NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SPRÁVA O KYBERNETICKEJ BEZPEČNOSTI

v Slovenskej republike v roku 2024

NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

SPRÁVA O KYBERNETICKEJ BEZPEČNOSTI

v Slovenskej republike
v roku 2024

OBSAH

1. Prehľad hrozieb za rok 2024

1.1 GLOBÁLNE FAKTORY OVPLYVŇUJÚCE KYBERNETICKÚ BEZPEČNOSŤ

1. 1. 1 Vojenské konflikty

Medzi ťažiskové geopolitické faktory vplývajúce na slovenský kybernetický priestor patria prebiehajúce vojenské konflikty, a to hlavne agresia Ruska voči Ukrajine, ktorá dlhodobo zásadným spôsobom ovplyvňuje bezpečnosť Európy. V tomto vojenskom konflikte sú kybernetické operácie významným prvkom ovplyvňujúcim dianie na bojisku, spravodajskú činnosť a kybernetickú bezpečnosť oboch strán. Skúsenosti z konfliktu v oblasti kybernetickej bezpečnosti a obrany sú už v súčasnosti cenným poučením pre celý svet .

Zvyšujúca sa asertivita Číny a jej snahy o rozširovanie vplyvu za región juhovýchodnej Ázie, predstavujú výzvu pre kybernetickú bezpečnosť, ale aj digitálnu suverenitu. Nemožno však prehliadať ani dianie na Blízkom východe – pretrvávajúci izraelsko-palestínsky konflikt a ambície ďalších aktérov regiónu (najmä Iránu).

1. 1. 2 Voľby v zahraničí

Rok 2024 sa vyznačoval vysokou mierou volebných aktivít, pričom voľby sa konali v siedmich z desiatich najľudnatejších krajín sveta, vrátane Spojených štátov amerických. V dňoch 6. až 9. júna 2024 tiež prebiehali v členských štátoch Európskej únie voľby do Európskeho parlamentu. Kybernetické útoky a šírenie dezinformácií sú stále častejším nástrojom na ovplyvňovanie verejnej mienky aj výsledkov volieb. Zanedbanie kybernetickej bezpečnosti v týchto prípadoch môže mať ďalekosiahle dôsledky nielen na vnútropolitický vývoj jednotlivých štátov, ale aj na stabilitu a smerovanie celých regiónov.

Voľby do Európskeho parlamentu predstavovali z hľadiska kybernetickej bezpečnosti osobitnú výzvu. Ich špecifickosť spočíva v paralelnom hlasovaní v 27 členských štátoch EÚ, pričom každá krajina disponuje odlišnou technologickou infraštruktúrou a úrovňou ochrany. Táto fragmentácia vytvára rozdiely v zraniteľnosti volebných systémov, čo zvyšuje riziko ich narušenia. Potenciálne incidenty môžu podkopať dôveru v legitimitu zvolených zástupcov, a tým oslabiť dôveryhodnosť Európskeho parlamentu ako celku.

Medzi najzásadnejšie hrozby, ktoré voľby v zahraničí sprevádzali, patrilo systematické ovplyvňovanie verejnej mienky prostredníctvom dezinformačných kampaní. Kampane boli často zamerané na posilnenie preferencií pre konkrétnych kandidátov alebo politické subjekty. Využívali sofistikované nástroje, ako sú falošné účty na sociálnych sieťach, automatizované boty, cielene upravený obsah a algoritmické zosilňovanie polarizujúcich tém. Ich cieľom nebolo len ovplyvniť volebný výsledok, ale aj prehĺbiť spoločenské rozdiely a znížiť dôveru občanov v samotný demokratický proces volieb.

Paralelne s tým prebiehali aj priame kybernetické útoky, ktoré cielili na viaceré úrovne volebných infraštruktúr. Útočníci sa zameriavali na národné volebné systémy, databázy voličov, ako aj na servery politických strán, kandidátov či inštitúcií zapojených do organizácie a vyhodnocovania volieb. Mimoriadne rizikové boli snahy kompromitovať aj systémy priamo súvisiace s technickým zabezpečením volieb v niektorých krajinách

Európskej únie, čo by mohlo spochybniť nielen priebeh, ale aj celkové výsledky volieb do Európskeho parlamentu.

Nemenej významná bola aj tretia rovina hrozieb – zneužitie ľudského faktora. V mnohých prípadoch sa útočníci snažili získať prístup k citlivým informáciám prostredníctvom kompromitácie osobných účtov jednotlivcov, ktorí zohrávali kľúčové úlohy vo volebných kampaniach, či pri organizácii hlasovania. Takto získané informácie mohli byť následne využité na vydieranie, diskreditáciu alebo manipuláciu rozhodovania týchto osôb.

1. 1. 3 Crowdstrike

V júli 2024 došlo k rozsiahlemu výpadku bezpečnostného softvéru Falcon Sensor od spoločnosti CrowdStrike, ktorý mal výrazný dopad na technologickú infraštruktúru naprieč rôznymi sektormi po celom svete. Hoci ide o softvér, ktorý je pre väčšinu bežných používateľov neznámy, jeho význam v oblasti kybernetickej bezpečnosti je zásadný. Používa sa na miliónoch zariadení, často bez vedomia samotných užívateľov, ktorí netušia, že tento „antivírus“ beží na pozadí ich systémov.

Falcon Sensor slúži na detekciu škodlivého softvéru a správania v reálnom čase a je implementovaný predovšetkým vo firemných a vládnych systémoch. V daný deň – 19. júla 2024 – CrowdStrike vydala rutinnú aktualizáciu tzv. Rapid Response Content, ktorou mala zlepšiť schopnosť senzorov reagovať na nové hrozby v rámci operačného systému Windows. Chyba v tejto aktualizácii však spôsobila, že milióny počítačov po celom svete prešli do kritického stavu „Blue Screen of Death“ (BSOD), čím sa stali nepoužiteľnými.

Tento incident je učebnicovým príkladom tzv. kaskádového zlyhania – teda situácie, pri ktorej technický problém v jednom komponente vedie k reťazovým poruchám v mnohých naviazaných systémoch. Postihnuté boli len zariadenia s verziou Falcon Sensor 7.11 a vyššou, ktoré dostali aktualizáciu v krátkom časovom okne medzi 04:09 a 05:27 UTC. Po odstránení chyby vydal CrowdStrike opravnú aktualizáciu, avšak v tom čase už bolo postihnutých vyše 8,5 milióna zariadení.

Následky boli okamžité a globálne. V Spojených štátoch amerických bolo zrušených viac ako 3-tisíc letov, ďalších 11-tisíc meškalo. Výpadok sa dotkol aj Slovenska – Letisko Milana Rastislava Štefánika v Bratislave zaznamenalo zlyhanie odbavovacieho systému. V zdravotníctve bolo pozastavených alebo odložených množstvo zákrokov, čo poukazuje na mieru závislosti tejto infraštruktúry od spoľahlivého fungovania IT systémov. Finančné inštitúcie čelili meškaniu transakcií a výplat, médiá ako Sky News hlásili výpadky vysielania.

Jedným z najzaujímavejších prípadov, ktoré vznikli počas výpadku CrowdStrike, bola vlna phishingových útokov zameraných na klientov v Latinskej Amerike. Hackeri sa snažili zneužiť zraniteľnosť vytvorenú výpadkom a rozposielali e-maily s infikovanými prílohami, ktoré sa tvárili ako oficiálne oznámenia od CrowdStrike. Tento typ útoku bol o to nebezpečnejší, že sa zameriaval na ľudí, ktorí si neboli vedomí technických detailov výpadku.

1. 1. 4 Rozvoj umelej inteligencie

V posledných rokoch sme svedkami výrazného nárastu sofistikovanosti kybernetických útokov, najmä vďaka integrácii umelej inteligencie (AI) do arzenálu kybernetických zločincov. Nedávne štúdie a incidenty poukazujú na to, že AI umožňuje útočníkom vytvárať mimoriadne presvedčivé a personalizované phishingové kampane, ktoré sú ťažko odhaliteľné aj pre skúsených používateľov.

Modely AI zlepšili v porovnaní s predchádzajúcimi rokmi svoje schopnosti v presvedčivosti a klamaní. Kým v minulosti potrebovali AI modely ľudskú asistenciu na dosiahnutie výkonu porovnateľného s ľudskými expertmi, súčasné modely dokážu generovať vysoko efektívne phishingové e-maily samostatne. Tento pokrok poukazuje na rýchly vývoj AI technológií a ich potenciálne zneužitie v kybernetických útokoch.

1. 2 NAJVÝZNAMNEJŠIE HROZBY V SLOVENSKEJ REPUBLIKE ZA ROK 2024

1. 2. 1 Sociálne inžinierstvo

V porovnaní s predchádzajúcim rokom nastal v prvom kvartáli roka 2024 mierny nárast počtu hlásených incidentov. Najvyššie množstvo incidentov naďalej súviselo so získavaním informácií, a to pomocou využívania sociálneho inžinierstva. Najviac zastúpený typ škodlivej aktivity predstavovali phishingové útoky. V rámci sledovaného obdobia došlo k uskutočneniu viacerých phishingových kampaní zameraných na zamestnancov subjektov v sektore verejná správa. Počas týchto kampaní sa útočníkom podarilo úspešne kompromitovať viaceré e-mailové účty, pričom tie boli následne zneužité na ďalšie šírenie phishingových správ. Obzvlášť nebezpečné boli kampane šírené z kompromitovaných e-mailových schránok s doménami .sk a .cz. Analýza ukázala, že tieto útoky zasiahli najmä systémy konkrétnych poskytovateľov, čo naznačuje prieniky do ich infraštruktúry.

V predmetnom období boli zaznamenané aj phishingové kampane cielené na širokú verejnosť, pričom pravdepodobným úmyslom útočníkov bolo získať osobné a citlivé údaje od obetí s cieľom ich zneužitia v ďalších škodlivých aktivitách alebo krádeže finančných prostriedkov z bankových účtov. Rozsiahle kampane mimo iných zneužívali identitu letiska pri využití tematiky predaja batožiny, ale aj identitu telekomunikačnej spoločnosti či poskytovateľa streamovacej služby.

V súvislosti s celosvetovými trendmi, medzi najväčšie kybernetické hrozby patril ransomvér. V uplynulom období sa obeťami tohto typu škodlivej aktivity stalo niekoľko prevádzkovateľov základnej služby aj organizácií zo súkromného sektora. Pri útokoch boli často použité ransomvérové nástroje z „rodiny“ LockBit 3.0 alebo RansomHub.

Spomedzi rôznych typov techník útočníci využívali aj tzv. malwaretisement, teda šírenie škodlivého kódu pomocou dôveryhodne pôsobiacich reklám na legitímnych webových stránkach. Bolo zaznamenaných niekoľko kampaní, pomocou ktorých bol rozširovaný malvér naprogramovaný na krádež údajov obetí. Jeden z prípadov sa týkal aj sektora verejná správa, pričom kampaň bola vedená aj pomocou slovenských kompromitovaných účtov.

Stúpajúci trend nahlasovaných kybernetických bezpečnostných incidentov pretrvával najmä v oblasti získavania informácií, a to hlavne prostredníctvom sociálneho inžinierstva, phishingu a smishingu (SMS). Používatelia informačných systémov verejnej správy

boli pravidelným cieľom phishingových kampaní za účelom kompromitácie e-mailového konta. V druhom kvartáli roka 2024 zaznamenal NBÚ snahu o falošný spôsob zmeny hesla na podvodnom webovom sídle e-mailového klienta.

Metódou smishingu (SMS) boli rozposielané falošné SMS s informáciou o konci platnosti diaľničných známok, ktoré adresátov presmerovali na falošný platobný portál. Na platforme Bazos.sk pokračovali podvody, pri ktorých útočníci zasielali inzerentom podvodné e-maily s falošnými inštrukciami pre kuriérske služby, čím sa snažili získať údaje o platobných kartách. Taktiež došlo k nárastu falošných telefonátov, v ktorých sa podvodníci vydávali za políciu alebo Europol a obete zastrašovali domnelým porušením zákona.

