phishingové weby obsahujú interaktívny chat, v ktorom útočník vedie obeť cez rôzne služby na vzdialenú správu, alebo ju naviguje počas telefonátu, pričom predstiera poskytovanie služieb technickej podpory.

Vzrástol tiež výskyt podvodných kampaní na sociálnych sieťach. Útočníci sa pokúšajú získať prístup k pracovným účtom alebo účtom s vysokým počtom sledovateľov za účelom šírenia škodlivého obsahu tak, že modifikujú obsah platenej reklamy, zdieľajú podvodné príspevky – napríklad súvisiace s kryptomenami – alebo šíria ilegálny obsah.

Novým zaznamenaným trendom bolo zneužívanie SMS platobných brán. Podvod spočíva v tom, že útočník pripraví žiadosť o SMS platbu na číslo obete a následne obeť presviedča, aby poslala SMS na štvorčíslie, ktorým sa daná platba potvrdí. Útočníci týmto spôsobom kupujú napr. kľúče na odomknutie hier alebo iných rýchlo predateľných produktov, ktoré následne speňažia.

1.2.2 NEDOSTUPNOSŤ SLUŽIEB A DDOS ÚTOKY

Rok 2023 bol poznačený množstvom DDoS útokov na kritickú infraštruktúru, bankový sektor a dopravu. Takisto bolo nahlásených viacero kategorizovaných incidentov.

Pozitívnym javom bola narastajúca odolnosť infraštruktúry obetí po útoku, ale aj v prevencii (vysoký počet medializovaných úspešných útokov) a vplyv osvety realizovanej bezpečnostnými zložkami (celoštátne varovania, adresné/sektorové varovania organizácií, na ktoré hacktivisti plánujú útok). Vo väčšine prípadov sa po ukončení útoku podarilo obnoviť prevádzku.

Pokračujúcim trendom boli útoky smerované z IP adries TOR, VPN, Open Proxy aj z kompromitovaných zariadení, často z botnetov, prenajímaných inými hackerskými skupinami ako služba, ktoré útočníci používajú na maskovanie svojej aktivity.

Výpadky a nedostupnosť systémov však nespôsobila vždy len škodlivá činnosť tretej strany, ale aj nepripravenosť systémov na veľký nával legitímnych návštevníkov, zle vykonávaná údržba systémov alebo nesprávne implementovaná/netestovaná aktualizácia systémov, či zavádzanie nových netestovaných prvkov a podobne.

1.2.3 MALVÉR

Na Slovensku boli zaznamenané početné infekcie zariadení rôznymi rodinami malvéru, a to najmä SystemBC, IcedID, Ursnif, Trickbot, JS.Agent.USU, QuakBot, Qbot,

Redline, Raccoon Stealer a Amadey. Významné zastúpenie mali aj infekcie ransomvérom, ktoré súviseli s činnosťou skupín Lockbit, Vice Society, Underground Team a Medusalocker.

Medzi najvýznamnejšie vektory prieniku patrilo sociálne inžinierstvo, zlá bezpečnostná politika (používanie vlastných zariadení a služobných účtov na súkromné účely a pod.), navštevovanie kompromitovaných webstránok alebo inštalácia trojanizovaného softvéru (napr. platený softvér s doinštalovaným kompromitovaným doplnkom).

1.2.4 ZRANITEĽNOSTI A POKUSY O PRIENIK DO SYSTÉMU

Najčastejším vektorom prieniku boli v roku 2023 phishingové útoky predstavujúce najefektívnejší spôsob pre útočníka prekonať bezpečnostné nastavenia systému.

Nasledovali zraniteľnosti a nesprávna konfigurácia zariadení – najmä verejne dostupné služby vzdialeného prístupu a výmeny dát (napr. RDP, FTP, SSH, SMB) a prihlasovacie rozhrania do priemyselných riadiacich systémov s nastaveniami od výroby a pôvodnými heslami alebo bez prihlasovania, prípadne so zlou politikou hesiel.

Častým dôvodom prieniku do systému je kompromitácia e-mailovej schránky ako následok phishingu a reťazové rozposielanie phisingových správ na kontakty kompromitovaného konta.

V oblasti zraniteľností NBÚ vydal veľké množstvo adresných varovaní – napríklad na zraniteľnosti v SYNOLOGY SRM, QNAP NAS, MS Exchange, Baracuda Networks Spam Firewall, Citrix, Jusnos OS, Apache HTTP Server, ZIMBRA, Atlassian Confluence, CISCO IOS XE, Roundcube, TeamCity Jetbrains a iné.

Naďalej bolo pozorované, že spoločnosti často zlyhávali pri monitoringu a riadení zraniteľností, na základe čoho neboli schopné reagovať na prípadné hrozby v adekvátnom čase.

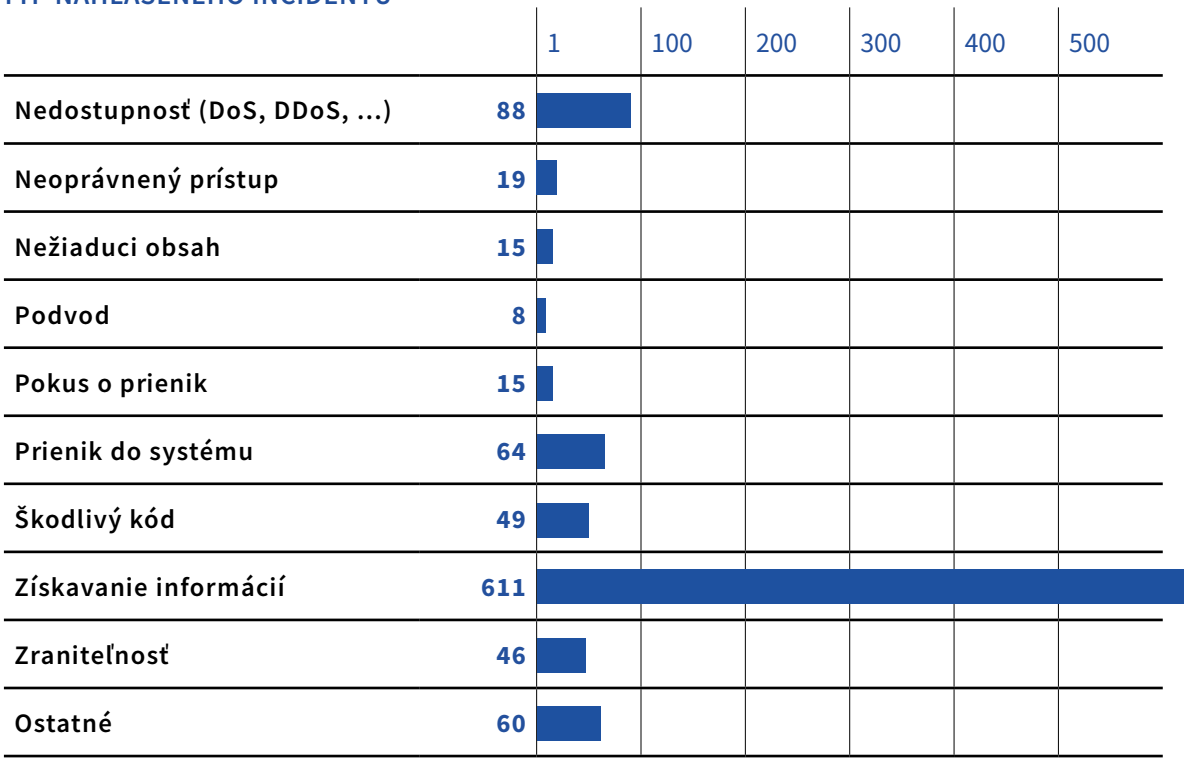
Veľmi často pozorovaným nedostatkom bola zanedbávaná údržba zastaraných a výrobcom nepodporovaných zariadení, pretože predstavujú vysoké finančné a personálne zaťaženie, čo spôsobuje nedostatočné riadenie aktualizácií alebo adekvátnej mitigácie.

2. Štatistický prehľad incidentov za rok 2023

Národné centrum kybernetickej bezpečnosti plnilo úlohy na úseku monitorovania slovenského kybernetického priestoru. Pracovalo na zhromažďovaní a analyzovaní informácií z prijímaných hlásení o kybernetických bezpečnostných incidentoch.

Oproti minulým rokom nastala zmena v štatistickom vyhodnocovaní zaznamenaných incidentov, v ktorom sa zhromažďujú údaje len o incidentoch nahlásených NCKB.

TYP NAHLÁSENÉHO INCIDENTU

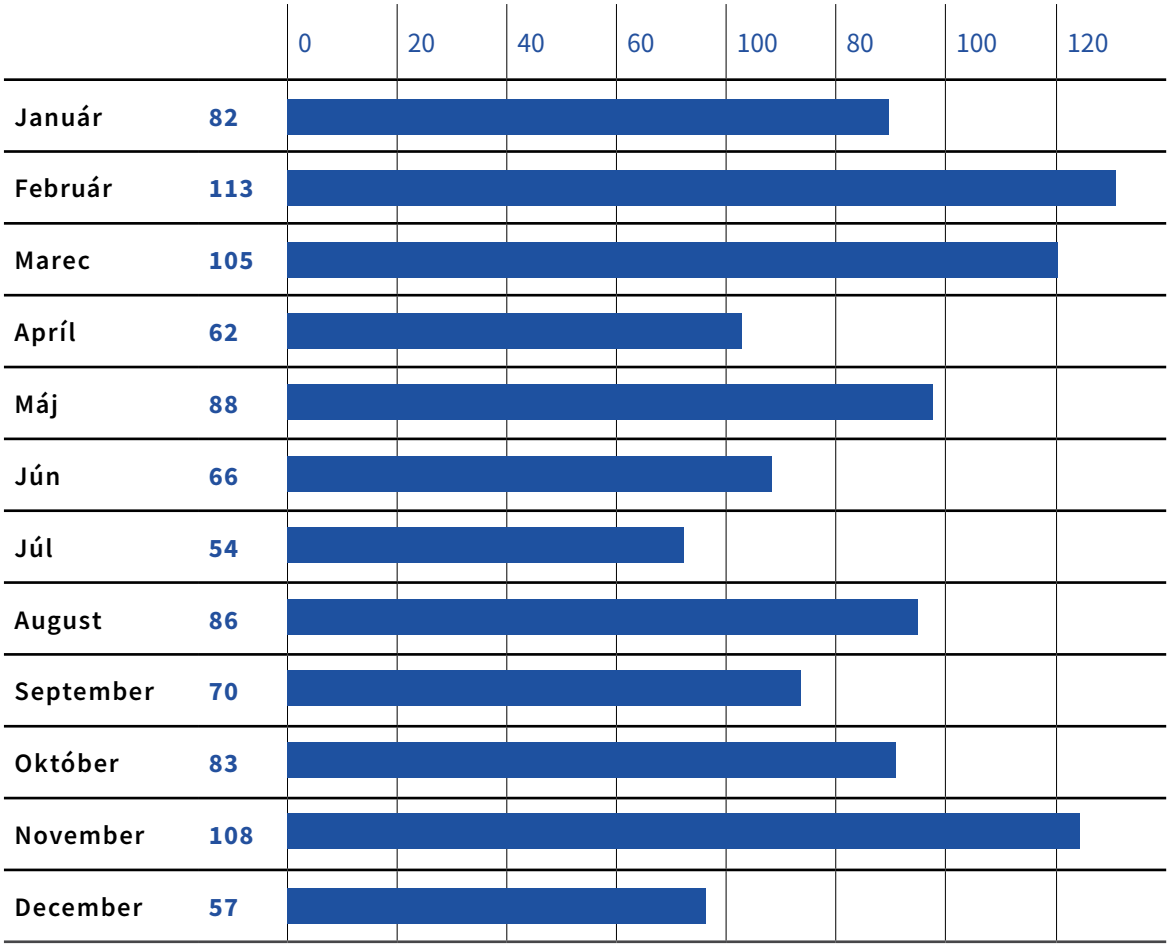


V roku 2023 dominovali technické typy útokov, ako sú získavanie informácií, nedostupnosť, prienik do systému, škodlivý kód a zraniteľnosť.

Phishing bol stále najrozšírenejšou a najúspešnejšou metódou získavania citlivých údajov a šírenia škodlivého obsahu. Nedostupnosť v sebe zahŕňa aj nedostupnosť systémov, ktorá nie je následkom kybernetického útoku (viď vyššie). Oproti predchádzajúcemu roku sme zaznamenali nárast ransomvérovej a malvérovej aktivity.

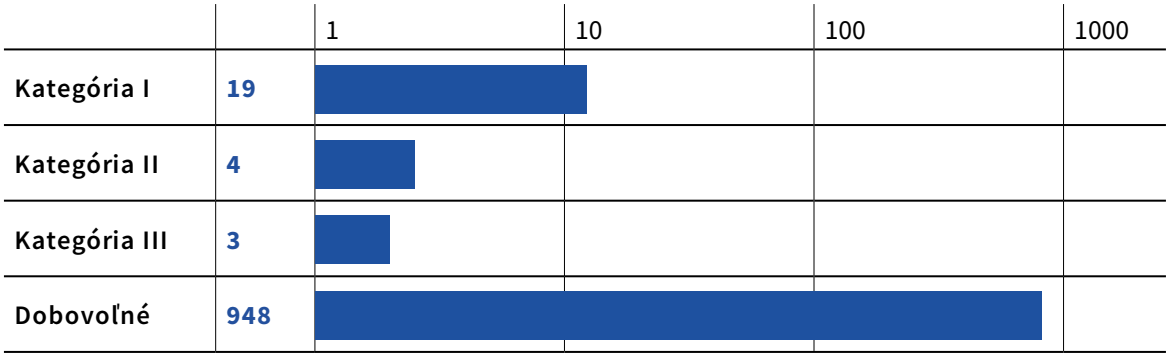
Aj v roku 2023 bolo najviac hlásení o kybernetických bezpečnostných incidentoch prijatých v prvej polovici roka. V roku 2023 prijal SK-CERT o 196 hlásení menej ako v predchádzajúcom roku. Z tohto sa však nedá nevyhnutne vyvodzovať záver, že slovenský kybernetický priestor sa stal bezpečnejším. Je nutné vziať do úvahy pretrvávajúcu neznalosť prevádzkovateľov základných služieb (PZS) a poskytovateľov digitálnych služieb (PDS) nahlasovať incidenty, či zvýšenie sofistikovanosti škodlivých aktérov, ktorých aktivity môžu byť ťažšie detekovateľné, prípadne kombináciu oboch možností.

