NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

SPRÁVA O KYBERNETICKEJ BEZPEČNOSTI

V SLOVENSKEJ REPUBLIKE V ROKU 2025

SPRÁVA O KYBERNETICKEJ BEZPEČNOSTI

V SLOVENSKEJ REPUBLIKE
V ROKU 2025

OBSAH

PREDSLOV

Vážené dámy, vážení páni,

rok 2025 opätovne potvrdil, že kybernetická bezpečnosť predstavuje neoddeliteľnú súčasť bezpečnosti a stability štátu. Informačné a komunikačné technológie sú základnou infraštruktúrou fungovania spoločnosti a ich spoľahlivá prevádzka je nevyhnutnou podmienkou zabezpečenia chodu verejnej správy, ekonomiky aj každodenného života občanov. Úroveň kybernetickej bezpečnosti na Slovensku sa postupne zvyšuje, avšak stále pretrvávajú výzvy vyplývajúce z dynamicky sa meniaceho bezpečnostného prostredia.

Kybernetické hrozby dnes priamo ovplyvňujú odolnosť štátu. Ohrozujú kontinuitu poskytovania služieb, oslabujú fungovanie kritickej infraštruktúry a narúšajú schopnosť reagovať na krízové situácie. Ich dopady sa neprejavujú len v technickej ale aj v spoločenskej sfére. Výpadky systémov či nedostupnosť služieb znižujú dôveru verejnosti v štátne inštitúcie, pričom nedostatočná alebo nejednoznačná komunikácia v čase incidentov môže tento efekt ešte prehĺbiť a vytvárať priestor pre šírenie dezinformácií.

Významný je aj ekonomický rozmer kybernetickej bezpečnosti. Náklady spojené s obnovou po incidente spravidla výrazne prevyšujú investície potrebné na jeho prevenciu. Okrem priamych finančných strát dochádza aj k zníženiu produktivity, narušeniu dôvery a celkovému oslabeniu postavenia orgánov verejnej moci a spoločností. Z pohľadu strategického vnímania sú pritom zraniteľné všetky sektory, ktoré tvoria kritickú infraštruktúru štátu, vrátane verejnej správy, energetiky, zdravotníctva či finančného sektora.

Rok 2025 priniesol viaceré významné zmeny, pričom pre Národný bezpečnostný úrad bola kľúčová najmä novela zákona o kybernetickej bezpečnosti, ktorá zásadne ovplyvnila fungovanie národného systému kybernetickej bezpečnosti. Tento rok uzavrel strategické obdobie Národnej stratégie kybernetickej bezpečnosti na roky 2020 – 2025.

Skúsenosti z praxe opakovane potvrdzujú, že kybernetickú bezpečnosť nie je možné efektívne zabezpečiť bez spolupráce všetkých relevantných aktérov. Štát musí v tejto oblasti spolupracovať so súkromným sektorom, avšak nemenej dôležitú úlohu zohráva aj zodpovedný prístup jednotlivcov. Súčasný vývoj potvrdzuje, že kybernetická bezpečnosť sa stala prioritou s dopadom naprieč všetkými oblasťami fungovania štátu. Slovenská republika podľa hodnotenia Európskej agentúry pre kybernetickú bezpečnosť dosahuje v tejto oblasti nadpriemerné výsledky v rámci členských štátov Európskej únie. Aj napriek tomuto pozitívnemu vývoju zostáva systematické posilňovanie kybernetickej bezpečnosti nevyhnutné pre schopnosť Slovenskej republiky reagovať na výzvy digitálnej éry.

Roman Konečný
riaditeľ Národného bezpečnostného úradu

ZOZNAM SKRATIEK

AI	umelá inteligencia
APT	štátom sponzorovaná skupina (eng. advanced persistent threat)
CBM	opatrenia na budovanie dôvery
CECSP	Stredoeurópska platforma pre kybernetickú bezpečnosť
CER	Smernica o odolnosti kritických subjektov
CERT-EU	Tím reakcie na núdzové počítačové situácie v európskych inštitúciách, orgánoch a agentúrach
CRA	Akt o kybernetickej odolnosti
CTF	typ kyberbezpečnostnej hry (eng. capture the flag)
CVE	Common Vulnerabilities and Exposures
CyCLONe	Európska sieť styčných organizácií pre kybernetické krízy
CySOLa	Nariadenie o kybernetickej solidarite
DoS	útok odmietnutia služby
DDoS	distribuovaný útok odmietnutia služby
DORA	Nariadenie o digitálnej prevádzkovej odolnosti finančného sektora
EBW	Európska peňaženka podnikateľa
ECCC	Európske centrum kompetencií v oblasti kybernetickej bezpečnosti
ECCG	Európska skupina pre certifikáciu kybernetickej bezpečnosti
ECSC	European CyberSecurity Challenge
EDA	Európska obranná agentúra
EEAS	Európska služba pre vonkajšiu činnosť
eIDAS2	Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1183, ktorým sa mení nariadenie (EÚ) č. 910/2014, o zriadení európskeho rámca digitálnej identity
EK	Európska komisia
ENISA	Európska agentúra pre kybernetickú bezpečnosť
EÚ	Európska únia
EU MSS	Európska schéma certifikácie spravovaných bezpečnostných služieb (eng. managed security services)
EU5G	Európska schéma certifikácie kybernetickej bezpečnosti pre služby 5G
EUCC	Európska certifikačná schéma založená na spoločných kritériách
EUSA	Vesmírny akt
GDPR	Všeobecné nariadenie o ochrane údajov
HWPCI	Horizontálna pracovná skupina Rady EÚ pre kybernetické záležitosti
IKT	informačné a komunikačné technológie
IS	informačné systémy
IT	informačné technológie
ITVS	informačné technológie vo verejnej správe
IWG	Neformálna pracovná skupina OBSE pre oblasť kybernetickej bezpečnosti a využívania informačných a komunikačných technológií
JISKB	Jednotný informačný systém kybernetickej bezpečnosti
JLR	Jaguar Land Rover
KBI	kybernetický bezpečnostný incident
KCCKB	Kompetenčné a certifikačné centrum kybernetickej bezpečnosti
MF	Ministerstvo financií Slovenskej republiky