Ďalšie kampane sa zameriavali na zneužitie identity portálu slovensko.sk. Obete boli v tomto prípade lákané na falošné správy o vrátení daní alebo pokutách za prekročenie rýchlosti. Cieľom útočníkov bolo získať prihlasovacie údaje. V iných prípadoch boli rozosielané e-maily napodobňujúce komunikáciu od dodávateľov energií. Tieto obsahovali prílohy so škodlivým softvérom, ako napríklad infostealer REMCOS, ktorý je navrhnutý na krádež citlivých údajov. Útočníci taktiež registrovali domény, ktoré sa podobali oficiálnym vládnym webovým stránkam, napríklad „govenment.sk“ alebo „vladagov.sk“. Tieto domény boli zneužité na rozosielanie phishingových e-mailov, pričom v určitých fázach útoku útočníci upravili DNS záznamy, aby imitovali legitímne stránky siete Govnet. V rámci riešenia tejto situácie vznikla potreba zaviesť kontrolné mechanizmy, ktoré by zabránili registrácii domén napodobňujúcich názvy štátnych inštitúcií.

1.2.2 Nedostupnosť služieb a DDoS útoky

Prognóza o možných kybernetických incidentoch počas volieb do Európskeho parlamentu sa naplnila. Úrad zaznamenal rozsiahly DDoS útok na významné webové sídlo v rámci sektora verejnej správy, ktoré bolo na krátky čas nedostupné.

Hacktivistické skupiny v období po pokuse o atentát na predsedu vlády SR spustili vlnu DDoS útokov na bankový sektor a sektor verejnej správy. Cieľom takýchto útokov býva zvyčajne snaha o nedostupnosť často využívaných produktov a služieb.

Europol potvrdil kompromitáciu portálu platformy pre expertov (EPE). Táto udalosť mala vplyv na inštitúcie SR a ich používateľov, ktorí participujú na činnosti Europolu za Slovenskú republiku.

Slovensko tiež čelilo viacerým závažným kybernetickým incidentom, ktoré poukázali na narastajúce riziká a zraniteľnosti v rôznych sektoroch. Medzi najzávažnejšie patrila kompromitácia spoločnosti pôsobiacej v oblasti vodohospodárstva, kde útočníci zneužili zraniteľnosť v platforme ESXi. Podobne bol napadnutý aj systém sociálneho zariadenia pre seniorov, pričom ransomvérový útok narušil jeho prevádzku.

1.2.3 Bombové hrozby

Na Slovensku dlhodobo dochádza k anonymným vyhrážkam bombovými útokmi. Vyhrážky sú poväčšine cielené na školské zariadenia, súdy, mestá a obce, letiská a podobne. Typicky sú oznamované telefonicky alebo e-mailom a orgánom činným v trestnom konaní sa často podarilo vypátrať páchateľov.

Od decembra 2023 však pozorujeme výrazný nárast prípadov anonymných bombových vyhrážok. Vyhrážky sa začali objavovať čoraz častejšie a cieľom boli veľké skupiny subjektov naraz. Tento trend viedol k zvýšeniu strachu v spoločnosti, preťaženiu

bezpečnostných zložiek a významným časovým a finančným stratám v postihnutých organizáciách.

V treťom kvartáli 2024 sa zvýšil záujem útočníkov o medializovanie a publikovanie informácií o bombových hrozbách, čo je výrazný posun v porovnaní s druhým kvartálom toho istého roku. Lokálna televízia na východe Slovenska dokonca zverejnila kompletný screenshot výhražného e-mailu vrátane odkazov na profil a komunikáciu útočníka cez Telegram, čo vyvolalo nárast návštevnosti a popularity spomenutého telegramového účtu.

Kým v prvej polovici roka 2024 boli hlavnými cieľmi školské inštitúcie, v treťom kvartáli sa spektrum cieľov výrazne rozšírilo. Bombové hrozby začali zasahovať aj letiská, jadrové elektrárne, budovy samospráv, cirkevné objekty a miesta s vysokou koncentráciou ľudí. Tento posun poukazuje na zmenu taktiky zo strany útočníkov, ktorí začali cieliť na širší okruh kritickej infraštruktúry s cieľom zvýšiť chaos a narušiť chod viacerých sektorov.

Jedným z ďalších dôležitých trendov v treťom kvartáli 2024 je adaptácia útočníkov. Kým v minulosti boli nahlasovania bombových hrozieb často vykonávané prostredníctvom bežných e-mailových služieb, útočníci začali vo väčšej miere využívať anonymizačné nástroje, ako VPN siete a službu Mail2Tor. Tento prechod sťažuje identifikáciu zdrojov hrozieb a predlžuje čas potrebný na odhalenie páchateľov. Anonymizácia komunikácie predstavuje vážny problém pri vyšetrovaní, pretože bezpečnostné zložky musia čeliť rastúcej technickej sofistikovanosti útočníkov. Zvyšuje sa tak potreba investovať do nových technológií na monitorovanie a analýzu šifrovanej komunikácie, pričom kľúčovou sa stáva spolupráca so zahraničnými partnermi, ktorí disponujú pokročilejšími nástrojmi a skúsenosťami s riešením podobných hrozieb.

1.3 AKTÉRI HROZIEB

1. 3. 1 APT skupiny

V období roka 2024 dochádzalo k snahám o kompromitáciu prevažne zo strany ruských a čínskych skupín, najmä s cieľom krádeže dát a kybernetickej špionáže. Využívali na to rôzne zraniteľnosti, šírenie malvéru a metódy sociálneho inžinierstva (predovšetkým phishing a spearphishing). Identifikované bolo aj zvýšené využívanie AI modelov, ktoré mali za cieľ zefektívniť aktivity APT skupín.

V období prezidentských volieb v USA boli zaznamenané zvýšené aktivity severokórejských a iránskych APT skupín. Identifikované boli aj ich snahy o prieniky do zariadení súvisiacich s americkými prezidentskými voľbami. Severokórejské skupiny začali vo vyššej miere vykonávať kampane, v ktorých sa vydávali za spoločnosti ponúkajúce lukratívne pracovné príležitosti osobám v záujmových oblastiach.

V európskom priestore patrili hybridné aktivity voči Rumunsku v období prezidentských volieb medzi najväčšie udalosti roku 2024. V krajine dochádzalo k masívnym kybernetickým útokom sprevádzaným vplyvovými kampaňami na sociálnych sieťach. Vzhľadom na rozsah týchto aktivít možno predpokladať, že išlo o štátom sponzorovanú skupinu. Zásadnou kompromitáciou bol aj prienik čínskej APT skupiny do štátnych systémov USA a oblasti kritickej infraštruktúry.

Na Slovensku sme zaznamenali pokusy o kompromitáciu štátnych inštitúcií prevažne zo strany ruských a čínskych APT skupín. Väčšina z identifikovaných aktivít nebola cielená výhradne na slovenské štátne inštitúcie, avšak Slovensko bolo hromadným cieľom ako súčasť kampaní smerovaných špeciálne na krajiny Európskej únie.

1. 3. 2 Hacktivistické skupiny

Primárne ruské hacktivistické skupiny vykonávali prevažne z ideologických dôvodov DDoS útoky voči štátnym inštitúciám, mimovládnym organizáciám, súkromným spoločnostiam, a to najmä v európskom priestore a v krajinách NATO. Dôvodom útokov bolo najmä to, že napadnuté krajiny finančne, vojensky alebo humanitárne podporovali Ukrajinu. Útoky boli vykonávané aj v kontexte volieb do Európskeho parlamentu. Ruské hacktivistické skupiny začali koncom roka vo väčšej miere vykonávať útoky aj na Taiwan. Medzi najvýznamnejšie skupiny patrili Killnet, NoName057(16), Kybernetická armáda Ruska Reborn, HackNeT a projekt DDOSIA.

Jednou z najvýznamnejších aktivít hacktivistických skupín v roku 2024 bol prienik skupiny Kybernetická armáda Ruska Reborn do systémov, ktoré kontrolovali vodnú infraštruktúru v USA. Existuje predpoklad, že skupina je napojená na ruskú APT skupinu Sandworm. Táto APT skupina je známa tým, že maskuje svoje aktivity prostredníctvom rôznych hacktivistických skupín.

Na Slovensku hacktivistické skupiny vykonávali útoky voči slovenským cieľom v oveľa nižšej miere ako v roku 2023. V prvej polovici roka 2024 bola identifikovaná zvýšená aktivita, ale aj tá predstavovala oveľa menší počet útokov ako v roku 2023. K sérii útokov došlo po pokuse o atentát na predsedu vlády SR. Po zvyšok roka boli útoky hacktivistických skupín na Slovensku vykonávané sporadicky.

1. 3. 3 Kriminálne skupiny

Kriminálne skupiny vykonávali ransomvérové útoky na súkromné spoločnosti, nemocnice, dodávateľov služieb aj štátnu správu. Skupiny vykonávali svoje aktivity oportunisticky, s cieľom čo najvyššieho zisku. Najvýznamnejšie boli aktivity skupín Qilin, Medusa, INC Ransom, LockBit, BianLian, RansomHub, Lynx Ransomware.

V Slovenskej republike boli pri viacerých incidentoch identifikované aktivity kriminálnych skupín LockBit, RANSOMHUB, MIMIC, MEDUSALOCKER a YZQE.

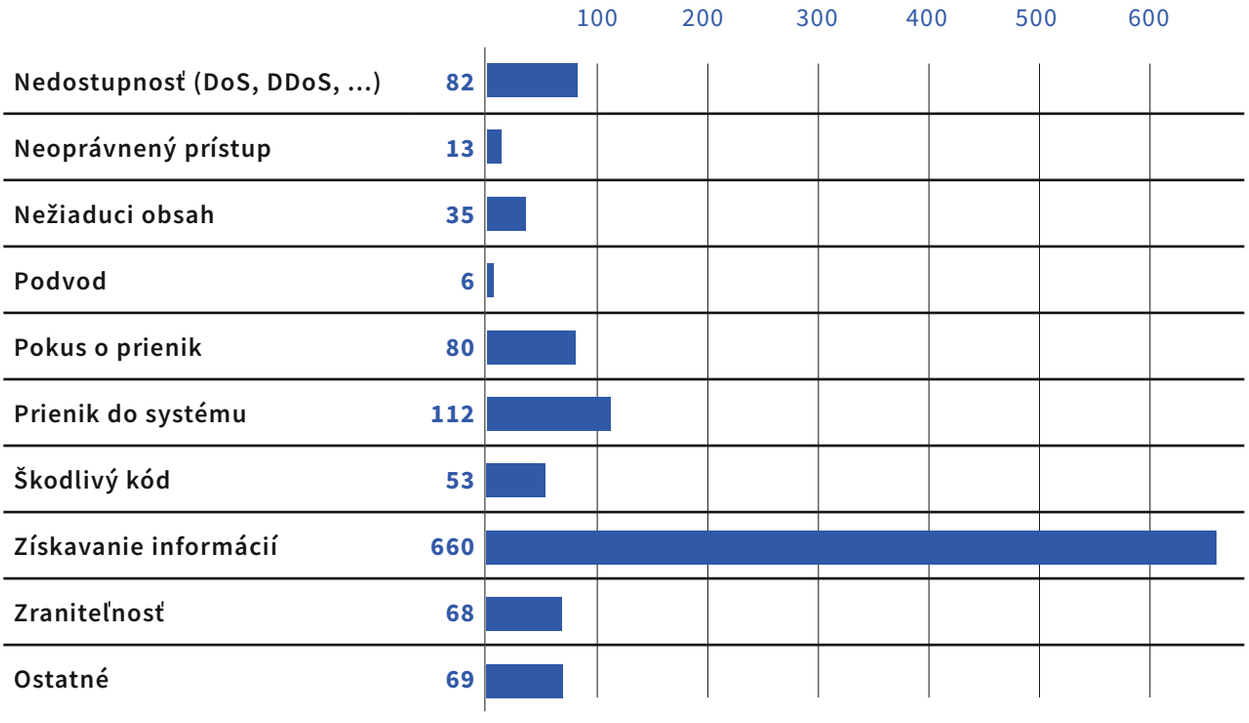
2. Štatistický prehľad incidentov za rok 2024

2. 1 ZÁKLADNÝ PREHĽAD

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

Štatistické vyhodnotenie kybernetických bezpečnostných incidentov vychádza z metodiky zavedenej v roku 2023 a zahŕňa len incidenty hlásené NCKB.