POČET HLÁSENÝCH KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV Z ČASOVÉHO HĽADISKA



Dobrovoľné hlásenia výrazne prevládali nad povinnými kategorizovanými hláseniami. Pri dôvodoch nehlásenia bola najčastejšie pozorovaná neznalosť právnych noriem – subjekty nevedia o povinnosti hlásenia. Bola tiež zaznamenaná rôzna úroveň zrelosti a povedomia subjektov v SR – mnoho subjektov sa napríklad obáva sankcií alebo iných negatívnych dôsledkov.

HLÁSENIA INCIDETOV PODĽA ZÁVAŽNOSTIROK 2022

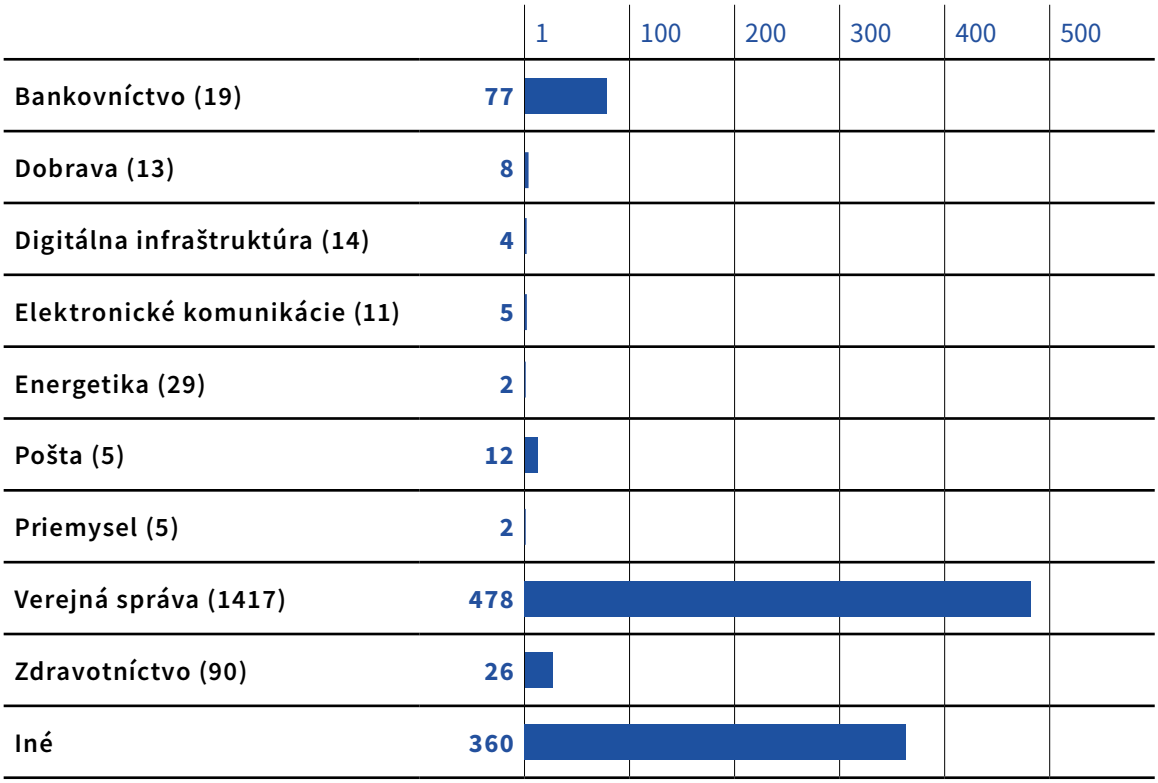


Najviac hlásení v roku 2023 pochádzalo zo sektorov verejná správa, bankovníctvo a zdravotníctvo.

Vyšší počet hlásení implikuje viac incidentov v sektore a vyššiu úroveň zrelosti a povedomia hlásiaceho subjektu (nebojí sa hlásiť, komunikuje, hlási aj dobrovoľne a pod).

Je však potrebné brať do úvahy rozdielne počty subjektov v jednotlivých sektoroch aj atraktívnosť potenciálnych ziskov v prípade aktivít škodlivých aktérov. Takisto s prichádzajúcou novelou zákona v nadväznosti na NIS 2 je možné do ďalších rokov očakávať nárast hlásení, pretože novela rozšíri pôsobnosť na ďalšie subjekty.

HLÁSENIA KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV V SEKTOROCH – ROK 2023



3. Prehľad stavu počítačovej kriminality v Slovenskej republike za rok 2023

Policajný zbor eviduje len všeobecné údaje k trestným činom na úseku počítačovej kriminality.

Trestný čin (paragraf, názov)	Zistené	Objasnené	% objasnenosti	Spôsobená škoda €
§ 201a Sexuálne zneužívanie	6	2	33,33	
§ 219 Neoprávnené vyrobenie a používanie platobného prostriedku, elektronických peňazí alebo inej platobnej karty	2116	457	21,6	5 953 000
§ 226 Neoprávnené obohatenie	9	2	22,22	76 000
§ 247 Neoprávnený prístup do počítačového systému	23	1	4,35	600 000
§ 247a Neoprávnený zásah do počítačového systému	8	–	0	15 000
§ 247b Neoprávnený zásah do počítačového údaja	5	–	0	10 000
§ 247c Neoprávnený prístup do počítačového systému	2	1	50	–
§ 247d Neoprávnené zachytávanie počítačových údajov	–	–	–	–
§ 283 Porušovanie autorského práva	44	9	20,45	1 848 000
§ 368 Výroba detskej pornografie	33	16	48,48	7 000
§ 369 Rozširovanie detskej pornografie	201	56	27,86	30 000
§ 370 Prechovávanie detskej pornografie a účasť na detskom pornografickom predstavení	37	23	62,16	13 000
Spolu	**2 447**	**567**	**23,17**	**8 552 000**

Pre sledovanie vývoja trestnej činnosti na úseku počítačovej kriminality je jediným nástrojom v podmienkach Policajného zboru Evidenčno-štatistický systém kriminality (EŠSK) podľa nariadenia ministra vnútra Slovenskej republiky č. 83/2014 o používaní informačných systémov Policajného zboru evidenčno-štatistického systému kriminality a systému súčasne stíhaných osôb.

Počítačová kriminalita je špecifická trestná činnosť, ktorú je možné spáchať iba pomocou výpočtovej techniky (je nástrojom páchateľa na spáchanie trestného činu), alebo je výpočtová technika objektom trestného činu.

Odhaľovanie a dokumentovanie tejto trestnej činnosti si vyžaduje vysokú odbornú pripravenosť a kvalitné počítačové vybavenie, pretože trestná činnosť týkajúca sa poškodenia a zneužitia záznamu na nosiči informácií je páchaná najmä cez internet.

Nízka objasnenosť tejto trestnej činnosti na úseku počítačovej kriminality výrazne súvisí s rozmachom nových informačných technológií a služieb spojených s využívaním najrôznejších sofistikovaných spôsobov v prostredí P2P/TOR sietí a pod., pričom zaznamenávame stále nízke percento objasnenosti trestných činov neoprávneného prístupu/zásahu do počítačového systému/údaja resp. zachytávanie počítačových údajov.

Celkový nápad trestných činov na úseku detskej pornografie je spôsobený zasielaním informácií k detskej pornografii z Národného centra pre nezvestné a vykorisťované deti z USA (National Center for Missing and Exploited Children – NCMEC) cez EUROPOL, Národnej ústredne Europol úradu medzinárodnej policajnej spolupráce P PZ na odbor ako podozrenia z výroby, prechovávania a rozširovania detskej pornografie.

Uvedené informácie sú na odbore vyhodnocované, triedené a podnety na trestné stíhanie zasielané na vecne a miestne príslušné útvary Policajného zboru. V priebehu roku 2023 bolo na odbor doručených prostredníctvom Europolu celkovo 41 SIENA balíkov NCMEC, ktoré obsahovali celkovo 9 601 NCMEC reportov, čo je v porovnaní s rokom 2022, kedy bolo doručených 7 627 NCMEC reportov nárast o 20 %.

Jednotlivé NCMEC reporty boli vzhľadom na obsah materiálu analyzované na prítomnosť detskej pornografie a relevantnosť ich odstúpenia ako informácií pre začatie trestného konania. Celkovo bolo spracovaných 420 podnetov/odstúpení informácií na začatie trestných konaní na príslušné útvary Policajného zboru. Distribúcia materiálov s detskou pornografiou je najčastejšie zaznamenávaná na internetových komunikačných portáloch a internetových fórach.

V prevencii rôznych online podvodov a podvodných kampaní odbor spolupracuje aj s odborom komunikácie a prevencie policajného zboru. Odbor poskytuje podklady o nových spôsoboch páchania trestných činov v online priestore, ktoré sú zverejňované na oficiálnej facebookovej stránke Policajného zboru, aby bola verejnosť informovaná v čo najkratšom čase.

4. SEKTOROVÝ POHĽAD

Pohľad na kybernetickú bezpečnosť v rôznych sektoroch sa formuje na základe dvoch pilierov: výsledkov auditných správ a hodnotenia aktivít ústredných orgánov. Je možné konštatovať, že úroveň kybernetickej bezpečnosti sa v závislosti od sektora značne líši.

Sektor **bankovníctvo** je dlhodobo v predstihu v oblasti kybernetickej bezpečnosti. Prevádzkovatelia v tomto sektore (PZS) k danej problematike pristupujú zodpovedne, a to ako pri implementácii bezpečnostných požiadaviek, tak aj v komunikácii s Národným bezpečnostným úradom (NBÚ). V prípade incidentov či iných problémov reagujú promptne a bezodkladne. Zástupcovia PZS v sektore bankovníctva sa taktiež aktívne podieľajú na budovaní komunity zameranej na kybernetickú bezpečnosť.

V sektore **zdravotníctvo** pozorujeme postupné zvyšovanie povedomia o dôležitosti kybernetickej bezpečnosti. K tomuto trendu prispieva aj zlepšujúca sa práca ústredného orgánu. Postupne sa upevňuje vnímanie zodpovednosti za ochranu dát aj za funkčnosť systémov a služieb, od ktorých závisia ľudské životy.

Sektor **energetika** vyniká najvýraznejšími rozdielmi medzi podsektormi aj v ich internej štruktúre. Podsektor plynárenstva dosahuje z hľadiska auditných výsledkov najlepšie umiestnenie spomedzi všetkých sektorov a podsektorov. V elektroenergetike sa prejavujú značné rozdiely medzi jednotlivými prevádzkovateľmi.

Naopak, tepelná energetika trpí extrémne zlými výsledkami auditov, a to napriek dôležitosti daného podsektora. Jeho fungovanie má značný vplyv na bežný život občanov. Obmedzenie alebo výpadok služieb v tomto sektore môžu mať vážne dôsledky na život a zdravie obyvateľstva.

V sektoroch **infraštruktúra finančných trhov, priemysel a pošta** chýba jasný obraz o stave kybernetickej bezpečnosti. Dôvodom je nedostatok relevantných informácií od ústredných orgánov zodpovedných za tieto sektory. Neuviedli konkrétne detaily o kybernetickej bezpečnosti v daných oblastiach a zároveň chýba aj dostatočný počet auditných správ, z ktorých by sa dala vytvoriť anonymizovaná štatistická vzorka.

V sektore **verejná správa**, konkrétne v podsektore informačné systémy verejnej správy, sa kybernetická bezpečnosť dlhodobo nemení napriek najväčšiemu počtu prevádzkovateľov. V niektorých prípadoch je zanedbaná až kriticky. Najmä samosprávy a menší prevádzkovatelia si neuvedomujú jej dôležitosť.

K problematike pristupujú povrchne a zameriavajú sa na formálne úkony ako nákup generických dokumentov. Často sa snažia preniesť zodpovednosť na externé firmy vrátane neprenosných povinností štatutára. Celkové riadenie kybernetickej bezpeč-

nosti chýba, je chaotické alebo neúplné. Problémy sa netýkajú len samospráv, ale aj niektorých veľkých prevádzkovateľov v tomto podsektore vrátane štátnych inštitúcií.

Pri získavaní informácií od ústredných orgánov podľa zákona 69/2018 o kybernetickej bezpečnosti dochádzalo často k nepochopeniu postavenia a úloh ústredného orgánu od kompetentných ministerstiev. Odpovede boli často koncipované tak, že opisovali stav na ministerstve ako u prevádzkovateľa základnej služby, nie ako subjektu, ktorý má na starosti určitý sektor alebo podsektor. Z tohto hľadiska je nevyhnutné najmä zo strany ústredných orgánov lepšie pochopiť ich postavenie a úlohy podľa § 9.

4.1 Sankcie

V zmysle zákona o kybernetickej bezpečnosti je NBÚ oprávnený uložiť pokutu, ak PZS poruší svoje povinnosti, ktoré mu zo zákona vyplývajú. Úrad v roku 2023 vykonal kontrolu kybernetickej bezpečnosti u **18** prevádzkovateľov základných služieb, pričom nedostatky boli zistené až u **17** kontrolovaných subjektov s celkovým počtom **67** kontrolných zistení, ktoré môžeme rozdeliť do nasledujúcich oblastí:

- Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahu s tretími stranami – **11 porušení**,
- Zaznamenávanie udalostí a monitorovanie sietí a informačných systémov – **7 porušení**,
- Riadenie rizík – **12 porušení**,
- Riadenie aktív – **5 porušení**,
- Identifikácia technických zraniteľností – **7 porušení**,
- Riešenie kybernetických bezpečnostných incidentov – **6 porušení**,
- Klasifikácia informácií a kategorizácia sietí a informačných systémov – **6 porušení**,
- Obsah a štruktúra bezpečnostnej dokumentácie – **2 porušenia**,
- Riadenie bezpečnosti prevádzky sietí a informačných systémov – **4 porušenia**,
- Personálna bezpečnosť – **2 porušenia**,
- Sieťová a komunikačná bezpečnosť – **1 porušenie**,
- Riadenie prístupov osôb k sieti a informačnému systému – **1 porušenie**,
- Určenie manažéra kybernetickej bezpečnosti – **1 porušenie**,
- Uzatvorenie zmlúv o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa zákona – **1 porušenie**,
- Nedodaný audit kybernetickej bezpečnosti – **1 porušenie**.