MH	Ministerstvo hospodárstva Slovenskej republiky
MIRRI	Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky
MKB	manažér kybernetickej bezpečnosti
MV	Ministerstvo vnútra Slovenskej republiky
MZVEZ	Ministerstvo zahraničných vecí a európskych záležitostí Slovenskej republiky
NANDO	New Approach Notified and Designated Organisations
NASES	Národná agentúra pre sieťové a elektronické služby
NATO	Organizácia Severoatlantickej zmluvy
NATO CCDCOE	Centrum excelentnosti kooperatívnej kybernetickej obrany NATO
NOS	Bezpečnostný úrad NATO
NBÚ	Národný bezpečnostný úrad
NCC	Národné koordinačné centrum
NCCA	Národná autorita pre certifikáciu kybernetickej bezpečnosti
NCIA	Agentúra NATO pre komunikačné a informačné technológie
NCKB	Národné centrum kybernetickej bezpečnosti
NEV	nežiadúce elektromagnetické vyžarovanie
NIS	Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii
NIS2	Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii
NOKC	Národný orgán pre kyberbezpečnostnú certifikáciu
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OBSE	Organizácia pre bezpečnosť a spoluprácu v Európe
OČTK	orgány činné v trestnom konaní
OEWG	Otvorená pracovná skupina OSN pre využívanie informačných a komunikačných technológií
OSINT	spravodajstvo z otvorených zdrojov
OSN	Organizácia Spojených národov
OT	priemyselné riadiace systémy
OVM	orgány verejnej moci
PIKB	Posilnenie informačnej a kybernetickej bezpečnosti
PZ	Policajný zbor Slovenskej republiky
SIS	Slovenská informačná služba
SK-CERT	Národná jednotka CSIRT
SOC	bezpečnostné operačné centrum
SR	Slovenská republika
STU	Slovenská technická univerzita v Bratislave
ÚGKK	Úrad geodézie, kartografie a katastra Slovenskej republiky
UK	Univerzita Komenského v Bratislave
VJ CSIRT	Vládna jednotka pre riešenie počítačových incidentov
VS	Vojenské spravodajstvo
VšZP	Všeobecná zdravotná poisťovňa
ZoKB	Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
ZÚ	zastupiteľský úrad

1. PREHĽAD KYBERNETICKEJ BEZPEČNOSTI ZA ROK 2025

1. 1. Geopolitický kontext

Kybernetický priestor sa stal strategickou doménou, prostredníctvom ktorej štáty presadzujú svoje záujmy, demonštrujú moc a realizujú nátlakové či destabilizačné aktivity. Viaceré krajiny v roku 2025 využívali kybernetické operácie v rámci svojej zahraničnej a bezpečnostnej politiky. Kybernetické útoky nie sú len súčasťou širších hybridných aktivít, ale predstavujú aj prvotnú fázu ozbrojených konfliktov tradičného typu. Ich cieľom je najmä poškodzovanie kritickej infraštruktúry, destabilizácia politického systému, nátlak a psychologické operácie, ktoré ovplyvňujú verejnú mienku.

Najvýznamnejším faktorom ovplyvňujúcim kybernetickú bezpečnosť zostáva aktuálna geopolitická situácia, najmä pokračujúce vojenské konflikty, ale aj stupňujúce sa napätie na Blízkom východe. V európskom priestore má zásadný vplyv pokračujúca agresia Ruska proti Ukrajine a s ňou spojené hybridné a kybernetické aktivity. Popri tradičných aktéroch, ako sú Rusko, Čína, Irán či Severná Kórea, sa čoraz výraznejšie presadzujú aj menší aktéri, ktorí využívajú stále ľahšiu dostupnosť nástrojov na realizáciu kybernetických útokov. Skupiny aktérov, ktoré sú vládami uvedených krajín priamo riadené alebo aspoň podporované, sa svojimi kybernetickými aktivitami stále častejšie zameriavajú na štátne orgány a inštitúcie členských krajín NATO a EÚ s cieľom získavať citlivé informácie. Pokračuje aj technologický tlak zo strany Číny, ktorý je už viditeľný aj v oblasti AI.