TYP NAHLÁSENÉHO INCIDENTU



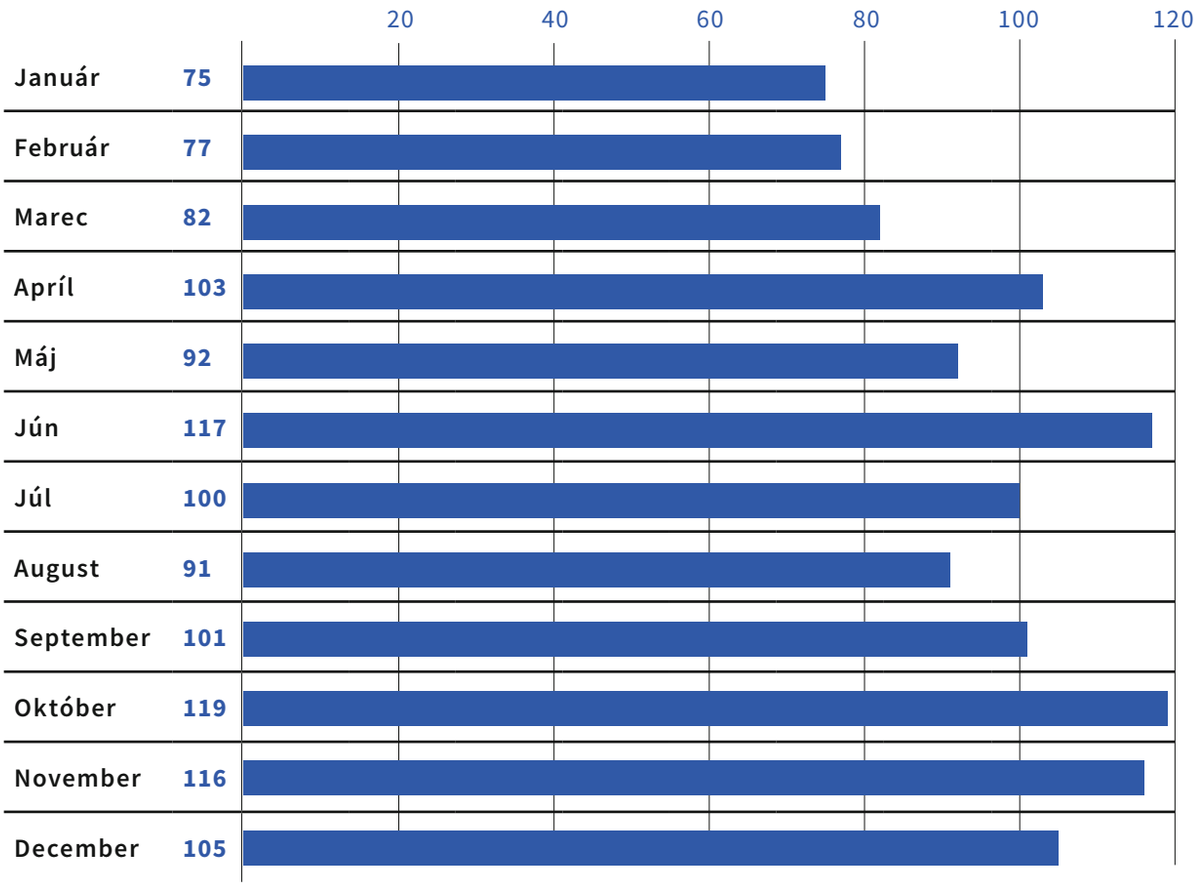
V roku 2024 dominovali technické typy útokov, ako sú získavanie informácií, nedostupnosť, prienik do systému, pokus o prienik a zraniteľnosť.

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.

V roku 2024 bolo najviac hlásení o kybernetických bezpečnostných incidentoch prijatých v druhej polovici roka. V roku 2024 prijal SK-CERT o 204 hlásení viac ako v predchádzajúcom roku. Nárast hlásení incidentov je možné pripísať legislatívnemu procesu transpozície smernice NIS2, ktorá rozširuje pôsobnosť na ďalšie subjekty. Verejná diskusia k novele zákona o kybernetickej bezpečnosti nepochybne zvýšila povedomie týkajúce sa povinnosti hlásiť incidenty. Aj preto sa zo zvýšeného počtu nahlásených incidentov nedá jednoznačne vyvodzovať záver, že slovenský kybernetický priestor sa stal menej bezpečnejším.

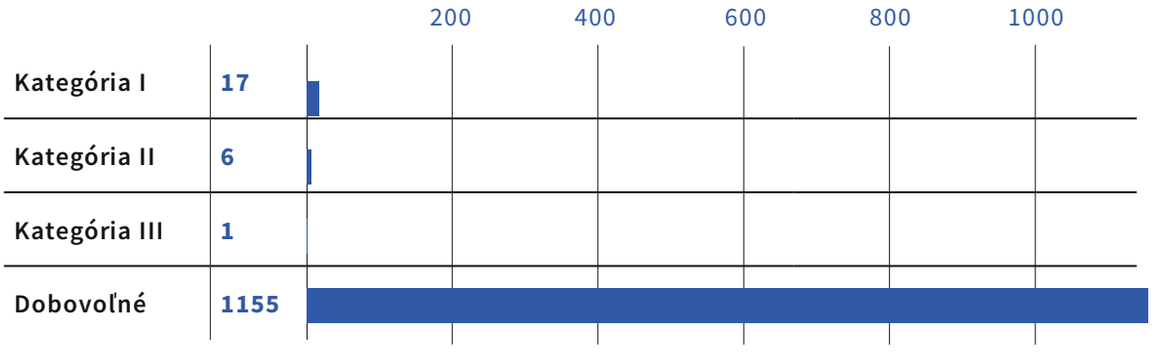
Celkové počty hlásených incidentov opačným smerom ovplyvňuje pretrvávajúca neznalosť alebo neochota nahlasovať incidenty u niektorých prevádzkovateľov základných služieb (PZS) a poskytovateľov digitálnych služieb (PDS), ale aj zvyšujúca sa sofistikovanosť škodlivých aktivít aktérov hrozieb, ktoré sú ťažšie detekovateľné.

POČET HLÁSENÝCH KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV Z ČASOVÉHO HĽADISKA



Dobrovoľné hlásenia výrazne prevládali nad povinnými kategorizovanými hláseniami. Pretrvávajú rozdiely v zrelosti a právnom povedomí prevádzkovateľov základných služieb, ktoré má za následok nehlásenie incidentov, ich oneskorené hlásenie alebo preferovanie dobrovoľného hlásenia pred povinným hlásením závažného incidentu.

HLÁSENIA INCIDETOV PODĽA ZÁVAŽNOSTI



2. 2 INCIDENTY PODĽA SEKTOROV

V roku 2024 stúpol počet hlásených kybernetických incidentov. Tento trend však neprejavuje vo všetkých sektoroch.

V sektore bankovníctvo pozorujeme zníženie počtu hlásení bezpečnostných incidentov. V tomto sektore sú kontinuálne vykazované najlepšie výsledky auditných správ a hodnotení kybernetickej bezpečnosti.

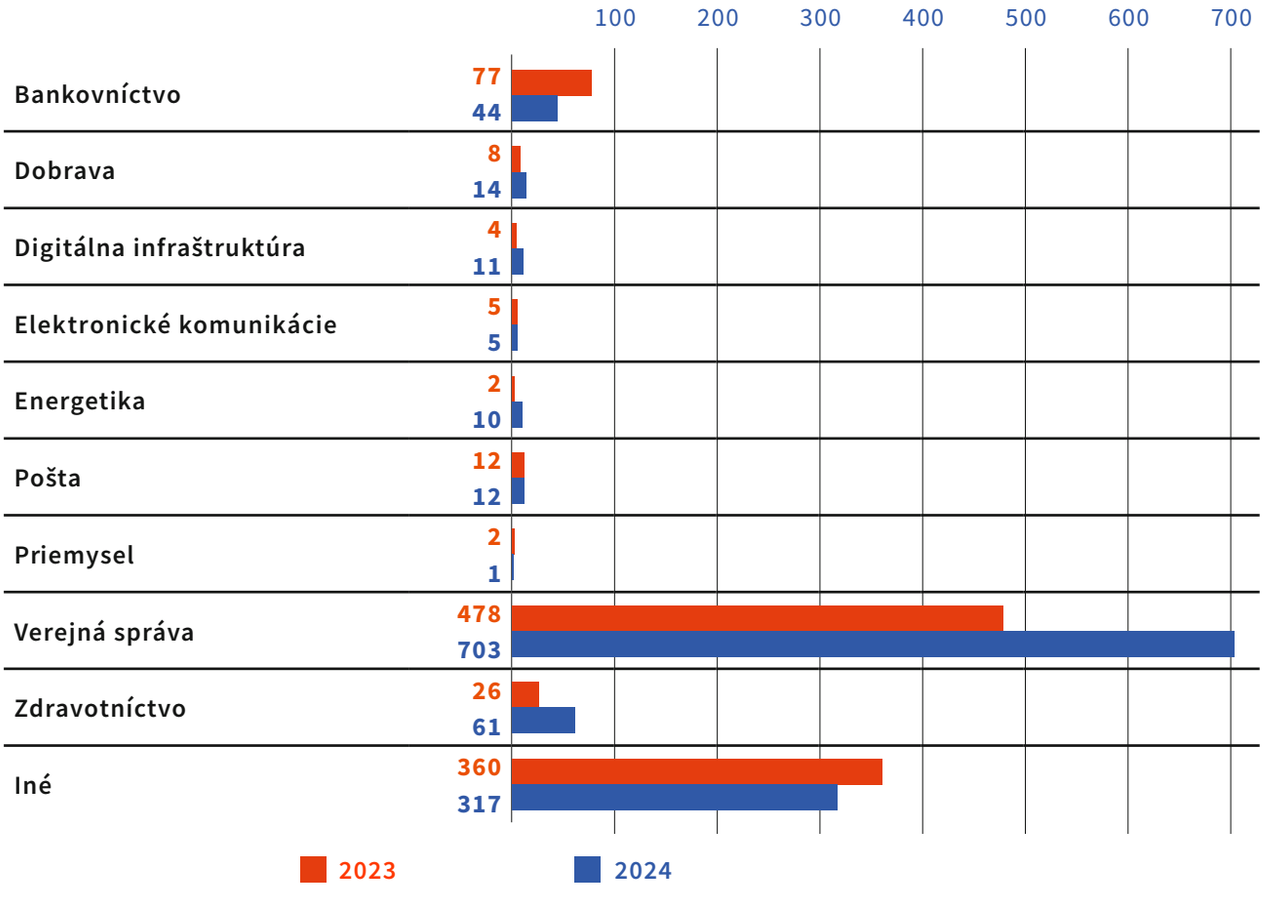
Najviac incidentov bolo hlásených vo verejnej správe, kde počet prípadov výrazne narástol z 478 v roku 2023 na 703 v roku 2024. Tento nárast môže naznačovať jednak zvýšenú hrozbu, teda motiváciu útočníkov, ale aj zlepšenie v oblasti detekcie a hlásenia incidentov.

Sektor zdravotníctva zaznamenal výrazný nárast z 26 na 61 incidentov, čo odráža zvyšujúci sa záujem útočníkov o citlivé údaje a často slabšiu technickú pripravenosť zdravotníckych zariadení.

Energetika a digitálna infraštruktúra taktiež zaznamenali rast hlásených incidentov, čo môže byť reakcia na rastúce geopolitické napätie a rastúcu závislosť na digitálnych technológiách.

Pošta, elektronické komunikácie a doprava zostávajú stabilné alebo zaznamenali mierny nárast.