4.2 Audity a samohodnotenia

Auditom kybernetickej bezpečnosti sa preveruje efektívnosť implementácie opatrení, vykonávania opatrení a prípadne nedostatky implementovaných opatrení v prostredí PZS v oblasti informačno-komunikačných technológií (IKT) a v oblasti kybernetickej bezpečnosti v zmysle platnej regulácie a bezpečnostného rámca. Za rok 2023 bolo Národnému bezpečnostnému úradu **doručených 135 auditných správ.**

AUDITY

Sektor	Počet PZS	Počet PZS s povinnosťou auditu v roku 2023
Bankovníctvo	19	19
Digitálna infraštruktúra	15	9
Doprava	13	7
Elektronické komunikácie	11	8
Energetika	28	17
Infraštruktúra finančných trhov	1	1
Pošta	5	1
Priemysel	7	4
Verejná správa	1 400	122
Voda a atmosféra	18	15
Zdravotníctvo	94	69
Spolu	**1 611**	**272**

DORUČENÉ SAMOHODNOTENIA

Sektor	Počet doručených samohodnotení
Verejná správa	307
Zdravotníctvo	6
Doprava	2
Pošta	2
Voda a atmosféra	6
Energetika	1
Priemysel	1
SPOLU	**325**

4.3 Bankovníctvo

Ústredný orgán: Ministerstvo financií Slovenskej republiky (MF SR)

Počet PZS : 19

Počet PZS s povinnosťou auditu v roku 2023: 19
(možné splniť aj samohodnotením podľa §34a ods. 2 ZoKB)

Počet odovzdaných auditných správ: 9

Počet odovzdaných samohodnotení: 0

Podsektory: žiadne

4.3.1 ZHODNOTENIE STAVU KYBERNETICKEJ BEZPEČNOSTI ZA ROK 2023 ÚSTREDNÝM ORGÁNOM

Kritické hrozby:

Najvýznamnejšie hrozby, na ktoré bolo ministerstvo financií v kybernetickom priestore upozornené, boli sofistikované techniky na získanie neoprávneného prístupu do systémov organizácie, ransomvérové útoky, bezpečnostné hrozby v cloude, sociálne inžinierstvo a zraniteľnosti v IT produktoch.

Zákonné aktivity:

MF SR udržiava Security operations center (SOC) ako oddelenie ministerstva. Tamojší SOC bol realizovaný v projekte „Zvýšenie úrovne informačnej a kybernetickej bezpečnosti MF SR“ a bol úspešne implementovaný v novembri 2023. V súčasnosti beží fáza udržateľnosti projektu.

Je členom medzinárodného združenia TF CSIRT pod štatútom „Listed team“. Počas roka 2023 bolo MF SR v pracovnom kontakte s NBÚ za účelom implementácie prístupového bodu MF SR do JISKB z dôvodu požiadavky implementácie zákona o kybernetickej bezpečnosti.

Aktivity nad rámec zákona:

MF SR stále udržiava v prevádzke mechanizmus vzdelávania rezortných pracovníkov v boji proti kybernetickým hrozbám (e-learningový portál LMS, interné vzdelávanie pracovníkov, rozširovanie bezpečnostného povedomia zamestnancov). Zároveň je udržiavaná aj generická adresa podozrivaposta@mfsr.sk na odoslanie podozrivej a potenciálne škodlivej elektronickej komunikácie. Na preverenie a na riešenie kybernetických incidentov je určená generická adresa incident@mfsr.sk.

Plánované aktivity:

Ústredný orgán plánuje naďalej prevádzkovať mechanizmus vzdelávania rezortných pracovníkov v oblasti prevencie pred kybernetickými hrozbami; akreditovať oddelenie bezpečnostného monitoringu SOC v medzinárodnom združení TF CSIRT a plánuje spustiť projekt z fondov EÚ, ktorého cieľom bude rozšíriť služby oddelenia bezpečnostného monitoringu SOC pre rezortné organizácie ministerstva.

Plánovaná stratégia:

V decembri 2023 bol finalizovaný návrh novej Bezpečnostnej stratégie informačnej a kybernetickej bezpečnosti, avšak bez špecifikácie sektorov ochrany v gescii ministerstva v zmysle zákona o kybernetickej bezpečnosti. Špecifická stratégia kybernetickej bezpečnosti pre sektory v jeho gescii v súčasnosti nie je na pláne.

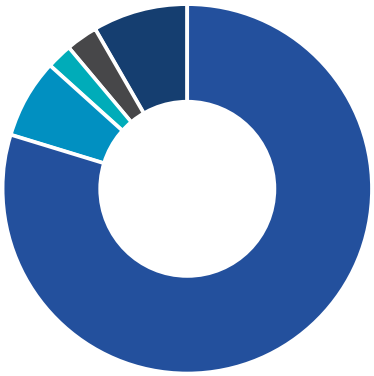
Ľudské zdroje v KB:
MF SR má zriadený Security operations center (SOC) ako oddelenie bezpečnostného monitoringu na odbore informačnej a kybernetickej bezpečnosti, sekcie informačných technológií od roku 2022, avšak plošne iba pre aktivity ministerstva.

Externé subjekty v sektoroch v gescii MF SR (napr. banky, poisťovne, Štátna pokladnica) nie sú pokryté uvedenými aktivitami. Ministerstvo plánuje rozšíriť služby oddelenia bezpečnostného monitoringu SOC pre rezortné organizácie.

Spolupráca v KB:
Spolupráca s medzinárodnou organizáciou TF CSIRT. MF SR komunikuje s NATO Computer Incident Response Capability Technical Center, je priamym odberateľom ich bezpečnostných varovaní a informačných bulletinov a zúčastňuje sa na odborných sympóziách a konferenciách organizovaných v ich gescii. Ministerstvo komunikuje aj s Centrom výnimočnosti pre Kybernetickú bezpečnosť (CCDCOE) v estónskom Talline, kde sa jeho zástupcovia v roku 2023 zúčastnili na medzinárodnej konferencii Cyber Conflict – CyCon 2023.

4. 4. 2 VÝSLEDKY AUDITOV V SEKTORE BANKOVNÍCTVO

Národnému bezpečnostnému úradu bolo k 31. 12. 2023 doručených celkovo 9 auditných správ zo sektora bankovníctvo. Na základe štatistiky súladu s auditnými požiadavkami, v sektore bankovníctvo je priemerná percentuálna miera súladu nasledujúca:



PRIEMERNÁ PERCENTUÁLNA MIERA SÚLADU (ROK 2023)	
SÚLAD	79 %
ČIASTOČNÝ SÚLAD	7 %
NESÚLAD	2 %
NEAPLIKOVATEĽNÉ	3 %
OVERENÉ NA INOM MIESTE	8 %
NEVYHODNOTENÉ AUDÍTOROM	0 %

Pri pohľade na jednotlivých PZS v sektore bankovníctvo je vysoká miera súladu s auditnými požiadavkami kontinuálna naprieč všetkými prevádzkovateľmi a je len veľmi nízka miera nesúladov.

4. 3. 2 NAJČASTEJŠIE AUDITNÉ ZISTENIA V SEKTORE BANKOVNÍCTVO

Medzi najčastejšie auditné zistenia v sektore bankovníctvo patria:

- zmluvy so všetkými dodávateľmi nie sú aktuálne uzavreté a podpísané podľa § 19 ods.2,
- neexistuje formalizovaná stratégia KB,
- spoločnosť nevykonala celkovú analýzu rizík,
- procesy a postupy pre riadenia aktív, hrozieb a rizík nie sú nastavené a formalizované,
- nie sú stanovené postupy pri presune práv, povinnosti a zodpovednosti vo vzťahu ku KB na inú osobu,

4.4 Doprava

Ústredný orgán: Ministerstvo dopravy Slovenskej republiky (MD SR)

Počet PZS : 13

Počet PZS s povinnosťou auditu v roku 2023: 7
(možné splniť aj samohodnotením podľa §34a ods. 2 ZoKB)

Počet odovzdaných auditných správ: 5

Počet odovzdaných samohodnotení: 2

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

4.4.1 ZHODNOTENIE STAVU KYBERNETICKEJ BEZPEČNOSTI ZA ROK 2023 ÚSTREDNÝM ORGÁNOM

Kritické hrozby:

V sektore dopravy neboli v roku 2023 zistené závažné kybernetické bezpečnostné incidenty. S ohľadom na zabezpečenie súladu s aktuálne platnou legislatívou a pripravovanou transpozíciou smernice NIS2 je potrebné riešiť otázku technologického a investičného dlhu v oblasti kybernetickej bezpečnosti.

V sektore je hrozbou absencia centralizovaného bezpečnostného dohľadu aj nedostatok financií a kvalifikovaných personálnych zdrojov, ktoré by boli schopné realizovať pravidelné profilaktické činnosti v oblasti monitoringu, kybernetickej ochrany a mitigácie rizík.

Zákonné aktivity:

Ministerstvo kontinuálne monitoruje a analyzuje potreby či požiadavky relevantné pre sektor dopravy. V súlade s týmito úlohami intenzívne pracuje na implementácii Smernice NIS2, ktorá predstavuje kľúčový legislatívny rámec Európskej únie v oblasti kybernetickej bezpečnosti.

V kontexte projektu NIS2SK MD SR realizuje prípravné práce pre transpozíciu tejto smernice do národného právneho poriadku, pričom zohľadňuje špecifiká a potreby identifikované pri trhových konzultáciách s relevantnými sektorovými subjektmi.

Tento proces umožňuje zabezpečiť, aby prijaté normy a regulácie boli adekvátne a efektívne reagovali na aktuálne výzvy v oblasti kybernetickej bezpečnosti. Po ukončení analytického a konzultačného procesu pristúpi ministerstvo k vydaniu sektorových vyhlášok. Budú explicitne definovať bezpečnostné opatrenia, ktoré budú musieť byť implementované subjektmi pôsobiacimi v jednotlivých sektoroch, aby sa posilnila ochrana kritických informačných infraštruktúr a zabezpečila vyššia úroveň kybernetickej bezpečnosti v Slovenskej republike.

Ministerstvo v projekte *„Rozvoj governance a úrovne informačnej a kybernetickej bezpečnosti v podsektore VS – ministerstvo dopravy a výstavby SR“* realizovalo aktivity so zabezpečením dokumentácie súvisiacej so spracovaním a aktualizáciou základných dokumentov v oblasti informačnej a kybernetickej bezpečnosti a zavedenie SW nástroja pre procesno-organizačné riadenie informačnej a kybernetickej bezpečnosti.

Ministerstvo začalo na základe útokov s realizáciou nasadenia 2FA/MFA na IS MD SR. Zabezpečilo aj MS ATA monitoring pre DDoS útoky, ktoré boli realizované na jeho webové služby (webmail, OA, EWS).

Aktivity nad rámec zákona:
Ministerstvo dopravy sa v spolupráci s Národným bezpečnostným úradom (NBÚ) a Kompetenčným a certifikačným centrom kybernetickej bezpečnosti (KCCKB) aktívne podieľalo na príprave a realizácii spoločného projektu zameraného na implementáciu smernice NIS2, financovaného z fondov Európskej komisie.

Projekt je významným krokom smerujúcim k posilneniu kybernetickej bezpečnosti a k ochrane kritických informačných infraštruktúr na národnej úrovni, a to nielen v sektoroch, ktoré sú v pôsobnosti ministerstva. V projekte sa kladie dôraz na aktívnu účasť a zapojenie trhových subjektov cez trhové konzultácie.

Prístup umožňuje získať cenné pohľady a návrhy od expertov a zainteresovaných strán, ktoré sú priamo ovplyvnené implementáciou novej legislatívy. Práve vďaka tomuto inkluzívnemu procesu sa projekt teší všeobecnému uznaniu a pozitívnemu hodnoteniu.

Cieľom spoločného úsilia ministerstva a partnerov je zabezpečiť hladký prechod na nový regulačný rámec, ktorý bude v súlade s európskymi normami a zároveň bude reflektovať špecifické potreby a výzvy pre sektor dopravy v oblasti kybernetickej bezpečnosti. Implementácia smernice NIS2 v sektoroch spadajúcich do vecnej gescie ministerstva dopravy predstavuje strategický záväzok zvýšiť odolnosť informačných systémov a infraštruktúr voči kybernetickým hrozbám a podporiť bezpečný rozvoj digitálneho prostredia.

Plánované aktivity:
MD SR plánuje realizovať aktivity, ktoré zvýšia povedomie o plánovaných opatreniach v sektore – cez rôzne informačné kanály bude jasne a zreteľne informovať o povinnostiach a skúsenostiach z praxe, ktorými je možné splniť očakávané opatrenia. Budú vo forme workshopov, webinárov, podcastov a cez webové sídlo.

Plánovaná stratégia:
MD SR má implementovanú stratégiu kybernetickej bezpečnosti ako strategický dokument platný pre svoj úrad. V prípade požiadavky a spätnej väzby zo strany sektora dopravy bude ministerstvo zvažovať vydanie stratégie kybernetickej bezpečnosti pre sektor dopravy, prípadne vydanie sektorovej vyhlášky.

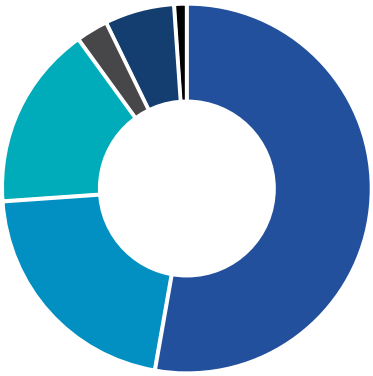
Ľudské zdroje v KB:
Rezort dopravy má v organizačnej štruktúre vytvorené oddelenie stratégie IT a kybernetickej bezpečnosti. Nemá však dedikované personálne kapacity pre plnenie role ústredného orgánu.

Spolupráca v KB:
MD SR v otázkach kybernetickej bezpečnosti spolupracuje s partnermi v štátnej správe – NBÚ a CSIRT.

4.4.1 VÝSLEDKY AUDITOV PZS V SEKTORE DOPRAVA

Národnému bezpečnostnému úradu bolo k 31. 12. 2023 doručených celkovo 5 auditných správ a 2 samohodnotenia zo sektora doprava.

V sektore doprava je priemerná miera súladu nad 50 %, čo vykazuje oproti minulým rokom mierne zlepšenie. Počet nesúladov auditovaných požiadaviek predstavuje 16 %, čo predstavuje priestor na zlepšenie.



PRIEMERNÁ PERCENTUÁLNA MIERA SÚLADU (ROK 2023)	
SÚLAD	53 %
ČIASTOČNÝ SÚLAD	21 %
NESÚLAD	16 %
NEAPLIKOVATEĽNÉ	3 %
OVERENÉ NA INOM MIESTE	6 %
NEVYHODNOTENÉ AUDÍTOROM	1 %

4.4.1 NAJČASTEJŠIE AUDITNÉ ZISTENIA V SEKTORE DOPRAVA

Medzi najčastejšie auditné zistenia v sektore doprava patria:

- nedostatočne definované role a zodpovednosti v oblasti kybernetickej bezpečnosti,
- nie je definovaná a implementovaná klasifikácia informácií a kategorizácia sietí a informačných systémov na základe zákona o kybernetickej bezpečnosti,
- manažér KB nie je menovaný, zásady najnižších privilégií a oddeľovania zodpovedností nie sú formalizované,
- procesy riadenia personálnej bezpečnosti nie sú formálne zavedené, nie je vypracovaný plán rozvoja bezpečnostného povedomia a vzdelávania,
- PZS nemá zavedený plán rozvoja bezpečnostného povedomia,
- programové zraniteľnosti a zraniteľnosti technických prostriedkov sa systematicky nemonitorujú a neriešia,
- schopnosť monitorovania a analyzovania udalostí u PZS je na slabej úrovni.

4.5 Digitálna infraštruktúra

Ústredný orgán: Národný bezpečnostný úrad (NBÚ)

Počet PZS: 15

Počet PZS s povinnosťou auditu v roku 2023: 9
(možné splniť aj samohodnotením podľa §34a ods. 2 ZoKB)

Počet odovzdaných auditných správ: 7

Počet odovzdaných samohodnotení: 0

Podsektory: žiadne

4.5.1 ZHODNOTENIE STAVU KYBERNETICKEJ BEZPEČNOSTI ZA ROK 2023 ÚSTREDNÝM ORGÁNOM

Kritické hrozby:
V sektore digitálna infraštruktúra čelíme závažným kybernetickým hrozbám. NBÚ identifikoval tie najvýznamnejšie, s ktorými sa najčastejšie stretávame v slovenskom kybernetickom priestore.

Patria medzi ne útoky využívajúce sociálne inžinierstvo – najmä phishing a vishing; šírenie škodlivého kódu a zneužívanie zraniteľností. Ďalšou významnou hrozbou pre sektor je zneužívanie kompromitovanej infraštruktúry prevádzkovateľov základných služieb (PZS) na vykonávanie rôznych útokov. Útočníci takýmto spôsobom dokážu riadiť botnetové siete, spúšťať DDoS útoky, šíriť phishing a škodlivý kód.

Okrem týchto hrozieb NBÚ upozorňuje aj na nárast sofistikovanosti kybernetických útokov, nedostatočnú úroveň kybernetickej bezpečnosti v niektorých organizáciách a nedostatočné povedomie o kybernetických hrozbách medzi používateľmi.

Aktivity:
NBÚ v sektore digitálna infraštruktúra aktívne bojuje proti kybernetickým hrozbám. Medzi jeho najvýznamnejšie aktivity patrí koordinácia riešenia kybernetických bezpečnostných incidentov. Úrad koordinuje a usmerňuje reakciu na kybernetické incidenty v sektore a poskytuje pomoc postihnutým subjektom.

Okrem toho NBÚ vykonáva aj preventívne aktivity. Varuje pred hrozbami a posiela relevantné informácie prevádzkovateľom základných služieb v sektore. Poskytuje im aj pravidelné odborné konzultácie v oblasti kybernetickej bezpečnosti. Cieľom aktivít je zvýšiť úroveň kybernetickej bezpečnosti v sektore digitálna infraštruktúra a chrániť tak kritickú infraštruktúru Slovenska.

Plánované aktivity:
NBÚ sa zaviazal k trvalému zlepšovaniu kybernetickej bezpečnosti v sektore. Plánuje kontinuálne pokračovať v existujúcich aktivitách a postupne zlepšovať služby poskytované PZS.

Úrad tiež plánuje pravidelne prehodnocovať situáciu v sektore a v prípade potreby bude reagovať na nové hrozby a výzvy. Cieľom je udržiavať krok s najnovšími trendmi v oblasti kybernetickej bezpečnosti.

Plánovaná stratégia:
NBÚ je zodpovedný za tvorbu a napĺňanie Národnej stratégie kybernetickej bezpečnosti, pričom v akčnom pláne realizácie tejto stratégie má niekoľko úloh. Týkajú sa kybernetickej bezpečnosti na národnej úrovni, a teda aj digitálnej infraštruktúry.

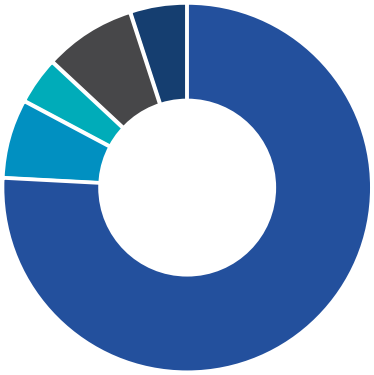
Ľudské zdroje v KB:
NBÚ buduje personálne kapacity v oblasti kybernetickej bezpečnosti kontinuálne, avšak možno konštatovať, že nedostatok odborníkov na pracovnom trhu a trvalé podceňovanie vzdelávania v oblasti kybernetickej bezpečnosti nedokáže adekvátne pokryť všetky požiadavky úradu na personálne obsadenie. Momentálne je situácia zastabilizovaná, avšak s pribúdajúcimi úlohami úradu v oblasti kybernetickej bezpečnosti bude potrebné prijať viac kompetentného personálu.

Spolupráca v KB:
Spolupráca úradu vyplýva priamo zo zákona č. 69/2018 o kybernetickej bezpečnosti. Komplexný pohľad na oblasť spolupráce nájdete v tejto správe nižšie v kapitole „Opatrenia a aktivity“.

4. 5. 2 VÝSLEDKY AUDITOV PZS V SEKTORE DIGITÁLNA INFRAŠTRUKTÚRA

Národnému bezpečnostnému úradu bolo k 31. 12. 2023 doručených celkovo 7 auditných správ zo sektora digitálna infraštruktúra.

Pri pohľade na jednotlivých PZS v sektore je 75 percentná miera súladu s auditnými požiadavkami kontinuálna u väčšiny prevádzkovateľov, čo sa prejavilo aj na celkovej miere súladu v sektore. Tento sektor výrazne zlepšil svoje hodnotenia v porovnaní s predchádzajúcimi rokmi.



PRIEMERNÁ PERCENTUÁLNA MIERA SÚLADU (ROK 2023)	
SÚLAD	76 %
ČIASTOČNÝ SÚLAD	7 %
NESÚLAD	4 %
NEAPLIKOVATEĽNÉ	8 %
OVERENÉ NA INOM MIESTE	5 %
NEVYHODNOTENÉ AUDÍTOROM	0 %

4.5.3 NAJČASTEJŠIE AUDITNÉ ZISTENIA V SEKTORE DIGITÁLNA INFRAŠTRUKTÚRA

Medzi najčastejšie auditné zistenia v sektore digitálna infraštruktúra patria:

- podrobnosti o prijatých technických opatreniach nie sú uvedené v existujúcom zozname prijatých bezpečnostných opatrení,
- PZS nevykonáva a v praxi neimplementoval klasifikáciu informácií,
- spoločnosť nemá jasne definované interné kontrolné prostredie,
- nie sú jednoznačne definované matice prístupov/konfliktných rolí,
- zmluvy s dodávateľmi neobsahujú povinné náležitosti podľa zákona o KB,
- spoločnosť má minimálny počet používateľov vzhľadom na počet koncových zákazníkov,
- nástroj na riadenie prístupových opatrení v spoločnosti nie je zavedený,
- v spoločnosti sú využívané aj lokálne administratívne prístupy, ktoré však nemajú opodstatnenie.

4.6 Elektronické komunikácie

Ústredný orgán: Ministerstvo dopravy Slovenskej republiky (MD SR)

Počet PZS : 11

Počet PZS s povinnosťou auditu v roku 2023: 8
(možné splniť aj samohodnotením podľa §34a ods. 2 ZoKB)

Počet odovzdaných auditných správ: 2

Počet odovzdaných samohodnotení: 0

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

4.6.1 ZHODNOTENIE STAVU KYBERNETICKEJ BEZPEČNOSTI ZA ROK 2023 ZO STRANY ÚSTREDNÉHO ORGÁNU

Zhodnotenie stavu ústredným orgánom pre tento sektor sa nelíši od vyjadrenia v sektore doprava.Okrem týchto hrozieb NBÚ upozorňuje aj na nárast sofistikovanosti kybernetických útokov, nedostatočnú úroveň kybernetickej bezpečnosti v niektorých organizáciách a nedostatočné povedomie o kybernetických hrozbách medzi používateľmi.

4.6.2 VÝSLEDKY AUDITOV PZS V SEKTORE ELEKTRONICKÉ KOMUNIKÁCIE

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

4.7 Energetika

Ústredný orgán: Ministerstvo hospodárstva Slovenskej republiky (MH SR)

Počet PZS: 28

Počet PZS s povinnosťou auditu v roku 2023: 17
(možné splniť aj samohodnotením podľa §34a ods. 2 ZoKB)

Počet odovzdaných auditných správ: 13

Počet odovzdaných samohodnotení: 1

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

3.7.1 ZHODNOTENIE STAVU KYBERNETICKEJ BEZPEČNOSTI ZA ROK 2023 ZO STRANY ÚSTREDNÉHO ORGÁNU

Kritické hrozby

MH SR za rok 2023 z dôvodu nedostatočných personálnych kapacít nevyhodnocovalo žiadne hrozby vo svojich sektoroch. Na požiadanie však MH SR poskytovalo súčinnosť pri riešení kybernetických incidentov.

Zákonné aktivity

Ministerstvo hospodárstva metodicky i na požiadanie spolupracovalo s prevádzkovateľmi podriadených organizácií (napríklad odpovedali na otázky a požiadavky ohľadom KB, pripomienkovali interné riadiace akty týkajúce sa kyberbezpečnosti a prevádzkovej IT bezpečnosti, metodicky pomáhali pri príprave auditov kybernetickej bezpečnosti, v pilotnom projekte rezortnej kybernetickej bezpečnosti riešili vstupné školenia pre novonastupujúcich zamestnancov aj pre jednu z podriadených organizácií, odborne pomáhali niektorým podriadeným organizáciám pri riešení implementácie nových Firewallových riešení).

V spolupráci s CSIRT MIRRI poskytovali súčinnosť pri riešení kybernetického incidentu.

Aktivity nad rámec zákona

V roku 2023 z dôvodu nedostatočných personálnych kapacít nevykonali žiadne ďalšie aktivity nad rámec § 9 ods. 1 písm c).

Aktivity nad rámec zákona
V roku 2023 z dôvodu nedostatočných personálnych kapacít nevykonali žiadne ďalšie aktivity nad rámec § 9 ods. 1 písm c).

Plánované aktivity
Hlavným plánom je posilniť personálne kapacity minimálne o pozíciu koordinátora rezortnej a sektorovej kybernetickej bezpečnosti.

Plánovaná stratégia
Ministerstvo plánuje vydať stratégiu kybernetickej bezpečnosti, čo by mala byť jedna z povinností v pracovnej náplni koordinátora rezortnej a sektorovej kybernetickej bezpečnosti.

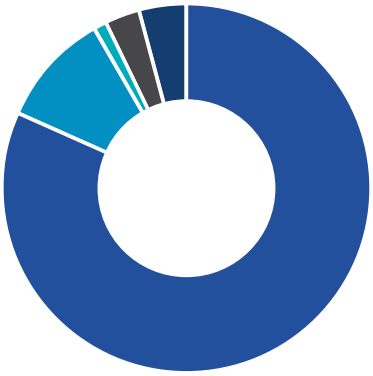
Ľudské zdroje v KB
Ústredný orgán nemá v organizačnej štruktúre vytvorené pozície, ktoré sa venujú kybernetickej bezpečnosti. Nemá ani dostatočné personálne kapacity na spoluprácu v otázkach kybernetickej bezpečnosti s inými sektorovými gestormi a zahraničnými partnermi.

MH SR žiadne iné informácie k uvedeným oblastiam neposkytlo.

4.7.2 VÝSLEDKY AUDITOV PZS V SEKTORE ENERGETIKA

Národnému bezpečnostnému úradu bolo k 31. 12. 2023 doručených celkovo 13 auditných správ zo sektora Energetika.

V sektore energetika je viac ako 80-percentná miera súladu a 10 % čiastočných súladov, čo je dôkazom zlepšovania kvality služieb, avšak ešte stále pretrvávajú výrazné rozdiely miery súladu medzi jednotlivými podsektormi – najmä medzi podsektorom tepelná energetika a ostatnými.



PRIEMERNÁ PERCENTUÁLNA MIERA SÚLADU (ROK 2023)	
SÚLAD	81 %
ČIASTOČNÝ SÚLAD	10 %
NESÚLAD	1 %
NEAPLIKOVATEĽNÉ	3 %
OVERENÉ NA INOM MIESTE	4 %
NEVYHODNOTENÉ AUDÍTOROM	0 %

4.7.3 NAJČASTEJŠIE AUDITNÉ ZISTENIA V SEKTORE ENERGETIKA

Medzi najčastejšie auditné zistenia v sektore energetika patria:

- zoznam kontrolných aktivít v spoločnosti nie je definovaný. Rovnako chýba spôsob uchovávania vykonaných kontrolných aktivít a ich výsledkov,
- informačné systémy, ktoré sú aktuálne vyvíjané nie sú klasifikované a kategorizované do momentu, kým sa nedostanú do ostrej produkcie,
- centrálna konfiguračná databáza nie je zavedená a kompletná ani v IT servisnom nástroji ASET,

- definovaný plán rozvoja nie je zatiaľ pravidelne realizovaný a hodnotená úspešnosť vzdelávania zamestnancov,
- pravidlá a postupy pri riadení prevádzky IT nie sú stanovené a formalizované,
- spoločnosť netestuje procesy riadenia kontinuity činností nakoľko táto povinnosť je úplne nová,
- pre centrálne riadiace systémy existujú vlastné plány obnovy z pohľadu prevádzky, avšak neprihliadajú na zvyšné prostredie spoločnosti.

4.8 Pošta

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

Počet PZS: 5

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

Počet odovzdaných auditných správ: 2

Počet odovzdaných samohodnotení: 2

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

4.8.1 ZHODNOTENIE STAVU KYBERNETICKEJ BEZPEČNOSTI ZA ROK 2023 ZO STRANY ÚSTREDNÉHO ORGÁNU

Zhodnotenie stavu zo strany ústredného orgánu pre tento sektor sa nelíši od vyjadrenia MD SR v sektore doprava.

4.8.2 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.

4.9 Priemysel

Ústredný orgán: Ministerstvo hospodárstva Slovenskej republiky (MH SR)

Počet PZS: 7

Počet PZS s povinnosťou auditu v roku 2023: 4
(možné splniť aj samohodnotením podľa §34a ods. 2 ZoKB)

Počet odovzdaných auditných správ: 3

Počet odovzdaných samohodnotení: 1

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

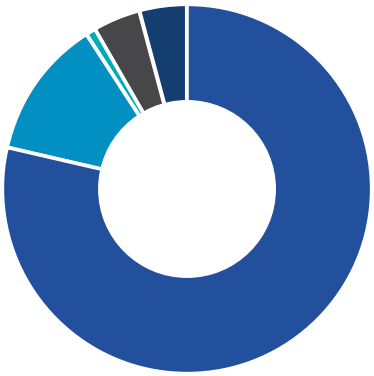
4.9.1 ZHODNOTENIE STAVU KYBERNETICKEJ BEZPEČNOSTI ZA ROK 2023 ZO STRANY ÚSTREDNÉHO ORGÁNU

Zhodnotenie stavu pre tento sektor sa nelíši od vyjadrenia MH SR v sektore energetika, pretože nebolo rozdelené na jednotlivé sektory.