Tabuľka odhaľuje dôležité trendy a upozorňuje na potrebu ďalšieho posilňovania kybernetickej bezpečnosti, najmä v kľúčových sektoroch ako verejná správa, zdravotníctvo či energetika.



3. STAV KYBERNETICKEJ BEZPEČNOSTI

3. 1 CELKOVÝ POHĽAD

Na hodnotenie stavu kybernetickej bezpečnosti v SR za rok 2024 boli analyzované auditné správy jednotlivých prevádzkovateľov základných služieb, ktoré boli doručené NBÚ ako aj výstupy niektorých ústredných orgánov.

Celkový stav kybernetickej bezpečnosti sa v roku 2024 v jednotlivých sektoroch zlepšoval. Stále však pretrvávajú významné rozdiely medzi sektormi v prístupe ku kybernetickej bezpečnosti, ako aj v úrovni plnenia relevantných povinností a aplikovania bezpečnostných opatrení. Tieto rozdiely možno pozorovať v personálnej zložke, v procesoch a aj na technologickej úrovni. Kým v sektore bankovníctvo a elektronické komunikácia je úroveň kybernetickej bezpečnosti vysoká, verejná správa, zdravotníctvo a sektor voda a atmosféra stále výrazne zaostáva.

V sektore verejná správa síce dochádza, na úrovni niektorých prevádzkovateľov základných služieb, ku čiastkovým zlepšeniam, predovšetkým, v schopnosti identifikácie a hodnotenia zraniteľností (najmä vďaka projektu Achilles, ktorý prevádzkuje Ministerstvo investícií, regionálneho rozvoja a informatizácie SR) a detekcie kybernetických bezpečnostných incidentov. Stále však chýba koncepčný prístup v riadení kybernetickej bezpečnosti a systematickej aplikácii bezpečnostných opatrení v ich vzájomnej súvislosti a prepojení na reálne riziká. Nedostatočné sa javí aj efektívne riešenie a odstraňovanie už zistených zraniteľností. Niektoré kritické zraniteľnosti sú tolerované značne dlhú dobu, pričom riziko ich zneužitia útočníkmi v čase výrazne stúpa. Celkovo tento stav spôsobujú nielen chýbajúce stratégie a politiky kybernetickej bezpečnosti v rezortoch a u subjektov, absentujúce systematické riadenie rizík či jasné rozdelenie zodpovedností, ale aj nedostatok špecialistov kybernetickej bezpečnosti a systém financovania IT a kybernetickej bezpečnosti vo verejnej správe. Financovanie je vo všeobecnosti nedostatočné (investičný dlh), neefektívne a nevyvážené z hľadiska zdrojov (vlastné/ EÚ, prevádzkové/ kapitálové). Ide najmä o fenomén využívania financovania zo zdrojov EÚ cez rôzne projektové výzvy, ktoré je nárazové a často nezohľadňuje potreby, riziká alebo schodky subjektov v oblasti kybernetickej bezpečnosti. Je to tak najmä v prípade, ak financovanie cez projekty nie je vhodne dopĺňané vlastnými finančnými zdrojmi na ďalšie potreby mimo predmetu projektových výziev, napríklad na ľudské zdroje a prevádzku.

Ďalším sektorom, v ktorom je nevyhnutné zvýšiť úsilie a podporu v oblasti kybernetickej bezpečnosti je zdravotníctvo. V tomto sektore sú stále veľmi veľké rozdiely medzi jednotlivými prevádzkovateľmi z hľadiska úrovne ich kybernetickej bezpečnosti. Najmä štátom vlastnení najväčší poskytovatelia zdravotnej starostlivosti sústavne bojujú s problémami podfinancovania, ktoré sa prejavuje nedostatkom zdrojov v oblasti IT a digitalizácie, ako aj v oblasti kybernetickej bezpečnosti.

3. 2 AUDITY A SAMOHODNOTENIA

Auditom kybernetickej bezpečnosti sa overuje plnenie povinností podľa zákona o kybernetickej bezpečnosti, posúdenie zhody prijatých bezpečnostných opatrení s požiadavkami podľa tohto zákona a osobitných predpisov, ktoré sa vzťahujú na bezpečnosť sietí a informačných systémov prevádzkovateľa základnej služby pre jednotlivé siete a informačné systémy služby a pre prostriedky, ktoré podporujú služby. Cieľom auditu kybernetickej bezpečnosti je merať, zabezpečiť požadovanú úroveň kybernetickej bezpečnosti, predchádzať kybernetickým bezpečnostným incidentom a identifikovať nedostatky pri zabezpečovaní kybernetickej bezpečnosti prevádzkovateľom základnej služby. Cieľom je aj navrhnúť a prijať opatrenia na odstránenie týchto nedostatkov a napraviť existujúci stav.

V roku 2024 bolo Národnému bezpečnostnému úradu doručených 202 auditných správ.

Samohodnotenie, teda preverenie účinnosti prijatých bezpečnostných opatrení a plnenie zákonom ustanovených požiadaviek prostredníctvom manažéra kybernetickej bezpečnosti, prevádzkovatelia základnej služby, NBÚ v roku 2024 nevykonával. Vykonať samohodnotenie bolo možné do 31. decembra 2023.

K samotnému vyhodnocovaniu stavu kybernetickej bezpečnosti z auditných správ je ešte potrebné podotknúť, že tento prístup má limity. Jedným z nich je dvojročný cyklus povinných auditov. To znamená, že v danom kalendárnom roku doručí auditné správy iba časť subjektov, čo je v niektorých sektoroch pomerne málo. Prístup je nejednotný a často prináša nesystematicky štruktúrovaný obsah, ktorý nie je možné jednoducho porovnávať a spracúvať do agregovaných výstupov.

Práve rok 2024 je rokom, v ktorom povinnosť vykonať audit podľa §29 zákona o kybernetickej bezpečnosti v dvojročnom cykle pripadá na pomerne málo PZS. Z tohto dôvodu nízky počet auditov v niektorých sektoroch nie je vhodným predpokladom na detailnejšie vyhodnocovanie stavu kybernetickej bezpečnosti v danom sektore. Napríklad v sektore priemysel bola NBÚ doručená iba jedna správa z auditu. Vyhodnotenie stavu bezpečnosti v sektoroch, v ktorých bol vykonaný iba jeden audit, prípadne žiadny, nebolo možné, a preto nie je súčasťou tejto správy. Iba v sektore verejná správa bol doručený vyšší počet auditných správ (163), a preto iba v tomto sektore má detailnejší pohľad na auditné zistenia význam.

V budúcnosti bude potrebné rozvíjať aj iné spôsoby systematického zberu dát zo sektorov a od jednotlivých subjektov takým spôsobom, aby ich bolo možné jednoduchšie analyzovať z hľadiska ich výpovednej hodnoty (kvantitatívne a kvalitatívne ukazovateľa), agregovať a vizualizovať. Benefitom by mal byť nielen komplexnejší a objektívnejší pohľad na stav kybernetickej bezpečnosti a dynamiku vývoja, ale aj zmysluplné meradlo pre jednotlivé sektory a PZS.

3. 3 ŠTÁTNY DOHĽAD

Národný bezpečnostný úrad vykonal v roku 2024 celkovo kontrolu u 16 prevádzkovateľov základných služieb. Nedostatky zistil u 14 prevádzkovateľov základných služieb. Kontrolné skupiny v roku 2024 zaznamenali celkovo 117 kontrolných zistení v oblasti:

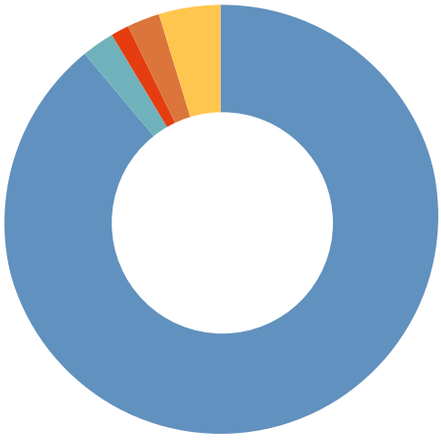
- riadenia kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahu s tretími stranami – **10 porušení**
- zaznamenávania udalostí a monitorovanie sietí a informačných systémov – **8 porušení**
- riadenia rizík – **19 porušení**
- riadenia aktív – **3 porušenia**
- identifikácie technických zraniteľností – **4 porušenia**
- riešenia kybernetických bezpečnostných incidentov – **17 porušení**
- klasifikácie informácií a kategorizácie sietí a informačných systémov – **3 porušenia**
- obsahu a štruktúry bezpečnostnej dokumentácie – **6 porušení**
- riadenia bezpečnosti prevádzky sietí a informačných systémov – **11 porušení**
- personálnej bezpečnosti – **2 porušenia**
- sieťovej a komunikačnej bezpečnosť – **6 porušení**
- riadenia prístupov osôb k sieti a informačnému systému – **10 porušení**
- určenia manažéra kybernetickej bezpečnosti – **2 porušenia**
- uzatvorenia zmluvy o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa zákona – **4 porušenia**
- nedodania auditu kybernetickej bezpečnosti – **3 porušenia**
- absencie stratégie kybernetickej bezpečnosti – **2 porušenia**

3. 4 SEKTOR BANKOVNÍCTVO

Národnému bezpečnostnému úradu bolo k 31. decembru 2024 doručených celkovo päť auditných správ zo sektora bankovníctvo. Na základe štatistiky súladu s auditnými požiadavkami je v sektore bankovníctvo priemerná percentuálna miera súladu nasledujúca:

VYHODNOTENIE SEKTORA BANKOVNÍCTVO

SÚLADY	89,05 %
ČIASTOČNÉ SÚLADY	2,46 %
NESÚLADY	1,42 %
NEAPLIKOVATEĽNÉ	2,53 %
OVERENÉ NA INOM MIESTE	4,47 %

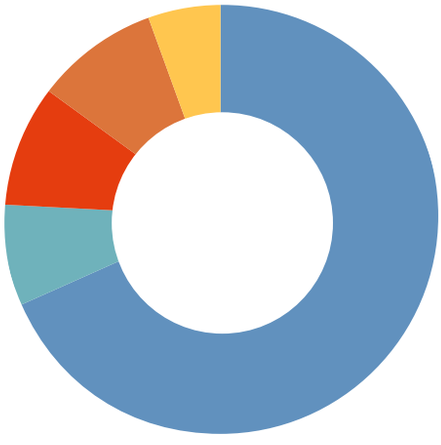


3. 5 SEKTOR DIGITÁLNA INFRAŠTRUKTÚRA

Národnému bezpečnostnému úradu boli k 31. decembru 2024 doručené celkovo štyri auditné správy zo sektora digitálna infraštruktúra. Na základe štatistiky súladu s auditnými požiadavkami je v sektore digitálna infraštruktúra priemerná percentuálna miera súladu nasledujúca:

VYHODNOTENIE SEKTORA DIGITÁLNA INFRAŠTRUKTÚRA

SÚLADY	64,46 %
ČIASTOČNÉ SÚLADY	7,07 %
NESÚLADY	8,52 %
NEAPLIKOVATEĽNÉ	8,88 %
OVERENÉ NA INOM MIESTE	5,17 %

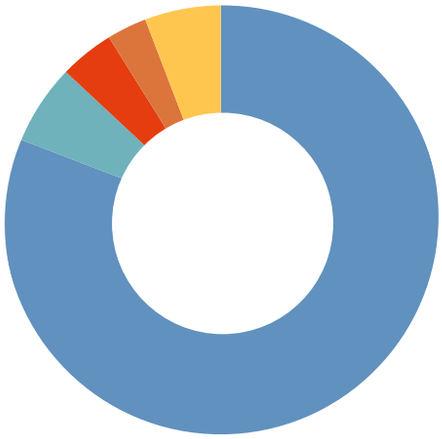


3. 6 SEKTOR ELEKTRONICKÉ KOMUNIKÁCIE

Národnému bezpečnostnému úradu boli k 31. decembru 2024 doručené celkovo tri auditné správy zo sektora elektronické komunikácie. Na základe štatistiky súladu s auditnými požiadavkami je v sektore elektronické komunikácie priemerná percentuálna miera súladu nasledujúca:

VYHODNOTENIE SEKTORA ELEKTRONICKÉ KOMUNIKÁCIE

SÚLADY	81,10 %
ČIASTOČNÉ SÚLADY	6,07 %
NESÚLADY	4,05 %
NEAPLIKOVATEĽNÉ	3,15 %
OVERENÉ NA INOM MIESTE	5,62 %

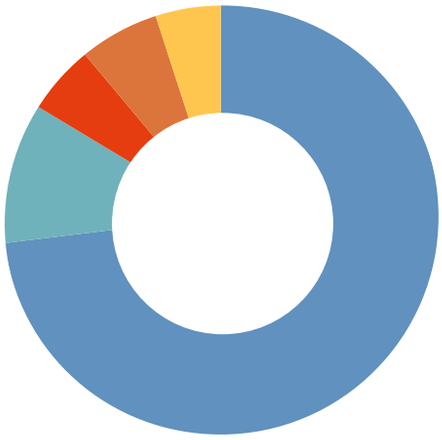


3. 7 SEKTOR ENERGETIKA

Národnému bezpečnostnému úradu bolo k 31. decembru 2024 doručených celkovo sedem auditných správ zo sektora energetika. Na základe štatistiky súladu s auditnými požiadavkami je v sektore energetika priemerná percentuálna miera súladu nasledujúca:

VYHODNOTENIE SEKTORA ENERGETIKA

SÚLADY	73,13 %
ČIASTOČNÉ SÚLADY	10,49 %
NESÚLADY	5,41 %
NEAPLIKOVATEĽNÉ	6,18 %
OVERENÉ NA INOM MIESTE	4,79 %

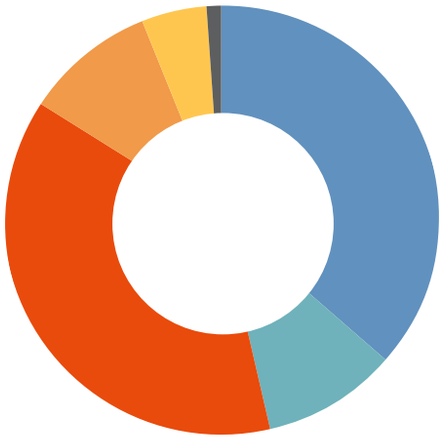


3. 8 SEKTOR VEREJNÁ SPRÁVA

Národnému bezpečnostnému úradu bolo k 31. decembru 2024 doručených celkovo 163 auditných správ zo sektora verejná správa. Na základe štatistiky súladu s auditnými požiadavkami je v sektore verejná správa priemerná percentuálna miera súladu nasledujúca:

VYHODNOTENIE SEKTORA ENERGETIKA

SÚLADY	37 %
ČIASTOČNÉ SÚLADY	10 %
NESÚLADY	38 %
NEAPLIKOVATEĽNÉ	10 %
OVERENÉ NA INOM MIESTE	5 %
NEVYHODNOTENÉ	1 %



Analýza správ z auditov v sektore verejná správa za rok 2024 ukázala, že u viacerých prevádzkovateľov základných služieb sa opakujú kľúčové nedostatky v riadení kybernetickej bezpečnosti. Ide najmä o tieto nedostatky:

- stratégia kybernetickej bezpečnosti s definíciou cieľov kybernetickej bezpečnosti nie je vypracovaná alebo nie je aktuálna,
- pravidlá a postupy pre klasifikáciu informácií a kategorizáciu informačného systému (IS) nie sú zavedené do praxe
- analýza rizík a analýza dopadov sa nevykonáva na pravidelnej báze, zavedené opatrenia nie sú naviazané na výsledky analýzy rizík
- riadenie dodávateľských služieb nie je komplexne zavedené, PZS nemajú uzavreté dodatky ku zmluvám, ktoré by odzrkadľovali povinnosti zákona kybernetickej bezpečnosti
- nie je definovaná a implementovaná politika riadenia prístupov a práv alebo nie je komplexne implementovaná
- pravidlá, postupy a zodpovednosti pre riadenie bezpečnosti IS a sietí nie sú formalizované
- nie sú zavedené postupy na akvizíciu, vývoj a údržbu IS a sietí
- systémy na detekciu zraniteľností nie sú zavedené komplexne a absentujú postupy na ich efektívne odstraňovanie alebo mitigáciu
- spôsobilosti na detekciu kybernetických bezpečnostných incidentov a reakciu na ne nie sú dostatočné
- postupy na riadenie kontinuity činností nie sú dostatočne zavedené a aktualizované

3. 9 SEKTOR VODA A ATMOSFÉRA

Národnému bezpečnostnému úradu boli k 31. decembru 2024 doručené celkovo tri auditné správy zo sektora voda a atmosféra. Na základe štatistiky súladu s auditnými požiadavkami je v sektore voda a atmosféra priemerná percentuálna miera súladu nasledujúca:

VYHODNOTENIE SEKTORA VODA A ATMOSFÉRA

SÚLADY	46,20 %
ČIASTOČNÉ SÚLADY	22,15 %
NESÚLADY	21,30 %
NEAPLIKOVATEĽNÉ	4,79 %
OVERENÉ NA INOM MIESTE	5,54 %

3. 10 SEKTOR ZDRAVOTNÍCTVO

Národnému bezpečnostnému úradu bolo k 31. decembru 2024 doručených celkovo 11 auditných správ zo sektora zdravotníctvo. Na základe štatistiky súladu s auditnými požiadavkami je v sektore zdravotníctvo priemerná percentuálna miera súladu nasledujúca:

VYHODNOTENIE SEKTORA ZDRAVOTNÍCTVO

SÚLADY	45,75 %
ČIASTOČNÉ SÚLADY	16,93 %
NESÚLADY	25,54 %
NEAPLIKOVATEĽNÉ	6,05 %
OVERENÉ NA INOM MIESTE	5,73 %

3. 11 HODNOTENIE STAVU KYBERNETICKEJ BEZPEČNOSTI ZO STRANY ÚSTREDNÝCH ORGÁNOV

3. 11. 1 Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky

Ako najzávažnejšiu hrozbu v sektore verejná správa Ministerstvo investícií a regionálneho rozvoja SR vyhodnotilo ransomvérové útoky, ktoré dokážu ochromiť celkový chod organizácií a za určitých podmienok znefunkčniť ich prevádzku na dlhú dobu. Vládna jednotka CSIRT (VJ CSIRT) riešila počas roku 2024 šesť ransomvérových incidentov. Medzi závažné hrozby patrí taktiež phishing, ktorý je úvodným vektorom útoku v 80 až 90 percentách prípadov.

V rámci proaktívnych činností VJ CSIRT využívala systém Achilles na vykonávanie pravidelného neinvazívneho skenovania a overovania zraniteľností v službách a zariadeniach IT infraštruktúr organizácií štátnej a verejnej správy, ktoré sú verejne dostupné z internetu. Služba zároveň monitoruje dostupnosť webových domén organizácií ITVS, uvedených v jej databáze. Túto situáciu má zlepšiť novela zákona o informačných technológiách vo verejnej správe, ktorá ukladá registráciu subjektu do Vládneho informačného systému kybernetickej bezpečnosti (VISKB) VJ CSIRT organizáciám v sektore ITVS ako povinnosť. Táto aktivita sa dotýka ústredných orgánov aj iných prevádzkovateľov základnej služby.

Zároveň prebieha finálna fáza na optimalizáciu monitoringu zapojených subjektov do SOC NASES a príprava na zapojenie niekoľkých ďalších subjektov v sektore verejnej správy.

V rámci prípravy novelizácie zákona o kybernetickej bezpečnosti, na základe smernice NIS2, boli vykonané konzultácie s inými ústrednými orgánmi štátnej správy. Konzultácie prebiehali medzi NBÚ, Ministerstvom vnútra SR a Ministerstvom investícií a regionálneho rozvoja SR.

V rámci sektora verejná správa boli počas minulého roka vykonávané aj preventívne aktivity v rámci osvetovej činnosti, zamerané hlavne na stredné školy, a taktiež aj na zamestnancov inštitúcií samosprávy. Osvetová činnosť bola zameraná na tému bezpečného pohybu v online priestore a na sociálnych sieťach. Celkovo bolo vyškolených cez 3-tisíc študentov stredných škôl a 780 zamestnancov inštitúcií verejnej správy.
Pre verejnú správu boli v roku 2024 realizované viaceré dopytové výzvy a projekty, do ktorých sa mohli zapojiť subjekty zo sektora, a tak zvýšiť úroveň svojej kybernetickej a informačnej bezpečnosti.

Ministerstvo tiež spustilo Centrálny portál kybernetickej bezpečnosti, ktorý subjektom verejnej správy poskytuje aktuálne metodiky, návody, vzory dokumentov, ako aj novinky v oblasti kybernetickej bezpečnosti s cieľom zvyšovania bezpečnostného povedomia a zručností. V roku 2024 ministerstvo vyškolilo v novozriadenom výcvikovom a školiacom stredisku (Kyberaréna) viac ako 100 odborníkov.

V rámci prevencie a dohľadu ministerstvo vykonávalo častejšie kontroly bezpečnostných opatrení v zmysle zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov a príslušnej vyhlášky č. 179/2020

Z. z. u subjektov verejnej správy, a tiež školenia k týmto kontrolám, čím sleduje zvýšenie súladu so zákonom u subjektov v sektore.

VJ CSIRT spolupracovala s viacerými sektorovými gestormi ako napríklad Ministerstvo vnútra SR a NBÚ. Významná je taktiež medzinárodná spolupráca v rámci „CSIRT network" po celom svete ako aj organizácie zastrešené v združeniach Trusted Introducer alebo First.org.

3. 11. 2 Ministerstvo vnútra Slovenskej republiky

Ministerstvo vnútra Slovenskej republiky, ako ústredný orgán za sektor verejná správa v podsektore bezpečnosť v roku 2024, zaregistrovalo mierne zvýšené aktivity, hrozby a nebezpečné činnosti v oblasti kybernetickej bezpečnosti zamerané na infraštruktúru a informačné systémy ministerstva v porovnaní s rokom 2023.

V roku 2024 ministerstvo nezaznamenalo vo svojej infraštruktúre žiaden kybernetický bezpečnostný incident, ktorý by bol klasifikovaný ako závažný. Ako ústredný orgán eviduje niekoľko potenciálnych pokusov o ohrozenie kritickej infraštruktúry v rámci rezortnej siete ministerstva, ktoré boli z hľadiska klasifikácie incidentov klasifikované ako DDoS (Distributed Denial of Service) útoky na internetové služby rezortu s cieľom narušenia ich dostupnosti. Celkovo sme zachytili deväť DDoS útokov cielených na služby ministerstva, čo reprezentuje pokles DDoS útokov o viac ako 50 % v porovnaní s rokom 2023. Pokles DDoS útokov na rezort je značne zapríčinený ich efektívnou mitigáciou na perimetri. Tieto útoky patria do kategórie menej významných incidentov, nakoľko vo väčšine prípadov nepredstavujú významný dopad na kybernetickú bezpečnosť.

Ministerstvo ďalej zaznamenalo prostredníctvom (interného) jednotného kontaktného miesta na nahlasovanie kybernetických bezpečnostných incidentov, ktoré sa týkajú infraštruktúry ministerstva alebo zamestnancov ministerstva, 1756 hlásení s podozrením na kybernetický incident. Išlo predovšetkým o aktivity metódou sociálneho inžinierstva, kde vo väčšine prevládali phishingové útoky s cieľom kompromitácie používateľských účtov, ďalej podvodné e-maily a spear-phishingové útoky. Kvalita týchto útokov exponenciálne rastie s vývojom a používaním umelej inteligencie pre potreby sociálneho inžinierstva.