4.9.2 VÝSLEDKY AUDITOV PZS V SEKTORE PRIEMYSEL

Národnému bezpečnostnému úradu boli k 31. 12. 2023 doručené celkovo 3 auditné správy a 1 samohodnotenie zo sektora priemysel.

V sektore je vykazovaných 78 % súladov a 12 % čiastočných súladov, počet nesúladov auditovaných položiek tvoril len 1 %.



PRIEMERNÁ PERCENTUÁLNA MIERA SÚLADU (ROK 2023)	
SÚLAD	72 %
ČIASTOČNÝ SÚLAD	12 %
NESÚLAD	1 %
NEAPLIKOVATEĽNÉ	4 %
OVERENÉ NA INOM MIESTE	4 %
NEVYHODNOTENÉ AUDÍTOROM	0 %

4.9.3 NAJČASTEJŠIE AUDITNÉ ZISTENIA V SEKTORE PRIEMYSEL

Medzi najčastejšie auditné zistenia v sektore priemysel patria:

- nie je vykonávaná analýza funkčného dopadu,
- nie je vykonávaná evidencia realizovaných opatrení KB,
- organizácia nevykonáva pravidelnú analýzu rizík pre informačné systémy základnej služby,
- zoznam kontrolných aktivít v spoločnosti nie je definovaný. Rovnako chýba spôsob uchovávania vykonaných kontrolných aktivít a ich výsledkov,
- proces nie je zavedený konzistentne s dokumentáciou a nevykonáva sa pravidelne. Nie je identifikovaná pravdepodobnosť účinku hrozieb,
- spoločnosť nevykonala analýzu funkčného dopadu základnej služby podľa kritérií pre určenie závažných kybernetických bezpečnostných incidentov podľa § 24 ZoKB.

4.10 Voda a atmosféra

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

Počet PZS: 18

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

Počet odovzdaných auditných správ: 6

Počet odovzdaných samohodnotení: 6

Podsektory: Meteorologická služba, Vodné stavby, Zabezpečovanie pitnej vody

4.10.1 ZHODNOTENIE STAVU KYBERNETICKEJ BEZPEČNOSTI ZA ROK 2023 ZO STRANY ÚSTREDNÉHO ORGÁNU

Kritické hrozby:
Za najzávažnejšiu hrozbu MŽP SR považuje phishingové kampane, ktorých cieľom je získať citlivé informácie alebo peniaze od užívateľov.

Zákonné aktivity:
Ministerstvo sa zúčastňovalo na vzdelávacích aktivitách v oblasti kybernetickej bezpečnosti, ktoré pripravilo MIRRI vďaka projektu „Výcvikové a školiace stredisko pre bezpečnosť prevádzky a správy IT pre sektor VS“.

Aktivity nad rámec zákona:
Gestor sektoru nevykonával nad rámec zákona žiadne iné činnosti alebo aktivity.

Plánované aktivity:
Rezort plánuje počas roka 2024 pokračovať v rozvoji úrovne informačnej a kybernetickej bezpečnosti len na ministerstve a naďalej bude posilňovať preventívne opatrenia pri zvýšení rýchlosti detekcie a riešení incidentov.

Plánovaná stratégia:
Gestor má schválenú stratégiu kybernetickej bezpečnosti na ministerstve a neustále pracuje na vylepšení bezpečnostnej dokumentácie.

Ľudské zdroje v KB:
Inštitúcia má pozície venujúce sa kybernetickej bezpečnosti prierezovo v organizačnej štruktúre. Samostatné oddelenie venujúce sa kybernetickej bezpečnosti ministerstvo nemá.

Spolupráca v KB:
MŽP SR nemá medzirezortnú alebo zahraničnú spoluprácu.

4.10.2 VÝSLEDKY AUDITOV PZS V SEKTORE VODA A ATMOSFÉRA

Národnému bezpečnostnému úradu boli k 31. 12. 2023 doručené celkovo 6 auditných správ a samohodnotení zo sektora Voda a atmosféra.

V sektore Voda a atmosféra je vykazovaných 70 % súladov a 15 % čiastočných súladov, počet nesúladov auditovaných položiek tvoril len 5 %.

PRIEMERNÁ PERCENTUÁLNA MIERA SÚLADU (ROK 2023)	
SÚLAD	70 %
ČIASTOČNÝ SÚLAD	15 %
NESÚLAD	5 %
NEAPLIKOVATEĽNÉ	6 %
OVERENÉ NA INOM MIESTE	4 %
NEVYHODNOTENÉ AUDÍTOROM	0 %

4.10.3 NAJČASTEJŠIE AUDITNÉ ZISTENIA V SEKTORE VODA A ATMOSFÉRA

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,
- proces nie je zavedený konzistentne s dokumentáciou a nevykonáva sa pravidelne. Nie je identifikovaná pravdepodobnosť účinku hrozieb,
- nie je vedená evidencia o oboznámení zamestnancov s politikami KB a nie je zavedený proces kontroly ich dodržiavania,
- riadenie zmien nie je evidované. Riadenie záplat nie je formalizované a vykonáva sa ad hoc,
- 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, havarijné plány aj plány obnovy nie sú testované.

4.11 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: 1 400

Počet PZS s povinnosťou auditu v roku 2023: 122
(možné splniť aj samohodnotením podľa §34a ods. 2 ZoKB)

Počet odovzdaných auditných správ: 53

Počet odovzdaných samohodnotení: 307

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

4. 11. 1 HODNOTENIE STAVU KYBERNETICKEJ BEZPEČNOSTI ZA ROK 2023 ZO STRANY ÚSTREDNÉHO ORGÁNU

MINISTERSTVO OBRANY

Kritické hrozby

Z pohľadu sektora obrany je možné konštatovať že Slovenská republika ako členská krajina NATO a EÚ je už tradičným predmetom záujmu štátnych aktérov vykonávajúcich operácie v kybernetickom priestore, ktoré ohrozujú naše národné záujmy, ale aj bezpečnostné záujmy Aliancie a Únie.

Okrem tradičných zdrojov hrozieb v podobe štátnych aktérov bol v roku 2023 významným zdrojom hrozieb ozbrojený konflikt na Ukrajine, pretože Slovensko jej poskytovalo politickú, ekonomickú a vojensko-technickú podporu.

V hodnotenom období rezort obrany zaznamenal viacero foriem kybernetických útokov – a to phisingové útoky, DDos útoky, útoky typu „hack and leak“, kompromitáciu používateľských účtov, kampane APT skupín a v neposlednom rade aj kybernetickú trestnú činnosť v podobe ransomvérových útokov.

Zákonné aktivity

Centrum pre kybernetickú obranu Slovenskej republiky rozvíjalo spoluprácu s národnou autoritou pre kybernetickú bezpečnosť, relevantnými aktérmi aj ostatnými ústrednými orgánmi a prevádzkovateľmi základných služieb vo svojej pôsobnosti. Cieľom je zlepšovať odolnosť národného kybernetického priestoru a posilňovať kybernetickú bezpečnosť Slovenskej republiky.

Medzi hlavné aktivity v roku 2023 možno zaradiť:

- Participáciu na príprave a novelizácii národnej legislatívy týkajúcej sa kybernetickej bezpečnosti aj interných právnych predpisov,
- Vykonávanie penetračných testovaní,
- Riešenie kybernetických počítačových incidentov v informačnej a komunikačnej infraštruktúre,
- Poskytovanie odborného poradenstva,
- Zdieľanie informácií s národnou autoritou pre kybernetickú bezpečnosť a ďalšími relevantnými národnými a medzinárodnými aktérmi,
- Distribuovanie bezpečnostných varovaní,
- Poskytovanie odborného vzdelávania a výcviku,
- Účasť na národných a medzinárodných cvičeniach kybernetickej bezpečnosti.

Centrum pre kybernetickú obranu Slovenskej republiky spolupracovalo s národnou autoritou aj v oblasti šifrovej ochrany informácií, ktorá zabezpečuje predovšetkým dôvernosť informácií.

Spolupráca sa týkala najmä certifikácie prostriedkov šifrovej ochrany informácií a novelizácie bezpečnostného štandardu systémov a prostriedkov šifrovej ochrany informácií. Tento štandard určuje podmienky posudzovania spôsobilosti chrániť informácie aj v nových prostriedkoch šifrovej ochrany informácií, ktoré sú vyvíjané v Centre pre kybernetickú obranu.

Aktivity nad rámec zákona

Nosnou aktivitou centra aj národnej autority pre kybernetickú obranu bolo okrem uvedených aktivít, týkajúcich sa problematiky kybernetickej bezpečnosti vyplývajúcich z § 9 ods. 1 písm. c) zákona č. 69/2018 o kybernetickej bezpečnosti, aj plnenie úloh vyplývajúcich zo zákona č. 500/2022 o vojenskom spravodajstve.

Úlohy sa týkali vykonávania príslušných kybernetických operácií pre potreby zabezpečovania obranyschopnosti a obrany štátu v kybernetickom priestore aj plnenia medzinárodných záväzkov Slovenskej republiky na úseku kolektívnej obrany a iných medzinárodných dohôd obranného charakteru.

Plánované aktivity

- V priebehu roka 2024 bude vo vzťahu k problematike kybernetickej bezpečnosti Centrum pre kybernetickú obranu Slovenskej republiky vykonávať aktivity, ktoré mu vyplývajú z príslušnej národnej legislatívy a existujúcich zmluvných záväzkov.
- Medzi hlavné aktivity na úseku riadenia kybernetickej bezpečností v podmienkach rezortu obrany v roku 2024 budú patriť:
- Zefektívnenie vykonávania bezpečnostného dohľadu nad rezortnou informačnou a komunikačnou infraštruktúrou,
- Riešenie kybernetických počítačových incidentov v informačnej a komunikačnej infraštruktúre rezortu obrany,
- Poskytovanie odborného poradenstva v rámci rezortu obrany,
- Prehlbovanie a posilňovanie spolupráce s verejnou správou, súkromným a akademickým sektorom,
- Zdieľanie informácií s národnou autoritou pre kybernetickú bezpečnosť a ďalšími relevantnými národnými a medzinárodnými aktérmi,
- Distribuovanie bezpečnostných varovaní v rámci rezortu obrany, ako aj našich partnerov,
- Poskytovanie odborného vzdelávania a výcviku,
- Účasť na národných a medzinárodných cvičeniach kybernetickej bezpečnosti,
- Zabezpečenie auditu kybernetickej bezpečnosti prevádzkovateľov základných služieb v pôsobnosti rezortu obrany,
- Kvalitatívne posilňovanie kybernetických spôsobilostí.

Plánovaná stratégia

V podmienkach rezortu obrany bola v roku 2022 vypracovaná a následne vládou Slovenskej republiky schválená Stratégia pre kybernetickú obranu Slovenskej republiky. Jej plnenie je podrobne rozpracované vo forme špecifických a merateľných úloh v dokumente Akčný plán pre implementáciu Stratégie kybernetickej obrany Slovenskej republiky, ktorých bol v roku 2022 takisto schválený vládou.

Jednou z úloh je vypracovanie interného predpisu záväzného pre všetky organizačné súčasti a zložky rezortu obrany aj organizácií zriadených v pôsobnosti rezortu obrany, ktorý plošne uchopí oblasti definované v prílohe č. 1 k vyhláške NBÚ č. 362/2018.

Ľudské zdroje v KB

V podmienkach Ministerstva obrany Slovenskej republiky je zriadená rezortná autorita pre kybernetickú bezpečnosť, ktorou je Centrum pre kybernetickú obranu Slovenskej republiky.

Ide o osobitné pracovisko Vojenského spravodajstva, ktoré okrem iného má vo vzťahu k problematike kybernetickej bezpečnosti komplexnú pôsobnosť pre sektor obrany. V štruktúre centra je zriadená a prevádzkovaná akreditovaná jednotka na riešenie kybernetických bezpečnostných incidentov v rezorte obrany – CSIRT.MIL.SK.

Spolupráca v KB

Centrum pre kybernetickú obranu Slovenskej republiky pri plnení svojich úloh kladie silný dôraz na spoluprácu – na národnej aj medzinárodnej úrovni.

Národná úroveň sa týka verejnej správy, súkromného a akademického sektora. Medzinárodná spolupráca prebieha na multilaterálnej a bilaterálnej úrovni.

Multilaterálna úroveň je zameraná na kľúčové medzinárodné a regionálne organizácie, ktorých je Slovenská republika členom – EÚ a V4, ale aj na plnenie záväzkov kolektívnej obrany – NATO, EDA a CCDCOE.

Na úseku bilaterálnej spolupráce úzko spolupracuje nielen s vybranými štátmi NATO a EÚ, ale aj s tretími krajinami mimo euroatlantického regiónu.

MINISTERSTVO VNÚTRA

Kritické hrozby:

Zvýšené aktivity a nebezpečné činnosti boli zamerané na infraštruktúru a informačné systémy ministerstva. Nárast škodlivých aktivít súvisí s vojnovým konfliktom na Ukrajine a technologickým pokrokom v oblasti umelej inteligencie.

V roku 2023 ministerstvo nezaznamenalo žiadny závažný kybernetický incident. Eviduje však niekoľko potencionálnych pokusov o ohrozenie kritickej infraštruktúry, z ktorých väčšina boli DDoS útoky.

Celkovo bolo zachytených 25 DDoS útokov, ktoré patria do kategórie menej významných incidentov. Pôvodcovia týchto útokov sú len zriedkavo identifikovaní. Ministerstvo v uplynulom roku nezaregistrovalo žiadny úspešný prípad, pri ktorom by prišlo k narušeniu bezpečnosti a integrity prostredia rezortu využitím phishingu alebo iných metód sociálneho inžinierstva

Zákonné aktivity:

Ministerstvo posilnilo monitoring kybernetického priestoru. Zvýšil sa monitoring nelegálnych webov, sociálnych sietí a komunikačných platforiem s cieľom sledovať aktivity hackerských skupín a hacktivistických hnutí.

Rezort reagovala na bezpečnostné varovania SK-CERT a odstraňoval zraniteľnosti v infraštruktúre. Počas roka sa ministerstvo zameralo na zvyšovanie kybernetického povedomia zamestnancov formou cvičení, vzdelávania a informačných kampaní.