Ministerstvo ako prevádzkovateľ základných služieb vykonalo v roku 2024 audit kybernetickej bezpečnosti u šiestich základných služieb na zaistenie zvýšenia miery súladu s požiadavkami zákona o kybernetickej bezpečnosti.

Ministerstvo sa v rámci svojej činnosti podieľalo aj na riešení rôznorodých protiprávnych konaní a iných nežiaducich aktivít, avšak za najzávažnejšie možno považovať kampane zamerané na problematiku rozposielania výhražných e-mailových správ rôznym entitám štátnej, ale aj komerčnej štruktúry v rámci SR. Závažnými boli však aj konania rôznych zahraničných organizovaných skupín zameraných podvodné konania, ktorých cieľom sú finančné prostriedky a platobné služby občanov SR. Rozsah a forma týchto konaní sa menia a vyvíjajú v závislosti od intenzity využívania platobných platforiem a nástrojov či popularity určitých kryptoaktív.

Odbor počítačovej kriminality vykonával najmä aktivity spojené s represívnym konaním Policajného zboru (PZ) SR, keďže odbor kybernetickej počítačovej kriminality v prevažnej väčšine vykonáva praktickú a metodickú pomoc útvarom štruktúr PZ. V rámci

aktivít zameraných na kybernetickú bezpečnosť išlo spravidla o preventívne aktivity formátu upozornení o výskyte rôznych podvodných konaní súvisiacich s využívaním informačných technológií.

V prípade potreby, v rámci špecifických, či obzvlášť závažných prípadov odbor spolupracuje so všetkými súčasťami štátnych, ale aj komerčných štruktúr zapojených do kybernetickej bezpečnosti, či všeobecnej bezpečnosti krajiny. V prípadoch, pri ktorých si to vyžaduje povaha či rozsah, odbor spolupracuje takisto s inštitúciami pôsobiacimi na území iných európskych krajín.

Súčasťou správy nie sú štatistické údaje týkajúce sa jednotlivých druhov počítačovej kriminality alebo kriminality páchanej prostredníctvom počítačov z dôvodu, že prebieha zmena metodiky vykazovania uvedených údajov.

3. 11. 3 Ministerstvo obrany Slovenskej republiky

Vojenské spravodajstvo (VS) sa v priebehu roka 2024 podieľalo na riešení 237 počítačových bezpečnostných incidentov rôznej úrovne závažnosti. VS vyhodnotilo za najzávažnejšie aktivity pokročilých zahraničných štátmi podporovaných aktérov, tzv. APT skupín, s potenciálnym dopadom na obranu Slovenskej republiky.

Zaznamenaný bol zvýšený záujem APT skupín spájaných s Ruskou federáciou o kritickú infraštruktúru v sektoroch energetiky a dopravy SR. Predmetom záujmu týchto skupín boli najmä subjekty pôsobiace v oblasti železničnej dopravy a prenosu energetických surovín. VS v danom roku analyzovalo aj phishingovú kampaň priamo smerovanú voči príslušníkom rezortu obrany. Nástroje vyžité útočníkmi v rámci predmetnej phishingovej kampane boli atribuované APT skupine verejne spájanej s vládou Iránu. Iné APT skupiny, odbornou komunitou atribuované s vládou Čínskej ľudovej republiky, zamerali svoju pozornosť na platformu verejného a súkromného sektora.

VS vykonávalo konzultácie a aktivity s cieľom identifikovať zraniteľné miesta v informačnej a komunikačnej infraštruktúre organizácií rezortu obrany. Na základe jednotlivých žiadostí realizovalo penetračné testovania viacerých systémov zložiek rezortu obrany a pravidelné skenovanie informačnej a komunikačnej infraštruktúry viacerých organizácií spadajúcich pod rezort obrany, ako aj iných orgánov ústrednej štátnej správy. Aktívne sa podieľalo najmä na zvyšovaní bezpečnostného povedomia a odbornej kvalifikácie príslušníkov a zamestnancov rezortu obrany a ústrednej štátnej správy a opakovane realizovalo školenia v oblasti kybernetickej obrany a bezpečnosti.

Osobitnú formu medzinárodnej spolupráce pre VS predstavujú cvičenia kybernetickej obrany. VS sa zapojilo do viacerých cvičení v oblasti kybernetickej obrany a kybernetickej bezpečnosti organizovaných pod záštitou NATO Communications and Information Agency, NATO CCDCOE a EDA, a to CROSSED SWORDS 2024, CYBER COALITION 2024, EDA milCERT exercise 2024, NATO Crisis Management Exercise 2024 a národných veliteľstiev – štábnych cvičení zameraných na preverenie obrany štátu v kybernetickom priestore. Medzi najvýznamnejšie patrí cvičenie Locked Shields 2024, kde SR obsadila celkovo 4. miesto spomedzi 24 zúčastnených tímov z približne 30 krajín NATO a EÚ. Spojený tím, ktorý tvorili zástupcovia Slovenskej republiky a Maďarska, svojim umiestnením opätovne potvrdil pripravenosť a preukázal kľúčové spôsobilosti SR v oblasti kybernetickej obrany.

4. Aktivity a opatrenia úradu

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 zostáva 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.

4. 1 NÁRODNÁ LEGISLATÍVA

Národný bezpečnostný úrad systematicky zbiera, analyzuje a vyhodnocuje informácie z činnosti útvarov úradu, zo spätnej väzby odbornej verejnosti, zo žiadostí o poskytnutie odborného stanoviska či iných podnetov orgánov verejnej moci, právnických osôb a fyzických osôb. V oblasti medzinárodného práva úrad harmonizuje národnú právnu úpravu s medzinárodne uznávanými prameňmi práva.

S cieľom transponovať smernicu Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS2) do právneho poriadku SR, úrad pripravil návrh zákona, ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony (ďalej len „návrh zákona“).

Príprave návrhu zákona predchádzalo organizovanie odborných aktivít – workshopov, konferencií, stretnutí pracovných skupín, konzultácií s akademickou obcou i odbornou verejnosťou na národnej aj medzinárodnej úrovni. Novelou zákona sa precizuje hlásenie incidentov a hlásenie zraniteľností, zavádza sa minimálna úroveň bezpečnostných opatrení, posilňuje sa dohľadová činnosť, podporuje sa vzdelávanie, dopĺňa sa zodpovednosť a posilňuje sa funkcia manažéra kybernetickej bezpečnosti.

Verejnosť sa do prípravy návrhu zákona mohla zapojiť zaslaním podnetov a návrhov v rámci zverejnenej predbežnej informácie - PI/2024/82 - od 10. apríla 2024 do 16. apríla 2024. Vyjadrenia zaslané v rámci predbežnej informácie boli predmetom konzultácií, ktoré úrad organizoval s cieľom optimálneho zapracovania vznesených podnetov do návrhu zákona.

Vypracovaný návrh zákona úrad predložil do medzirezortného pripomienkového konania, t. j. zverejnil materiál prostredníctvom právneho a informačného portálu Slov-Lex (legislatívny proces LP/2024/264) v období od 30. mája 2024 do 19. júna 2024. V uvedenom období mohli príslušné subjekty a aj verejnosť uplatňovať pripomienky. Legislatívny proces pokračoval vyhodnotením a vysporiadaním vznesených pripomienok.

Návrh zákona bol 24. septembra 2024 prerokovaný v Legislatívnej rade vlády Slovenskej republiky a následne po zapracovaní pripomienok bol predložený na rokovanie vlády Slovenskej republiky. Vláda Slovenskej republiky schválila návrh zákona uznesením č. 567/2024 z 2. októbra 2024 na svojom 52. rokovaní. Legislatívny proces pokračoval predložením návrhu zákona Národnej rade Slovenskej republiky 4. októbra 2024. V Národnej rade Slovenskej republiky bol návrh zákona schválený 28. novembra 2024 (za hlasovalo 117 poslancov zo 140 prítomných poslancov) a zákon prezident Slovenskej republiky 13. decembra 2024. V Zbierke zákonov Slovenskej republiky bol zákon publikovaný 19. decembra 2024 (zákon č. 366/2024 Z. z.) a nadobudol účinnosť 1. januára 2025.

Na zabezpečenie ochrany, odolnosti a posilnenie bezpečnosti subjektov ponúkajúcich služby v dôležitých sektoroch členských štátov Európskej únie okrem smernice NIS 2 boli prijaté aj nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene a nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011 a smernica Európskeho parlamentu a Rady (EÚ) 2022/2557 zo 14. decembra 2022 o odolnosti kritických subjektov a o zrušení smernice Rady 2008/114/ES.

S cieľom zosúladiť národný právny rámec v oblasti kybernetickej bezpečnosti úrad v rámci harmonizácie s právom EÚ aktívne participoval na implementácii a transpozícii predmetných právnych predpisov.

4. 2 EURÓPSKA ÚNIA

V oblasti kybernetickej bezpečnosti sa rok 2024 vyznačoval najmä dokončovaním legislatívnej činnosti v spojitosti s očakávaným ukončením legislatívneho cyklu v Európskom parlamente ako aj príchodom nového Kolégia komisárov Európskej komisie. Počas belgického predsedníctva sa dokončila politická diskusia k návrhu Nariadenia o riadených bezpečnostných službách (CSA+), ktoré tvorilo súčasť kybernetického balíčka predstaveného Európskou komisiou v apríli 2023. Z dôvodu administratívnych komplikácií a nedostatku kapacít prekladateľov sa nakoniec CSA+ ako aj druhý návrh tohto balíčka - Nariadenie k opatreniam na posilnenie solidarity a kapacít v Únii na odhaľovanie kybernetických hrozieb a incidentov, prípravu a reakciu na ne (CySOLa) dostali do procedúry korigenda, čoho dôsledkom bolo záverečné schvaľovanie až v novom Európskom parlamente a Rade Európskej únie počas maďarského predsedníctva. Tieto akty Európskej únie tak boli publikované vo Vestníku Európskej únie až začiatkom roka 2025. Do procedúry korigenda sa dostal aj návrh Nariadenia o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami (CRA), pričom bol podobne formálne uzatvorený na jeseň 2024. Vo Vestníku Európskej únie bol publikovaný v októbri 2024.

Slovensko, prostredníctvom zastúpenia príslušníkmi NBÚ, ciele väčšiny zmieňovaných právnych predpisov počas celého roka 2024 aktívne podporovalo, pričom počas ich negociácií zasielalo množstvo pripomienok a komentárov, ktoré boli pozitívne prijaté a slúžili na zefektívnenie a racionalizáciu prerokovávaných právnych noriem. Schválením uvedených právnych predpisov sa posilní úroveň kybernetickej bezpečnosti v Európskej únii, zvýši sa spotrebiteľská ochrana pri kúpe a využívaní rozličných softvérových a hardvérových produktov s digitálnymi prvkami a taktiež sa vytvorí predpoklad pre celounijné overovanie identity občanov, harmonizuje sa a zjednoduší sa systém certifikácie v oblasti kybernetickej bezpečnosti. Slovensko sa však zdržalo pri hlasovaní o návrhu CSA+, ktorý považuje za duplicitný k existujúcej právnej úprave.

Na úrovni komitologických výborov v zmysle už prijatej sekundárnej legislatívy Európskej únie, najmä revidovanej Smernice o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii (NIS2), Aktu o kybernetickej bezpečnosti

(CSA), či inej relevantnej legislatívy sa úrad zúčastňoval diskusií o implementácii jednotlivých opatrení. Po odbornej diskusii s členskými štátmi Európska komisia v októbri 2024 prijala prvé vykonávacie pravidlá o kybernetickej bezpečnosti kritických subjektov a sietí v zmysle smernice NIS2, ktoré sú výsledkom práce komitologického výboru Európskej komisie. Tento vykonávací akt podrobne uvádza opatrenia na riadenie rizík v oblasti kybernetickej bezpečnosti, ako aj prípady, pri ktorých by sa incident mal považovať za závažný, pričom spoločnosti zabezpečujúce digitálnu infraštruktúru a služby by ho mali nahlásiť vnútroštátnym orgánom.