Pre riešenie a nahlasovanie incidentov je k dispozícii 24/7 telefonická a e-mailová podpora. V roku 2023 bolo prešetrených viac ako 1 800 podozrivých e-mailov. V oblasti kybernetickej bezpečnosti ministerstvo vykonalo niekoľko auditov kybernetickej bezpečnosti v zmysle § 29 ods. 1 zákona č. 69/2018 o kybernetickej bezpečnosti

Aktivity nad rámec zákona:

Ministerstvo vykonávalo nad rámec § 9 ods. 1 písm. c) zákona č. 69/2018 o kybernetickej bezpečnosti zvýšený monitoring nelegálnych webov. Zameralo sa na aktivity hackerských skupín a hacktivistických hnutí podporovaných ruskou vládou a jej spriatelenými krajinami, ktoré sa organizujú na darknete, deepwebe aj darkwebe.

Potreba zvýšeného monitoringu súvisela s pretrvávajúcim vojenským konfliktom Ruska s Ukrajinou, ktorý spôsobuje kybernetický tlak na slovenské vládne inštitúcie, kritickú infraštruktúru a na strategické podniky.

Plánované aktivity:

Rezort vnútra začne budovať forenzné laboratórium pre orgány činné v trestnom konaní na zaistenie dôkazov pri kybernetických trestných činoch. Security Operations Center bude monitorovať kritickú infraštruktúru a základné služby ministerstva. Financované bude z Plánu obnovy a odolnosti SR. Ministerstvo plánuje navýšiť počet kvalifikovaných odborníkov v oblasti kybernetickej bezpečnosti. Automatizovaný systém školenia bude zvyšovať bezpečnostné povedomie a znalosti zamestnancov v oblasti kybernetickej bezpečnosti.

Plánovaná stratégia:
Ministerstvo v roku 2024 plánuje vydať *„Stratégiu rozvoja kybernetickej bezpečnosti ministerstva na obdobie rokov 2024 – 2028“* v súlade s rozpracovaným programovým vyhlásením vlády v podmienkach ministerstva.

Ľudské zdroje v KB:
V organizačnej štruktúre ministerstva existuje oddelenie kybernetickej bezpečnosti, ktoré riadi, koordinuje a kontroluje kybernetickú bezpečnosť na ministerstve. Oddelenie plní aj úlohu jednotného kontaktného miesta na nahlasovanie kybernetických incidentov, poskytuje služby na zvládnutie incidentov a následnú obnovu systémov a realizuje preventívne kampane na zvyšovanie povedomia o kybernetickej bezpečnosti.

Spolupráca v KB:
Ministerstvo v oblasti kybernetickej bezpečnosti úzko spolupracuje s Národným bezpečnostným úradom, CSIRT, NASES, NÚKIB a MV ČR. Cieľom je posilniť obranu pred kybernetickými útokmi, zdieľať informácie o aktuálnych hrozbách a koordinovať riešenie kybernetických incidentov na národnej a medzinárodnej úrovni.

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY (MIRRI SR)

Kritické hrozby:
Ako najzávažnejšie hrozby v sektore vidíme nedostatočné implementovanie procesov pre včasné odhaľovanie a opravu zraniteľností, častú absenciu procesov zálohovania dát. Absentuje bezpečnostný monitoring a kybernetické útoky v našom sektore vo veľkej miere zneužívajú sociálne inžinierstvo. V roku 2023 zaznamenal CSIRT v sektore verejnej správy 1 012 incidentov.

Trend hrozieb sa oproti roku 2022 takmer nezmenil. Výnimkou bol pokles použitia škodlivého kódu. Služba vulnerability assessmentu odhalila vlani 750 zraniteľností, z toho 374 kritických.

Zákonné aktivity:
Sekcia kybernetickej bezpečnosti zverejnila materiály pre kybernetickú a informačnú bezpečnosť v sektore ISVS. Materiály slúžia ako metodická príprava dokumentácie pre minimálne bezpečnostné opatrenia kategórie I., II. a III. v súlade so zákonmi o ITVS a KB.

Vzory a šablóny nie sú povinné, ale sú voľne dostupné a bezplatné pre potreby organizácií v sektore ISVS. Môžu sa využiť aj na vzdelávanie pracovníkov v oblasti kybernetickej a informačnej bezpečnosti.

Aktivity nad rámec zákona:
Sekcia kybernetickej bezpečnosti MIRRI SR aktívne posilňuje kybernetickú odolnosť verejnej správy. Implementuje systém včasného varovania a buduje bezpečnostné dohľadové centrá. Pri vzdelávaní rozširuje Cyber arénu a podporuje vznik kompetenčných centier na vysokých školách.

Katalóg orgánov verejnej moci a jednotný metodický rámec dokumentov posilňujú súlad so zákonom o kybernetickej bezpečnosti. Centrálny portál kybernetickej bezpečnosti bude slúžiť ako centrálna brána k informáciám pre subjekty verejnej správy.

Plánované aktivity:
V roku 2024 bude sekcia kybernetickej bezpečnosti pokračovať v plnení úloh vyplývajúcich z právnych predpisov na úseku kybernetickej bezpečnosti, v legislatívnej oblasti plánuje reagovať na návrh novely zákonov, konkrétne zákona č. 69/2018 o kybernetickej

bezpečnosti a zákona č. 45/2011 o kritickej infraštruktúre a s nimi súvisiace potrebné novely podzákonných právnych predpisov.

MIRRI SR má vo svojej gescii vyhlášku č. 179/2020, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy. Touto vyhláškou sa plánuje v najbližšom období zaoberať a novelizovať ju tak, aby reflektovala na všetky súčasné zákonné požiadavky a aby pokryla aj novoobjavené nedostatky.

Sekcia kybernetickej bezpečnosti MIRRI SR bude pokračovať vo finalizovaní vyššie spomínaných a rozbehnutých projektov a plánuje zastrešovať aj nové projekty v tejto oblasti.

Plánovaná stratégia:
V stratégii kyberbezpečnosti plánuje sekcia kybernetickej bezpečnosti MIRRI SR vypracovať tzv. Jednotný metodický rámec (JMR). Má slúžiť predovšetkým na pomoc jednotlivým subjektom verejnej správy, ktorým zákony ukladajú povinnosti v oblasti kybernetickej a informačnej bezpečnosti. Bude obsahovať vzory formulárov, pomocou ktorých si tieto povinnosti budú vedieť jednotlivé subjekty verejnej správy plniť.

Ľudské zdroje v KB:
Sekcia kybernetickej bezpečnosti MIRRI SR sa skladá z odboru riadenia kybernetickej a informačnej bezpečnosti a vládnej jednotky CSIRT. V budúcnosti sa plánuje rozšírenie o oddelenia napríklad na kontrolu kybernetickej a informačnej bezpečnosti a ďalšie.

Spolupráca v KB:
Sekcia kybernetickej bezpečnosti MIRRI SR v súčasnosti spolupracuje s ostatnými ministerstvami, ústrednými orgánmi štátnej a ďalšími subjektmi verejnej správy na úseku kybernetickej bezpečnosti predovšetkým v oblasti legislatívy, ktorá sa týka jednotlivých rezortov v tejto oblasti.

Zároveň plánuje spolupracovať aj s regionálnymi komorami Slovenskej obchodnej a priemyselnej komory a ďalšími subjektmi, ktoré vykonávajú činnosti súvisiace s kybernetickou bezpečnosťou. Výsledky auditov PZS v sektore verejná správa

4. 11. 2 VÝSLEDKY AUDITOV PZS V SEKTORE VEREJNÁ SPRÁVA

Národnému bezpečnostnému úradu bolo k 31. 12. 2023 doručených celkovo 53 auditných správ a 307 samohodnotení zo sektora verejná správa.

Sektor verejná správa má spomedzi všetkých sektorov najhoršie hodnotenia auditovaných požiadaviek. V tomto sektore je vykazovaných 47 % súladov a 16 % čiastočných súladov, počet nesúladov auditovaných položiek tvoril 26 %.

PRIEMERNÁ PERCENTUÁLNA MIERA SÚLADU (ROK 2023)	
SÚLAD	47 %
ČIASTOČNÝ SÚLAD	16 %
NESÚLAD	26 %
NEAPLIKOVATEĽNÉ	5 %
OVERENÉ NA INOM MIESTE	6 %
NEVYHODNOTENÉ AUDÍTOROM	0 %

4.10.3 NAJČASTEJŠIE AUDITNÉ ZISTENIA V SEKTORE VEREJNÁ SPRÁVA

Medzi najčastejšie auditné zistenia v sektore verejná správa patria:

- PZS nemá uzavreté dodatky ku zmluvám, ktoré by odzrkadľovali povinnosti zákona kybernetickej bezpečnosti,
- stratégia kybernetickej bezpečnosti s definíciou cieľov kybernetickej bezpečnosti nie je vypracovaná,
- pravidlá a postupy pre klasifikáciu informácií nie sú zavedené do praxe,
- manažér kybernetickej bezpečnosti nie je formálne určený a poverený výkonom pôsobnosti v zmysle zákona o kybernetickej bezpečnosti a vyhlášky,
- analýza rizík a analýza dopadov sa nevykonáva na pravidelnej báze,
- pravidlá, postupy a zodpovednosti pre riadenie bezpečností sietí nie sú formalizované,
- nie je definovaná a implementovaná politika riadenia prístupov.

4.12 Zdravotníctvo

Ústredný orgán: Ministerstvo zdravotníctva Slovenskej republiky (MZ SR)

Počet PZS: 94

Počet PZS s povinnosťou auditu v roku 2022: 69
(možné splniť aj samohodnotením podľa §34a ods. 2 ZoKB)

Počet odovzdaných auditných správ: 34

Počet odovzdaných samohodnotení: 6

Podsektory: Zdravotnícke zariadenia (vrátane nemocníc a súkromných kliník)

4.12.1 HODNOTENIE STAVU KYBERNETICKEJ BEZPEČNOSTI ZA ROK 2023 ZO STRANY ÚSTREDNÉHO ORGÁNU

Kritické hrozby:
Nedostatočné financovanie a zastaraná technológia ohrozujú kybernetickú bezpečnosť v zdravotníctve. Nízke povedomie personálu o kybernetických hrozbách a zraniteľnostiach zvyšuje riziko útokov.

Kybernetické útoky s využitím umelej inteligencie sú čoraz sofistikovanejšie a ohrozujú kontinuitu poskytovania starostlivosti. Chýbajú plány obnovy a riadenie informačných aktív, čo sťažuje zvládanie incidentov a môže mať vážne následky.

Zákonné aktivity:
V súvislosti s rastúcimi hrozbami v oblasti kybernetickej bezpečnosti zorganizovalo MZ SR stretnutia s vybranými prevádzkovateľmi základných služieb v sektore zdravotníctva.

Cieľom týchto stretnutí bolo vytvoriť funkčné procesy na podporu a koordináciu informačnej a kybernetickej bezpečnosti v organizáciách v jeho pôsobnosti.

Očakáva sa zvýšenie kybernetickej bezpečnosti v sektore zdravotníctva, čo povedie k lepšej ochrane citlivých údajov pacientov a k zníženiu rizika narušenia poskytovania zdravotnej starostlivosti v dôsledku kybernetických útokov.

Aktivity nad rámec zákona:
Ministerstvo zdravotníctva poskytlo súčinnosť Národnému bezpečnostnému úradu pri realizácií regionálnych workshopov pod názvom Kybernetická bezpečnosť v zdravotníctve.

Plánované aktivity:
Príprava a plánovanie stratégie kybernetickej bezpečnosti pre sektor v gescii MZ SR.

Plánovaná stratégia:
Ministerstvo zdravotníctva plánuje v najbližšom období vydať Stratégiu kybernetickej bezpečnosti. Cieľom je posilniť odolnosť rezortu voči kybernetickým hrozbám a chrániť citlivé dáta pacientov. Stratégia bude obsahovať opatrenia na zlepšenie prevencie, detekcie a reakcie na kybernetické bezpečnostné incidenty.

Ľudské zdroje v KB:
Odbor informačnej a kybernetickej bezpečnosti v MZ SR zodpovedá za ochranu informačných systémov a dát pred kybernetickými hrozbami. Implementuje bezpečnostné stratégie, riadi incidenty a podporuje kybernetickú odolnosť v sektore.

Spolupráca v KB:
MZ SR spolupracuje podľa potreby s inými gestormi v oblasti kybernetickej bezpečnosti. Spolupráca so zahraničným partnerom v tejto oblasti zatiaľ neprebiehala.

4. 12. 2 VÝSLEDKY AUDITOV PZS V SEKTORE ZDRAVOTNÍCTVO

Národnému bezpečnostnému úradu bolo k 31. 12. 2023 doručených celkovo 34 auditných správ a 6 samohodnotení zo sektora zdravotníctvo.

V tomto sektore je vykazovaných 61 % súladov a 10 % čiastočných súladov, počet nesúladov auditovaných položiek tvoril 17 %.

PRIEMERNÁ PERCENTUÁLNA MIERA SÚLADU (ROK 2023)	
SÚLAD	61 %
ČIASTOČNÝ SÚLAD	10 %
NESÚLAD	17 %
NEAPLIKOVATEĽNÉ	6 %
OVERENÉ NA INOM MIESTE	6 %
NEVYHODNOTENÉ AUDÍTOROM	0 %

4. 12. 2 NAJČASTEJŠIE AUDITNÉ ZISTENIA V SEKTORE ZDRAVOTNÍCTVO

Medzi najčastejšie auditné zistenia v sektore zdravotníctvo patria:

- nie je zadokumentované vymedzenie rozsahu a spôsobu plnenia všetkých bezpečnostných opatrení,
- stratégia kybernetickej bezpečnosti s definíciou cieľov kybernetickej bezpečnosti nie je vypracovaná,
- nie sú určené hranice a rozhrania informačného systému,
- 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,

- presun práv, povinností a zodpovedností nie je sformalizovaný, postupy pre výkon interných kontrol a auditov nie sú nastavené,
- použitie dvojfaktorovej autentizácie od každého vzdialeného pripojenia do internej siete nie je vyžadované,
- nie sú vyčlenené primerané zdroje pre riadenie kontinuity činností, nie sú zavedené procesy súvisiace s riadením kontinuity činností a dopracované súvisiace dokumenty.

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 NBÚ zriadil stály Monitorovací výbor pre implementáciu úloh Akčného plánu.

Výbor je nezávislým poradným orgánom riaditeľa úradu. Jeho úlohou je monitorovať a koordinovať implementáciu úloh z akčného plánu. Monitorovací výbor pravidelne zasadá a vyhodnocuje napĺňanie jednotlivých úloh. Predsedom výboru je príslušník úradu, členmi výboru sú zástupcovia všetkých subjektov, ktoré majú v akčnom pláne aspoň jednu úlohu.

Jednou z úloh výboru je každoročne pripraviť odpočet plnenia úloh. Vypracúva sa vždy za predchádzajúci rok. Odpočet za rok 2023 bude samostatným dokumentom.