V rámci aktivít v komitologických výboroch si osobitnú pozornosť zaslúžila aj príprava kandidátskych schém kybernetickej bezpečnosti EUCC (spoločné kritériá) a EUCS (cloudové schémy), z ktorých sa v priebehu roka 2024 práve EUCC dostalo do praxe. Príprava EUCS sa z politických dôvodov dočasne pozastavila.

Horizontálna pracovná skupina pre kybernetické záležitosti (HWPCI) v rámci svojich nelegislatívnych aktivít venovala svoju pozornosť aj ostatným strategickým prvkom oblasti kybernetickej diplomacie. V oblasti kybernetickej diplomacie, ktorá obsahovo presahuje do domén Spoločnej zahraničnej a bezpečnostnej politiky Európskej únie (EEAS) a Spoločnej bezpečnostnej a obrannej politiky Európskej únie (SBOP), sa aktivity Slovenska a ostatných členských štátov sústredili prevažne na koordináciu spoločných pozícií únie pre rokovania Pracovnej skupiny s otvoreným koncom (OEWG) pre bezpečnosť a využívanie informačných a komunikačných technológií pri OSN, či na diskusie ku Globálnemu digitálnemu paktu (GDC) a tiež k novému Dohovoru o boji proti počítačovej kriminalite.

Slovensko sa tiež zapojilo do kybernetických dialógov s tretími partnerskými krajinami, osobitne s USA, Veľkou Britániou, či Japonskom a zúčastnilo sa cvičenia aplikácie Súboru nástrojov kybernetickej diplomacie v praxi. V kontexte vyhodnocovania neustálych kybernetických hrozieb Slovensko spolupracovalo s ostatnými členskými štátmi, EEAS (INTCEN), agentúrou ENISA, či CERT-EU a zúčastnilo sa prípravy nových sankčných kybernetických zoznamov pre dotknuté fyzické osoby. Aktívne sa tiež zapojilo do procesu prípravy strategického materiálu k zaujatiu pozície Únie voči pokročilým aktérom hrozieb ako aj strategického materiálu ohľadom pozície Európskej únie v oblasti kybernetickej bezpečnosti v krajinách západného Balkánu.

Okrem toho sa v roku 2024 úrad aktívne zúčastňoval aj na zasadnutiach Skupiny pre spoluprácu – k transpozícii smernice NIS (NIS Cooperation Group) a v jej podksupinách pri oblastiach Work Stream Post-Quantum Cryptography (PQC), Work Stream on Election (volebné procesy), Work Stream on Health (zdravotníctvo) a Working Group on Aviation (letecká doprava). Stretnutia NIS Cooperation Group sú organizované na základe smernice NIS, ktorá stanovuje opatrenia na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Európskej únii a zavádza rámec pre spoluprácu medzi členskými štátmi v oblasti kybernetickej bezpečnosti. Cieľom Skupiny pre spoluprácu je dosahovať vysokú spoločnú úroveň bezpečnosti pre sieťové a informačné systémy v Únii, podporovať a uľahčovať strategickú spoluprácu a výmenu informácií medzi členskými štátmi najmä pokiaľ ide o zdieľanie poznatkov aplikačnej praxe a najlepších postupov. Práce v skupine boli počas roka zamerané na aktualizáciu procesov súvisiacich s implementáciu smernice NIS2, rovnako prípravou príručiek, usmernení a ďalších dokumentov súvisiacich s týmito procesmi.

Zástupcovia NCKB boli na úrovni Únie súčasťou viacerých pracovných skupín a iniciatív zameraných na budovanie spoločného rámca kybernetickej bezpečnosti. Medzi najvýznamnejšie aktivity patrí účasť v Európskej sieti styčných organizácií pre kybernetické krízy CyCLONe, sieti zástupcov členských štátov na zvládanie kybernetických kríz. V rámci stretnutí prebieha strategická diskusia zameraná na efektívne zdieľanie informácií

o kybernetickej bezpečnosti. Spolupráca podporuje výmenu dôležitých informácií v kybernetickom priestore. Stretnutia CyCLONu mali za cieľ v roku 2024 vylepšovanie a overovanie postupov pri riešení závažných incidentov s cezhraničným presahom a v rámci stretnutí prebehlo aj cvičenie Cyber Europe 2024, prostredníctvom simulácie eskalácie rozsiahleho kybernetického bezpečnostného incidentu so zameraním na energetický sektor. Cieľom cvičenia bolo zabezpečenie primeranosti a zlepšenia procesov operačných postupov, internej spolupráce, určenie jasného interného komunikačného kanálu, zlepšenie reakcie na vzťahy s verejnosťou počas kríz v oblasti kybernetickej bezpečnosti a preverenie schopnosti riešiť tieto krízy.

NCKB (organizačná zložka SK-CERT – národná jednotka CSIRT) aktívne pôsobil aj v rámci medzinárodných organizácií, združujúcich jednotky CSIRT. V rámci CSIRT Network, ktorý združuje národné CSIRT jednotky členských štátov EÚ, si SK-CERT s ostatnými členskými štátmi vymieňal operatívne informácie o hrozbách a incidentoch. Keďže vojenská situácia na východe Európy sa nezmenila, jednotlivé štáty si vymieňali informácie a skúsenosti s incidentami a útokmi, ktoré súviseli s vojnou na Ukrajine a poskytovali si vzájomnú pomoc podľa potreby. SK-CERT si v rámci CSIRT Network v roku 2024 udržal najvyšší status vyspelosti CSIRT jednotky „Advanced“, ktorý sa udeľuje po tzv. peer-review procese, v ktorom jedna CSIRT jednotka hodnotí vyspelosť inej CSIRT jednotky podľa nastavenej objektívnej metodiky.

Organizácia pre bezpečnosť a spoluprácu v Európe (OBSE)Zorganizované stretnutia účastníckych štátov Organizácie pre bezpečnosť a spoluprácu v Európe (OBSE), na ktorých mal aktívne zastúpenie v roku 2024 aj úrad, podčiarkli dôležitosť medzinárodnej spolupráce v oblasti kybernetickej bezpečnosti a zdieľania informácií o existujúcich a potenciálnych hrozbách. Napriek vysokému zastúpeniu účastníckych štátov OBSE boli však zasadnutia aj naďalej ovplyvnené geopolitickou situáciou, najmä prebiehajúcou vojnou Ruska proti Ukrajine, čo následne vplývalo aj na priebeh rokovaní o prevažne nesenzitívnych témach, ako je bezpečnosť informačných a komunikačných technológií.

4. 3 NATO

Počas roka 2024 sa uskutočnili rokovania Bezpečnostného výboru NATO (SC), ktoré prebehli vo všetkých svojich formátoch – vo formáte bezpečnostných politík, bezpečnosti komunikačných a informačných systémov (CISS) a na najvyššej úrovni – úroveň riaditeľov bezpečnostných úradov členských štátov. Predsedajúcim výboru bol riaditeľ Bezpečnostného úradu NATO (NOS) Galen Nace, ktorý diskutoval s predstaviteľmi bezpečnostných autorít o rôznych bezpečnostných témach, a to nielen v kontexte súčasnej geopolitickej situácie. Počas jarného zasadnutia SC mali zástupcovia národných bezpečnostných úradov možnosť navštíviť Akcelerátor obranných inovácií NATO - DIANA (Defence Innovation Accelerator for NATO), ktorý využíva svoj program a sieť testovacích centier na to, aby spojil start-up s operačnými koncovými používateľmi, vedcami a systémovými integrátormi s cieľom podporiť presvedčivé špičkové technológie s riešeniami s dvojakým použitím pre Alianciu.

Za hlavný míľnik v oblasti kybernetickej bezpečnosti/obrany NATO v 2024 určite možno považovať júlový varšavský summit, počas ktorého došlo k schváleniu dvoch zásadných dokumentov, ktoré jednoznačne prispejú do budovania a upevňovania celkovej zostavy odstrašovania a obrany NATO.

- Príručka strategických opatrení reakcií na závažné škodlivé kybernetické aktivity a kampane, ktorá umožní posilnenie integrovaného situačného povedomia, celkovej odolnosti NATO a podporí proces kolektívnej akcie.

- Zriadenie NATO Integrated Cyber Defence Centre (NICC), ktoré posilní schopnosť Aliancie chrániť svoje komunikačno-informačné systémy, ako aj vnímanie kyberpriestoru ako operačnej domény v rámci multidoménových operácií. Preto 2025 bude rokom implementovania politicko-vojenských odporúčaní tak, aby NICC mohlo byť plne funkčné na jeseň 2026.

Ďalšou udalosťou roka NATO bola konferencia Cyber Defence Pledge, ktorá sa uskutočnila v máji v Haagu. Veľvyslanci sa tak po ročnej prestávke, ktorá bola zameraná na efektívne úpravu dotazníka reflektujúceho na rýchlo sa meniaci kyberpriestor, zhodnotiť dosiahnutý pokrok v oblasti kybernetickej bezpečnosti/obrany Aliancie. Členské štáty tak po prvýkrát na základe samohodnotenia pri vyplňovaní dotazníka (od roku 2016) mohli kvantitatívne merať dosiahnutie pokroku. Tieto merateľné ukazovatele tak uľahčia porovnávanie dosiahnutie úrovne kybernetickej bezpečnosti u daného spojenca nielen naprieč rokmi, ale aj naprieč porovnávaniami s ostatnými spojencami, prípadne partnermi.

Druhá výročná konferencia o kybernetickej obrane NATO bola ďalšou dôležitou udalosťou roka, a to nielen v oblasti kybernetickej obrany. Konferencia sa uskutočnila v novembri v Londýne a prepojila všetky zainteresované strany na všetkých troch úrovniach (politickej, technickej a vojenskej) nielen v rámci štruktúr NATO ale aj u 32 spojencov. Slovensko bolo zastúpené predstaviteľmi úradu a Centra kybernetickej obrany.

4. 4 REGIONÁLNA SPOLUPRÁCA

Na základe rotácie predsedníctva krajín, ktoré sú členmi Stredoeurópskej platformy pre kybernetickú bezpečnosť (CECSP), Úrad rakúskeho spolkového kancelára v roku 2024 predsedal tejto platforme. Zástupcovia úradu sa aktívne zúčastnili na rokovaniach platformy spolu s ďalšími kolegami zastúpenými krajinami Vyšehradskej štvorky (Česká republika, Maďarsko, Poľsko) a Rakúsko. Predmetom samotných rokovaní boli aktuálne témy, ktoré na úrovni Európskej únie rezonovali počas celého roka 2024 a súčasne partneri sa v rámci týchto tém snažili nájsť spoločné prieniky a vzájomnú podporu. Zároveň rakúske predsedníctvo sa pustilo do „veľkého upratovania“ zakladajúcich dokumentov „Central European Cyber Security Platform – Declaration“ a „Working program for European Central Security Platform“. Medzi tie najdôležitejšie témy stretnutia patrili: „Aktuálny stav procesu transpozície smernice NIS 2.0 v jednotlivých členských štátoch.“; „Kybernetická bezpečnosť a kyberdiplomacia“, „Certifikácia kybernetickej bezpečnosti – nové prístupy“ a „Nariadenie CRA“.

V procese aproximácie smernice NIS 2 je najďalej práve Slovenská republika. Experti sa zhodli, že pri aproximácii sa vyžaduje adaptívny, koordinovaný a inovatívny prístup, ktorým sa dosiahne najširšia harmonizáciou naprieč celou úniou.

V rámci témy budovania kapacít zúčastnení prezentovali národné prístupy a know-how ako dosahovať stanovené ciele. Slovinsko sa zúčastnilo rokovaní už druhýkrát a práve zmenou statusových dokumentov začne cestu riadneho člena voči čomu nemajú zakladajúce krajiny žiadne výhrady a na princípe rozvoja spolupráce krajín strednej Európy v oblasti kybernetickej bezpečnosti členstvo Slovinska schvaľujú.

4. 5 BILATERÁLNE VZŤAHY

Príslušníci aktívne rozvíjali bilaterálne vzťahy naprieč všetkými pracovnými platformami a formátmi, či už pri osobnom kontakte počas zasadnutia pracovných skupín, alebo pri ad hoc plnení úloh práve na bilaterálnej úrovni.

Za hlavnú udalosť roka z pohľadu úradu možno považovať prijatie riaditeľa NATO Office of Security Galena Nacea (NOS NATO) na pôde NBÚ v septembri 2024. Počas stretnutia s riaditeľom a námestníčkou úradu sa riaditeľ NOS NATO zaujímal aj o úrad ako gestora tém kybernetickej bezpečnosti. Cieľom rokovaní bolo posilniť spoluprácu medzi Slovenskou republikou a NATO aj v oblasti predchádzania kybernetickým incidentom a hrozbám.

V nadväznosti na podpísanie memoranda o spolupráci v oblasti kybernetickej bezpečnosti s Kenskou republikou v prvej polovici roka 2024 a v záujme ďalšieho prehlbovania rozvojovej spolupráce zástupcovia úradu opäť navštívili Kenskú republiku v októbri 2024. Návšteva jednoznačne zvýraznila vzájomné snahy o výmenu skúseností a poznatkov v oblasti kybernetickej bezpečnosti a kybernetickej diplomacie. Kenská strana prejavila záujem o účasť na projekte CyberGame 2025. V tomto prípade sa realizujú ďalšie konzultácie a podpora zo strany NBÚ.

Okrem uvedených prijatí a zaužívaných bilaterálnych spoluprác prejavili záujem o nadviazanie spolupráce alebo o informácie týkajúce sa agendy kybernetickej bezpečnosti prostredníctvom krátkych návštev a stretnutí aj predstavitelia Španielskeho kráľovstva v zastúpení Instituto nacional de ciberseguridad (INCIBE). Prijatie sa uskutočnilo v apríli 2024 na základe prejaveného záujmu španielskej strany ohľadom tém ako transpozícia smernice NIS2 a nariadenia CRA vrátane aplikačnej praxe na Slovensku, európskej certifikačnej schémy a fungovania národných kompetenčných centier. Španielska strana predstavila svoju víziu budúcej spolupráce v daných oblastiach.

Príslušníci úradu a zástupcovia NCKB v rámci bilaterálnych vzťahov pravidelne komunikovali a vymieňali si informácie o aktuálnych právnych predpisoch na národnej úrovni, zraniteľnostiach, hrozbách a incidentoch a vymieňali si informácie o osvedčených postupoch a o dobrej praxi so svojimi zahraničnými partnermi aj mimo EÚ a zúčastňovali sa rôznych medzinárodných cvičení kybernetickej bezpečnosti. Takisto sa po vecnej stránke zástupcovia úradu a zástupcovia NCKB zúčastňovali bilaterálnych rokovaní a zahraničných prijatí zastrešovaných práve odborom medzinárodných vzťahov a bezpečnostných politík sekcie regulácie a dohľadu.

V roku 2024 úrad rozvinul aktívnu spoluprácu s partnerskou inštitúciou vo Francúzsku, l´Agence nationale de la sécurité des systèmes d´information (ANSSI). Tá je dôležitá nielen kvôli intenzívnej spolupráci pre oblasť európskej certifikačnej schémy pre cloudové služby, ale aj kvôli zdieľaniu analýz a správ o stave hrozieb vo Francúzskej republike (Olympijské hry, voľby do Európskeho parlamentu, potencionálne hrozby a incidenty...).

Spolupráca v oblasti kybernetickej bezpečnosti jadrových zariadení, ktorých súčasťou boli školenia o kybernetickej bezpečnosti, najmä v oblasti fyzickej bezpečnosti a dodávateľských vzťahov, prebieha medzi Medzinárodnej agentúry pre atómovú energiu (MAAE), Úradu jadrového dozoru SR a partnerskými organizáciami v Spojených štátoch amerických, The Office of International Nuclear Security (INS) a United States Department of Energy National Nuclear Security Administration (NNSA/DOE)

4. 6 VYDÁVANIE VAROVANÍ A BULLETINOV

NCKB vydávalo bezpečnostné varovania pred zraniteľnosťami a hrozbami. Bolo vydaných 51 súhrnných bezpečnostných bulletinov a 701 bezpečnostných varovaní.

Súhrnne upozornilo NCKB na 1493 zraniteľností a hrozieb.

BEZPEČNOSTNÉ BULLETINY A VAROVANIA

	JAN	FEB	MAR	APR	MÁJ	JÚN	JÚL	AUG	SEP	OKT	NOV	DEC
BULLETINY	4	3	4	5	4	4	5	4	4	5	4	5
VAROVANIA	53	46	53	58	50	67	57	55	80	69	65	48
CELKOM ZRANITEĽNOSTÍ	101	79	131	149	97	129	134	139	130	157	135	112

4. 7 CYBERGAME

V treťom ročníku národnej kyberbezpečnostnej súťaže CyberGame sa registrovalo vyše dvetisíc tristo účastníkov. Počas desiatich týždňov riešili úlohy rôzneho zamerania, ktoré pripravilo NCKB.

V roku 2024 obsahovala súťaž tri analytické vetvy – malvérovú, forenznú a OSINT analýzu. Ďalšia hracia vetva bola venovaná kryptografii a tá netechnická mala názov procesy a riadenie bezpečnosti. Novinkou bola ofenzívna bezpečnosť.

CyberGame predstavuje atraktívny a netradičný spôsob, ako hľadať a nadchnúť profesionálov pre kybernetickú bezpečnosť. V súťaži bodovalo 874 hráčov a hráčok, počínajúc prvákmi na strednej škole a končiac skúsenými programátormi. Každý dostal šancu, takže ocenenie bolo udelené absolútnemu víťazovi, najlepšiemu študentovi, najlepšej hráčke a organizátori odmenili aj najmladšieho účastníka, expertov vo vetvách, najlepšieho hráča z verejnej správy a učiteľa.

4. 8 ŠÍRENIE POVEDOMIA PRE ŠIROKÚ VEREJNOSŤ

Národný bezpečnostný úrad vypracoval v roku 2024 informačné kampane na šírenie povedomia o kybernetickej bezpečnosti. Zamerané boli na phishingové hrozby, ale aj hrozby, s ktorými sa môžu ľudia stretnúť počas dovoleniek. NBÚ šíril aj tipy pre rodičov, ktorí chcú, aby boli ich deti na internete v bezpečí. Odbor komunikácie v spolupráci s ďalšími rezortmi upozorňoval laickú verejnosť na podvody šíriace sa e-mailovou komunikáciou, ale aj SMS správami či telefonátmi. Cieľom aktivít bolo zvýšiť povedomie o hrozbách a varovať ľudí pred taktikami podvodníkov. Odbor sa na svojich sociálnych sieťach venoval aj téme kybernásilia páchaného na ženách.

Príslušníci úradu vyučovali v akademickom roku 2023/2024 aj predmet Bezpečnosť a práca novinára v online priestore na Katedre žurnalistiky Univerzity Komenského v Bratislave. Budúcim novinárom prezentovali zásady kybernetickej hygieny, ochranu dát, súkromia aj komunikácie či prácu s otvorenými zdrojmi.

Pozvanie dostali aj na základnú školu v obci Kriváň. Príslušníci úradu sa so žiakmi rozprávali o telefonických či textových podvodoch. Úrad tak nadviazal na obdobné aktivity z predošlých rokov.

4. 9 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 KCCKB manažovať európske finančné fondy pre kybernetickú bezpečnosť z priamo riadených programov EÚ.

V roku 2024 KCCKB uzavrelo grantovú dohodu s Európskou komisiou na nový projekt NCC na roky 2025-2028.

V rámci aktivít Národného koordinačného centra bola v roku 2024 vyhlásená výzva FSTP -Kaskádové financovanie ako súčasť NCC projektu z RRF, ktorej cieľom je významne prispieť k získaniu finančných zdrojov na zabezpečenie svojich kyberbezpečnostných potrieb. Do výzvy sa úspešne prihlásilo 46 subjektov so svojimi projektmi.

Súčasťou cieľov KCCKB v roku 2024 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 prostredníctvom NCC-SK stalo 162 slovenských subjektov.

Od 1. januára 2024 je na základe súhlasu Národného bezpečnostného úradu v zmysle § 59 zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov je KCCKB autorizované na:

- posudzovanie bezpečnostného projektu technického prostriedku podľa § 56 ods. 2 Zákona
- overovanie zhody vlastností technického prostriedku s požiadavkami bezpečnosti a schvaľovanie použitia technických prostriedkov podľa § 2 a § 5 vyhlášky č. 339/2004 Z. z. o bezpečnosti technických prostriedkov

O posudzovanie technických prostriedkov proti úniku utajovaných skutočností nežiaducim elektromagnetickým vyžarovaním (NEV) žiada výrobca, splnomocnený zástupca výrobcu, dovozca, distribútor, alebo užívateľ. V roku 2024 bolo vykonané meranie u viac ako 40 subjektov.

V rámci expertných činností vykonalo KCCKB 47 auditov kybernetickej bezpečnosti.

Počet certifikovaných osôb sa prostredníctvom KCCKB v roku 2024 navýšil o 14 certifikovaných audítorov a 37 certifikovaných manažérov.

KCCKB bolo úspešné aj v oblasti vzdelávania dospelých. Vydaná bola aktualizovaná vzdelávacia schéma. Do portfólia vzdelávania pribudol nový špecializovaný kurz a workshop Riadenie dodávateľov, a kurz a workshop Riadenia kontinuity činností. Aktualizované boli sylaby viacerých existujúcich kurzov.

Za rok 2024 bolo realizovaných celkovo 53 školení, z toho 8 kurzov Základy KB, 20 kurzov Manažér KB, 3 kurzy Audítor KB, 7 špecializačných kurzov a workshopov, 1 kurz manažérstva informačnej bezpečnosti podľa ISO/IEC 27001:2022 a 10 bezplatných webinárov Prehľad kybernetickej bezpečnosti s účelom zvyšovania povedomia o kybernetickej bezpečnosti, 1 seminár s témou transpozície smernice NIS2, 1 webinár s témou ako správne napísať projekt a získať európske financovanie. Celkovo sa na uvedených vzdelávacích aktivitách počas roku 2024 zúčastnilo 961 účastníkov.

KCCKB sa aktívne zúčastňovalo na konferenciách a podujatiach na Slovensku aj v zahraničí. Celkovo zástupcovia KCCKB v roku 2024 uskutočnili 47 odborných prednášok na konferenciách, ako aj na pôde vybraných vysokých škôl v SR.

V rámci publikačných aktivít vydávalo KCCKB letáky na účely zvyšovania bezpečnostného povedomia:

- Kategórie osobných údajov
- Čo je to ransomvér a ako sa chrániť?
- 10 manažérskych chýb, ktoré vedú k incidentu
- Aké silné je vaše heslo?
- Najbežnejšie typy útokov na heslá
- Kybernetická bezpečnosť 2024 – materiál k prieskumu verejnej mienky

Už každoročne sú na základe zadania KCCKB vypracovávané prieskumy stavu kybernetickej bezpečnosti, ktoré sú následne vydané aj vo forme verejného dokumentu. V roku 2024 bol uskutočnený prieskum verejnej mienky medzi verejnosťou na vzorke 1000 respondentov.

Aj v roku 2024 KCCKB ďalej rozširovalo okruh organizácií, s ktorými uzatvorilo spoluprácu formou podpisu memoranda.

V spolupráci s SK-CERT postavilo KCCKB tím mladých, talentovaných ľudí, ktorí Slovensko reprezentovali v októbri 2024 na podujatí European CyberSecurity Challenge (ECSC) v talianskom Turíne. Aktivitu zastrešuje Európska agentúra pre kybernetickú bezpečnosť (ENISA). Prítomných bolo 44 národných tímov. Slovenský tím reprezentovalo desať mladých talentov – deväť chlapcov a jedno dievča. Na súťaž sa tím pripravoval niekoľko mesiacov. V júni sa zúčastnili medzinárodného bootcampu vo Viedni a následne šiestich tréningových bootcampov v Brunovciach. Tím sa pripravuje aj naďalej na účasť na ECSC v roku 2025.