Subjekty pri plnení úloh pravidelne odpočtujú úlohy, aby ich bolo možné vyhodnotiť nasledovným spôsobom:

1. v prípade splnenia úloha musí subjekt dokázať, akým spôsobom bola splnená,
2. v prípade plnenia úlohy musí subjekt uviesť popis, v akom stave je úloha a kedy bude ukončená,
3. v prípade nesplnenej úlohy musí subjekt uviesť dôvod, prečo nebola splnená.

Plnenie úloh akčného plánu napreduje len v niektorých oblastiach. Niektoré subjekty vykazujú mnoho nesplnených úloh, prípadne odpočty za rok 2023 ani nezaslali.

Úlohy viacerých subjektov sú v stave rozpracovania. Oblasť s najnižšou úrovňou plnenia úloh je vzdelávanie. Subjekt s najviac úlohami v tejto oblasti – Ministerstvo školstva, vedy, výskumu a športu SR – označilo mnoho úloh za nesplnené.

Oproti predchádzajúcemu roku však došlo k miernemu posunu plnenia úloh. Bez ohľadu na to, že ide o jednu z najdôležitejších oblastí v oblasti kybernetickej bezpečnosti, zodpovedné subjekty mu neprikladajú adekvátnu dôležitosť a meškaním jednotlivých úloh sa vzďaľuje splnenie strategických cieľov, ktoré boli identifikované v Národnej stratégii kybernetickej bezpečnosti na roky 2021 až 2025.

6 AKTIVITY A OPATRENIA

Úrad potvrdil svoje smerovanie v budovaní bezpečnostného prostredia, ktoré zodpovedá princípom prijatým v Stratégii Európskej únie pre bezpečnostnú úniu na obdobie rokov 2020 až 2025 a v Stratégii kybernetickej bezpečnosti Európskej únie v digitálnej dekáde.

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

Príslušníci úradu sa podieľali na rozvoji medzinárodných vzťahov aj vďaka stálemu zastúpeniu v EÚ a NATO, na rozširovaní ďalších medzinárodných aktivít, bilaterálnych vzťahov aj regionálnej spolupráce.

6.1 Národná legislatíva

Úrad pokračoval v zbere, analýze a vyhodnocovaní informácií získaných z činnosti útvarov úradu, zo spätnej väzby odbornej verejnosti pri prednáškovej činnosti alebo prijatých formou žiadostí o poskytnutie odborného stanoviska s cieľom implementovať ich pri precizovaní všeobecne záväzných právnych predpisov.

Zároveň harmonizoval národnú právnu úpravu s medzinárodne uznávanými prameňmi práva, aby odstránil rozdiely medzi prístupmi v rámci európskych podmienok a zefektívnil stabilitu odborných činností.

V roku 2023 úrad inicioval legislatívny proces dvoch vykonávacích predpisov k zákonu č. 69/2018 o kybernetickej bezpečnosti.

Prvým bola novelizácia vyhlášky Národného bezpečnostného úradu č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov.

Cieľom návrhu novely je jasné vymedzenie kritérií na identifikáciu závažných kybernetických bezpečnostných incidentov. Vyhláškou sa zavádza štandardizovaný systém hodnotenia zraniteľností predstavujúci jednotný spôsob, ktorý slúži na vyjadrenie technických vlastností zraniteľností v hardvéri, softvéri, firmvéri a číselné ohodnotenie ich závažnosti. Aktuálne je návrh novely predmetom interného posudzovania.

Druhým inicializovaným a dokončeným legislatívnym procesom bola novela vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení, ktorá (vyhláška Národného bezpečnostného úradu č. 264/2023) nadobudla účinnosť 1. septembra 2023.

Cieľom novely je vytvorenie funkčného legislatívneho rámca nevyhnutného pre efektívnu realizáciu kľúčových opatrení pre bezpečnosť národného kybernetického priestoru transponujúceho priority a požiadavky, ktoré boli vytvorené na európskej úrovni.

Tento rámec sa zameriava na rozšírenie obsahu bezpečnostných opatrení, obsah a štruktúru bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

6.2 Európska únia

Úrad sa v roku 2023 zúčastňoval na pravidelných zasadnutiach Bezpečnostného výboru Rady EÚ (CSC), Skupiny expertov Európskej komisie (EK) pre bezpečnostnú politiku (ComSEG), Bezpečnostného výboru Európskej služby pre vonkajšiu činnosť (EEAS), Bezpečnostného výboru Agentúry Európskej únie pre vesmírny program (EUSPA), Implementačnej pracovnej skupiny pre TEMPEST (ITTF) a Agentúry Európskej únie pre kybernetickú bezpečnosť (ENISA).

Na pôde Rady EÚ 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 zabezpečená ochrana utajovaných skutočností.

Rok 2023 bol mimoriadne bohatý na legislatívnu aktivitu v Rade EÚ a Európskom parlamente (EP), navyše po právnej stránke bol ukončený legislatívny proces troch spisov. Prvým bol návrh nariadenia EP a Rady 2023/2841, ktorým sa stanovujú opatrenia na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v inštitúciách, orgánoch, úradoch a agentúrach Únie (KB EUIBAs).

Druhým spisom bol návrh nariadenia EP a Rady o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadenia (EÚ) 2019/1020 (CRA).

Tým posledným bol návrh nariadenia EP a Rady, ktorým sa mení nariadenie eIDAS, pokiaľ ide o stanovenie rámca pre európsku digitálnu identitu (eIDAS2). Slovenská republika aktívne podporovala ciele zmieňovaných spisov.

Schválením uvedenej legislatívy sa posilní úroveň kybernetickej bezpečnosti v európskych inštitúciách, zvýši sa spotrebiteľská ochrana pri kúpe a využívaní rozličných softvérových a hardvérových produktov s digitálnymi prvkami a taktiež sa vytvorí predpoklad pre jednoduché a celoúniové overovanie identity občanov EÚ využívajúcich elektronické služby.

Európska komisia (EK) v apríli 2023 zverejnila kybernetický balíček, ktorý sa skladal z dvoch nových legislatívnych a jedného nelegislatívneho spisu. Išlo o návrh nariadenia EP a Rady, ktorým sa stanovujú opatrenia na posilnenie solidarity a kapacít v Únii na odhaľovanie kybernetických hrozieb a incidentov, prípravu a reakciu na ne (CySOLa), o návrh nariadenia EP a Rady, ktorým sa mení nariadenie (EÚ) 2019/881, pokiaľ ide o riadené bezpečnostné služby, (CSA+) a o oznámenie k vytvoreniu Akadémie zručností v oblasti kybernetickej bezpečnosti.

Osobitnú pozornosť si však zaslúži príprava certifikačných schém kybernetickej bezpečnosti EUCC (spoločné kritériá) a EUCS (cloudové schémy).

Horizontálna pracovná skupina pre kybernetické záležitosti (HWPCI) sa vo svojich nelegislatívnych aktivitách venovala aj ostatným strategickým prvkom oblasti kybernetickej diplomacie. V roku 2023 sa jej podarilo aktualizovať rámec pre súbor nástrojov kybernetickej diplomacie (Cyber Diplomatic Toolbox), na základe ktorého bude môcť Rada prijať efektívnejšiu reakciu voči škodlivým kybernetickým aktivitám vrátane sankcií.

Súčasťou tohto rámca boli tiež rozšírené implementačné usmernenia, ktoré zohľadnili konflikt na Ukrajine, vplyvy nových technológií aj zhoršenú geopolitickú bezpečnostnú situáciu. Okrem uvedeného prijala Rada v máji 2023 na základe práce HWPCI závery Rady k európskej politike kybernetickej obrany a v júni 2023 závery Rady k digitálnej diplomacii.

Zástupcovia úradu sa zúčastnili zasadania pracovnej skupiny Certifikačná skupina Európskej únie pre kybernetickú bezpečnosť (ECCG). Hlavnou témou tejto skupiny bola príprava finálneho znenia nariadenia EK ohľadom implementácie horizontálnej certifikačnej schémy pre produkty kybernetickej bezpečnosti a pre samotné ochranné dokumenty, pridanie referencií na existujúce národné schémy, ako aj dohoda, že akceptácia a vzájomné uznanie medzi jednotlivými členskými štátmi má byť plnohodnotná.

Príslušníci NBÚ pôsobili v pracovných formátoch EK ako Skupina pre spoluprácu – NIS a Pracovná skupina pre hodnotenie národných stratégií. Ich hlavnou úlohou je zabezpečovať a zintenzívňovať vzájomnú strategickú a analytickú spoluprácu a zdieľať informácie medzi orgánmi zodpovednými za kybernetickú bezpečnosť členských štátov a ich jednotkami.

Medzi kľúčové priority Skupiny pre spoluprácu – NIS patrila príprava na implementáciu Smernice Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Európskej únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (Smernica NIS 2), a s tým súvisiaca aplikácia jednotlivých nových nástrojov.

K otázkam riešenia národnej implementácie smernice NIS 2 pribudli v súvislosti s hodnotením rizík a rizikových scenárov aj témy súvisiace s prijatými Závermi Rady o vývoji prístupu EÚ ku kybernetickej bezpečnosti.

Boli vytvorené nové subplatformy v Skupine pre spoluprácu ako Work Stream on Risk Evaluation, Work stream Supervision a Work Stream WHOIS s cieľom uchopiť témy hodnotenia rizík, dohľadu, kontroly a podpory bezpečnosti a stability internetu.

V druhom polroku 2023 sa Skupina pre spoluprácu – NIS z dôvodu incidentov, ktoré sa stali v Baltickom mori zamerala aj na „Diskusiu o podmorskej infraštruktúre (dátové káble, potrubia a miesta ich vyústenia)“. Súčasne rezonoval rozvoj vzťahov medzi Skupinou pre spoluprácu a Skupinou pre budovanie odolnosti kritickej infraštruktúry, pretože tieto platformy mali prvý raz spoločné rokovanie.

ENISA realizovala cestovnú mapu potrieb pre cvičenia pre oblasť kybernetickej bezpečnosti. Štáty si zdieľali svoje skúsenosti, pokiaľ išlo o najzávažnejšie incidenty a hrozby v oblasti kybernetickej bezpečnosti, ktoré ich počas roka zasiahli. Dominoval opäť ransomvér. Okrem toho ENISA pripravila prezentáciu, v ktorej sa zamerala na svoje nové povinnosti – najmä tie, ktoré sa týkali členských štátov v súvislosti s plnením notifikačných opatrení.

Príslušníci NBÚ pôsobili aj v nasledujúcich Work Streamoch Skupinách pre spoluprácu:

- Work Stream – Skupina zameraná na notifikačné povinnosti prevádzkovateľov základných služieb,
- Work Stream – Skupina pre riešenie kybernetických bezpečnostných incidentov veľkého rozsahu,
- Work Stream - Skupina pre Digitálnu infraštruktúru,
- Work Stream 5G – Skupina zabezpečenie a ochranu 5G sietí,
- Work Stream – Skupina pre sektor zdravotníctva,
- Work Stream – Skupina pre Voľby.

Vo svojom rozvoji pokračovala aj komunita zainteresovaných subjektov EU CyberNet, 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.

Pravidelné zasadanie Bezpečnostného výboru Európskej služby pre vonkajšiu činnosť (SC EEAS) v rámci svojich úloh a ich činnosti prinieslo revíziu a implementáciu programu bezpečnostného povedomia a zintenzívnili sa školenia personálu o možných kybernetických rizikách.

Naďalej pokračovali aktivity a práce súvisiace s inštitucionalizáciou Európského centra odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a sieť národných koordinačných centier (ECCC). Hlavnou úlohou tohto centra je strategický záujem EÚ zachovať a rozvíjať kapacity kybernetickej bezpečnosti s cieľom zabezpečiť jednotný digitálny trh, chrániť kritické siete a informačné systémy a poskytovať kľúčové služby v tejto oblasti.

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti aktívne zastupovalo úrad v správnej rade ECCC, pričom súčasne plnilo sprostredkované úlohy ECCC ako národné koordinačné centrum. Pozitívne by sa malo vnímať i predstavenie a zaslanie nominácie úradu za Slovenskú republiku na neobsadenú funkciu výkonného riaditeľa ECCC, ktorý bude vyberaný EK a volený správnou radou.

6.3 NATO

Za hlavný míľnik v oblasti kybernetickej bezpečnosti/obrany NATO možno považovať júlový summit vo Vilniuse, počas ktorého pilotne otestovali mechanizmu Virtual Cyber Incident Support Capability (VCISC). Predstavuje virtuálnu spôsobilosť, ktorú môžu spojenci využiť v prípade neschopnosti vyriešiť následky škodlivej kybernetickej aktivity vlastnými silami.

Členské štáty dokážu cez NATO požiadať o poskytnutie pomoci. Slovenská republika sa ešte pred summitom stala dobrovoľným prispievateľom do VCISC a príslušníci NBÚ aktívne participovali na jeho pilotnom testovaní. Ponaučenia z cvičenia budú pretransformované aj do stanovenia cieľov mechanizmu a budovania VCISC komunity.

Ďalšou udalosťou bola nepochybne prvá výročná konferencia o kybernetickej obrane NATO, ktorá bola v novembri v Berlíne a spojila všetky tri úrovne nielen v štruktúrach organizácie, ale aj u 31 spojencov. Slovenská republika bola zastúpená na politickej, technickej a vojenskej úrovni predstaviteľmi NBÚ, Ministerstva zahraničných vecí a európskych záležitostí Slovenskej republiky a Centra kybernetickej obrany.

Jej hlavnými posolstvami boli nevyhnutnosť spolupráce všetkých úrovní so súkromným sektorom, potreba budovania spoločného situačného povedomia, včasné zdieľanie informácií pre rýchlu reakciu na škodlivé kybernetické aktivity, budovanie partnerstiev a spolupráca (primárne EÚ), udržiavanie tempa pri implementovaní nových technológií, väčšia proaktivita a prípadná spoločná atribúcia.

6.4 Regionálna spolupráca

Na základe rotácie predsedníctva krajín, ktoré sú členmi Stredoeurópskej platformy pre kybernetickú bezpečnosť (CECSP), predsedal tejto platforme český Národný úřad pro kybernetickou a informační bezpečnosť (NÚKIB).

Zástupcovia úradu sa aktívne zúčastnili na rokovaniach platformy s kolegami zastupujúcimi krajiny Vyšehradskej štvorky a Rakúska. Predmetom samotných rokovaní boli aktuálne témy, ktoré rezonovali na úrovni EÚ a súčasne sa partneri v týchto témach snažili nájsť spoločné prieniky a vzájomnú podporu.

Medzi tie najdôležitejšie témy stretnutia patrili aktuálny stav procesu transpozície smernice NIS 2.0 v jednotlivých členských štátoch; výskum, vývoj a regionálna spolupráca – český prístup k cvičeniam v oblasti kybernetickej bezpečnosti, osvedčené postupy a možná spolupráca a „Rola právnych poradcov v GovCERT.CZ (LEGAD)“. Experti sa zhodli, že pri aproximácii sa vyžaduje adaptívny, koordinovaný a inovatívny prístup, ktorým sa dosiahne najširšia harmonizácia naprieč celou EÚ.

6.5 Bilaterálne vzťahy

Národný bezpečnostný úrad rozvíjal bilaterálne vzťahy na dennodennej báze naprieč všetkými pracovnými platformami a formátmi, či už pri kontakte počas zasadnutia pracovných skupín alebo pri ad hoc plnení úloh na bilaterálnej úrovni.

Príslušníci úradu pravidelne komunikovali a vymieňali si na národnej úrovni informácie o aktuálnych právnych predpisoch, zraniteľnostiach, hrozbách a incidentoch. Vymieňali si aj informácie o osvedčených postupoch a dobrej praxi so svojimi zahraničnými partnermi aj mimo EÚ. Zúčastňovali sa aj na bilaterálnych rokovaniach a zahraničných prijatiach.

V novembri 2023 NBÚ prijal historicky prvú delegáciu z afrického kontinentu – z Kene. Delegácia tvorili zástupcovia rezortov Ministerstva obrany Slovenskej republiky, Ministerstva vnútra Slovenskej republiky a NC4 výboru pre riadenie kybernetickej bezpečnosti.

Stretnutie bolo iniciované a organizované v spolupráci so Slovenskou agentúrou pre medzinárodnú rozvojovú spoluprácu (SlovakAid) a Veľvyslanectvom Slovenskej republiky v Nairobi. Kenská strana vyjadrila záujem o bližšiu spoluprácu s úradom. Agenda stretnutia bola orientovaná na otázky z oblasti kybernetickej bezpečnosti.

V marci a následne v auguste 2023 boli na žiadosť indonézskej strany iniciované stretnutia s predstaviteľmi Veľvyslanectva Indonézskej republiky v Slovenskej republike a ich odborníkmi pri prehlbovaní spolupráce v oblasti bezpečnosti, regionálnych bezpečnostných výziev a rozvoji bezpečnostnej spolupráce medzi obomi krajinami. Hlavným bodom bolo podpísanie memoranda o porozumení medzi oboma stranami v marci.

Začiatkom roka 2023 bolo v Brne v sídle českého NÚKIB stretnutie so zástupcami úradu na najvyššej úrovni. Cieľom stretnutia bolo podpísať Memorandum o spolupráci medzi Národným bezpečnostným úradom a Národním úřadem pro kybernetickou a informační bezpečnost oboma riaditeľmi úradov. Akt potvrdil aktívnu a dlhodobú spoluprácu medzi oboma úradmi.

V memorande bolo identifikovaných 17 oblastí spolupráce a medzi najdôležitejšie možno zahrnúť ochranu pred aktívnymi kybernetickými hrozbami, incidentami a útokmi; podporu zodpovedného správania štátu v kyberpriestore; cyber threat intelligence (CTI) a strategických analýz; bezpečnosť dodávateľského reťazca informačných a komunikačných technológií; budovanie kapacít a ďalšie.

V septembri 2023 bolo vytvorené miesto styčného dôstojníka úradu na Zastupiteľskom úrade Slovenskej republiky vo Washingtone, ktorého hlavnou úlohou je vytvorenie

úzkej spolupráce v oblasti kybernetickej bezpečnosti a rozvoj spolupráce s príslušnými orgánmi zaoberajúcimi sa ochranou utajovaných skutočností v Spojených štátoch amerických.

6.6 Vydávanie varovaní a bulletinov

Národné centrum kybernetickej bezpečnosti pravidelne vydáva bezpečnostné bulletiny a varovania, ktoré upozorňujú na zraniteľnosti v rôznych systémoch a službách. Sú určené najmä pre PZS a PDS. Na ich odber sa však môže prihlásiť ktokoľvek bezplatne.

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. Bezpečnostné varovania obsahujú kritické zraniteľnosti a v prípade, že majú veľký vplyv, vydáva úrad varovanie aj pre zraniteľnosti s nižšou závažnosťou.

Nasledujúci prehľad uvádza počet vydávaných týždenných bezpečnostných bulletinov a bezpečnostných varovaní za rok 2023.

	Celkový počet bulletinov za rok 2022	Celkový počet varovaní za rok 2022	Celkovo zraniteľností
Január	5	36	**79**
Február	4	30	**61**
Marec	4	27	**73**
Apríl	4	20	**64**
Máj	5	54	**127**
Jún	4	25	**86**
Júl	4	56	**102**
August	5	40	**117**
Október	5	34	**98**
November	4	36	**83**
December	4	27	**108**
SPOLU	48	385	**998**

6.7 Cybergame

V roku 2023 úrad opäť zorganizoval súťaž v oblasti kybernetickej bezpečnosti pod názvom CyberGame, ktorá sa v roku 2022 stala IT projektom roka. Scenáre a úlohy z kybernetickej bezpečnosti sú inšpirované praxou a skúsenosťami profesionálov. CyberGame trvala desať týždňov a obsahovala viac ako 70 úloh rôznej náročnosti.

Na účasť v hre stačil počítač a voľne dostupné analytické nástroje, pričom za každú vyriešenú úlohu hráči zbierali body a vlajky. Tím NCKB zároveň spravoval komunikačný kanál pre hráčov a poradenstvo.

V CyberGame 2023 na hráčov čakalo šesť hracích vetiev – malvérová analýza, forenzná analýza, a OSINT, kryptografia a dve novinky – vetva na zvýšenie úrovne bezpečnosti, takzvaný hardening a netechnická vetvu s názvom procesy a riadenie bezpečnosti.

Novinkou bolo, že CyberGame sa hrala aj na anglickej platforme. Hra sa nevyhla aktuálnemu fenoménu, ktorým je dostupnosť generatívnych jazykových modelov na báze umelej inteligencie.

Do druhého ročníka sa registrovalo 2 334 účastníkov na slovenskej aj anglickej platforme.

Na slovenskej platforme bolo 1 788 registrovaných, z toho 832 aktívnych hráčov, čo znamená v oboch kategóriách výrazný nárast. Vekovú kategóriu do 25 rokov reprezentovalo 754 účastníkov.

6.8 Šírenie povedomia pre širokú verejnosť

Národný bezpečnostný úrad vypracoval v roku 2023 informačné kampane na šírenie povedomia o kybernetickej bezpečnosti. Najrozsiahlejšou kampaňou bol adventný kyberkalendár, ktorý tvoril 24 príspevkov na sociálnych sieťach.

Obsahoval praktické rady, ako sa brániť pred hrozbami v kyberpriestore.

Príslušníci úradu vyučovali aj predmet Bezpečnosť a práca novinára v online priestore na katedre žurnalistiky Univerzity Komenského. Budúcim novinárom prezentovali zásady kybernetickej hygieny, ochranu dát, súkromia aj komunikácie či prácu s otvorenými zdrojmi. Na absolvovanie predmetu museli prepojiť novinárske zručnosti s novými poznatkami z predmetu.

Pozvanie dostali aj na základnú školu v Nitre, kde sa so žiakmi rozprávali o bezpečnom správaní sa na internete. Škola tým zakončila týždeň zameraný na bezpečnosť v kyberpriestore, počas ktorého žiaci riešili kvíz, rozprávali sa o sociálnych sieťach, kyberšikane a mnohom ďalšom. Úrad tak nadväzuje na obdobné aktivity z predošlých rokov a plánuje ďalšie so zapojením viacerých rezortov.

6.8 Činnosť KCCKB

Štátna príspevková organizácia Kompetenčné a certifikačné centrum kybernetickej bezpečnosti (KCCKB) plní úlohu Národného koordinačného centra (NCC-SK) v sieti európskych koordinačných centier a Európskeho centra priemyselných, technologických a výskumných kompetencií v zmysle nariadenia (EÚ) č. 2021/887.

Akreditácia od Európskej komisie potvrdzuje expertízu a kapacitu Kompetenčného centra manažovať európske finančné fondy pre kybernetickú bezpečnosť z priamo riadených programov EÚ.

Vo finančných programoch Slovensko dosiahlo výnimočný úspech na celoeurópskej úrovni. V programe Digital Europe v roku 2023 dominovalo medzi členskými štátmi v počte úspešných projektov. Aktivity Národného koordinačného centra významne prispeli k tomu, že slovenské spoločnosti získali podstatné finančné zdroje na zabezpečenie svojich kyberbezpečnostných potrieb.

KCCKB, NBÚ a Ministerstvo dopravy SR uzavreli grantovú dohodu s Európskou komisiou. Bola zameraná na efektívnu implementáciu smernice NIS2 na Slovensku. S cieľom neustále posilňovať odborné kapacity boli na MIRRI podané žiadosti na dofinancovanie európskych projektov z Plánu obnovy a odolnosti.

Súčasťou cieľov Kompetenčného centra bolo aj intenzívne budovanie odbornej komunity zameranej na kybernetickú bezpečnosť. Toto úsilie viedlo k vytváraniu silných partnerstiev, zdieľaniu osvedčených postupov a zvýšeniu povedomia o dôležitosti kybernetickej bezpečnosti medzi podnikmi, akademickou sférou a verejným sektorom.

Členmi európskej komunity kybernetickej bezpečnosti podľa Nariadenia (EÚ) č. 2021/887 sa vďaka NCC-SK stalo už niekoľko desiatok slovenských subjektov.

Podstatnou časťou úloh Kompetenčného centra je výkon posudzovania zhody v kybernetickej bezpečnosti v zmysle nariadenia (EÚ) 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). Neskôr, po jeho prijatí, sa bude Kompetenčné centrum uchádzať aj o akreditáciu v zmysle Nariadenia o kybernetickej odolnosti (Cyber Resilience Act - CRA).

Kompetenčné centrum je už v súčasnosti akreditované na certifikáciu audítorov a manažérov kybernetickej bezpečnosti podľa osobitného predpisu a normy STN EN ISO/IEC 17024 a integrovaných systémov manažérstva kvality, manažérstva informačnej bezpečnosti, manažérstva IT služieb a manažérstva kontinuity činností, podľa normy STN EN ISO/IEC 17021. Počet certifikovaných osôb sa vďaka Kompetenčnému centru navýšil o 5 certifikovaných audítorov a 7 certifikovaných manažérov.

Ministerstvo spravodlivosti Slovenskej Republiky v legislatívnom procese 2022/806 akceptovalo návrh Národného bezpečnostného úradu na rozšírenie znaleckých odvetví o nové odvetvie kybernetická bezpečnosť. V zmysle bola novelizovaná vyhláška Ministerstva spravodlivosti Slovenskej republiky č. 228/2018, ktorou sa vykonáva zákon č. 382/2004 o znalcoch, tlmočníkoch a prekladateľoch.

KCCKB má ambíciu byť prvou znaleckou organizáciou, ktorá bude vykonávať znalecké činnosti v novom znaleckom odvetví Kybernetická bezpečnosť.

Kompetenčné centrum bolo úspešné aj v oblasti vzdelávania dospelých. V roku 2023 sa podľa zákona č. 568/2009 celoživotnom vzdelávaní podarilo získať od Akreditačnej komisie Ministerstva školstva, vedy a výskumu a športu SR akreditáciu vzdelávacích programov ďalšieho vzdelávania pre školenia Manažér kybernetickej bezpečnosti a Audítor kybernetickej bezpečnosti. Vydaná bola aktualizovaná vzdelávacia schéma.

Do portfólia vzdelávania pribudol nový špecializovaný kurz a workshop Riadenie kontinuity a kurz Riadenie informačnej bezpečnosti. Aktualizované boli sylaby viacerých existujúcich kurzov.

Za rok 2023 bolo realizovaných celkovo 65 školení:

- 8 kurzov Prehľad KB
- 10 kurzov Základy KB,
- 20 kurzov Manažér KB,
- 3 kurzy Audítor KB,
- 9 špecializačných kurzov a workshopov,
- 1 kurz manažérstva informačnej bezpečnosti podľa ISO/IEC 27001:2022
- 14 bezplatných webinárov zvyšovania povedomia o kybernetickej bezpečnosti.

Celkovo sa na uvedených vzdelávacích aktivitách počas roku 2023 zúčastnilo 1 033 účastníkov.

Kompetenčné centrum zorganizovalo úspešnú akciu zvyšovania povedomia o kybernetickej bezpečnosti Cybersecurity Roadshow 2023. Realizované boli viaceré odborné prednášky na konferenciách a pre študentov vybraných vysokých škôl na Slovensku.

Kompetenčné centrum vydalo každý mesiac roka jeden leták na účely zvyšovania bezpečnostného povedomia:

- 10 spôsobov, ako si chrániť osobné údaje – ku Dňu ochrany osobných údajov
- 10 krokov ku kybernetickej bezpečnosti
- Architektúra nulovej dôvery
- Semaforový protokol (TLP)
- Princípy bezpečnostného vývoja SW
- Aké silné je vaše heslo?
- Princípy bezpečného vývoja SW
- 12 krokov ako ochrániť svoju firmu – KB pre malé a stredné podniky
- Kybernetická bezpečnosť v samospráve miest a obcí
- Výber dodávateľa služieb KB: Návod pre obce a mestá v 5 krokoch
- Nariadenie o umelej inteligencii

Už každoročne sú na základe zadania KCCKB spracované prieskumy stavu kybernetickej bezpečnosti. Následne sú vydané aj vo forme verejného dokumentu. Ide najmä o výsledky prieskumu medzi verejnosťou a výsledky prieskumu realizovaného medzi malými a strednými podnikmi.

KCCKB pokračovalo aj v rozširovaní okruhu organizácií, s ktorými uzatvorilo spoluprácu formou podpisu memoranda.

V spolupráci s Národným centrom kybernetickej bezpečnosti postavilo kompetenčné centrum tím mladých ľudí, ktorí Slovensko reprezentovali na podujatí European Cyber-Security Challenge.

Aktivitu zastrešuje Európska agentúra pre kybernetickú bezpečnosť (ENISA). Prítomných bolo 34 národných tímov – k tímom z 28 členských krajín EÚ sa pripojili aj hosťujúce tímy z USA, Kanady, Kostariky, Srbska, Gruzínska a Spojených arabských emirátov. Súťaž trvala od 24. do 27 októbra v Nórsku.

Slovenský tím reprezentovalo desať mladých talentov – deväť chlapcov a jedno dievča. Na súťaž sa tím pripravoval niekoľko mesiacov. V júni sa zúčastnili na medzinárodnom bootcampe vo Viedni a následne na niekoľkých bootcampoch v Bratislave pod vedením technických koučov z NBÚ.