V Európe zohrali kybernetické operácie významnú úlohu pri volebných procesoch v Moldavsku a Rumunsku, kde sa manipulácia prostredníctvom dezinformačných kampaní a deepfake obsahu s použitím umelej inteligencie ukázala ako silný nástroj ovplyvňovania verejnej mienky. Prezidentské voľby v Rumunsku boli osobitne sledované, pretože išlo o opakovanie volieb prezidenta z roku 2024, ktorých výsledok bol anulovaný ústavným súdom práve z dôvodu bezprecedentného a preukázaného zasahovania do ich priebehu zahraničným aktérom.

V priebehu roka 2025 bolo tiež viditeľné oslabovanie medzinárodnej spolupráce medzi tradičnými partnermi a rast geopolitického súperenia, čo sa prejavovalo v oblasti sankčných režimov, znižovania vzájomnej podpory, spolupráce a koordinácie medzi spojencami, ale tiež znižovania efektivity uplatňovania medzinárodného práva.

Dopady kybernetických incidentov často presahovali hranice štátov. Útoky na energetickú infraštruktúru v Európe, ako aj incidenty s vysokým dopadom na ekonomicky významné sektory (napr. v leteckom priemysle alebo automobilovom sektore) ukázali, že kybernetické hrozby môžu zásadne narušiť fungovanie štátu a jeho ekonomiky. Zároveň sa potvrdilo, že zraniteľnosti sa nevyhýbajú ani veľkým organizáciám a technologicky vyspelým podnikom, pri ktorých by sa vzhľadom na dostupné zdroje a úroveň zabezpečenia očakávala vyššia miera odolnosti.

Postupný rozvoj legislatívneho rámca na úrovni Európskej únie zároveň poukazuje na pretrvávajúcu potrebu zabezpečiť jeho efektívnu implementáciu a vymožiteľnosť v praxi. Regulačný rámec, formovaný na národnej aj európskej úrovni, vytvára predpoklady na systematické zvyšovanie úrovne kybernetickej bezpečnosti, jeho skutočný prínos však závisí od dôsledného uplatňovania v praxi a schopnosti reagovať na dynamicky sa meniace technologické a geopolitické prostredie.

1. 2. Kľúčové faktory ovplyvňujúce kybernetickú bezpečnosť

V roku 2025 došlo k zvýrazneniu niektorých faktorov, ktoré dominantným spôsobom ovplyvňovali celkový stav a dynamiku vývoja kybernetickej bezpečnosti. Tento vývoj zdôrazňuje komplexnosť rizík ovplyvňujúcich kybernetické prostredie a náročnosť jeho ochrany pred rastúcimi hrozbami.

Kybernetické operácie štátmi sponzorovaných skupín

Kybernetické operácie APT skupín, ktoré sú priamo riadené alebo aspoň podporované niektorými štátmi, najmä Ruskom a Čínou, sa aj v uplynulom roku zameriavali najmä na kybernetickú špionáž, získavanie citlivých informácií a prienik do kritickej infraštruktúry. Primárnymi cieľmi týchto aktivít sa stali najmä štátne inštitúcie a organizácie s vysokým významom pre fungovanie štátu. Mnohé z týchto aktivít neboli zamerané na okamžité narušenie prevádzky, ale na vytváranie a udržiavanie dlhodobého prístupu do informačných systémov, ktorý môže byť zneužitý v období zvýšeného geopolitického napätia.

Rastúca kvalita útokov využívajúcich sociálne inžinierstvo

V roku 2025 patrilo sociálne inžinierstvo medzi najvýznamnejšie výzvy v oblasti kybernetickej bezpečnosti. Phishing a podvody boli čoraz presvedčivejšie, pričom škodlivý obsah bol distribuovaný prostredníctvom rôznych komunikačných kanálov. Útočníci využívali široké spektrum moderných phishingových nástrojov na ich jednoduchú tvorbu a zverejnenie. Rozvoj AI v podobe generatívnych jazykových modelov umožnil okrem vysokej kvality klamlivého obsahu (deepfake) aj tvorbu cieleného a personalizovaného obsahu pre konkrétnu obeť. Významnú úlohu zohrával aj rastúci obchod s uniknutými údajmi, ktorý pri ich zneužití zabezpečoval ľahký a často nepozorovaný prienik do systémov.

Zneužívanie zraniteľností

Zraniteľnosť sa netýka len chyby alebo nežiaducej vlastnosti zariadenia alebo softvéru, prípadne chyby v logike procesu a služby, ale zahŕňa tiež ich nesprávnu konfiguráciu a použitie. V období stúpajúcej dynamiky a nárastu počtu zraniteľností nultého dňa je obzvlášť alarmujúce prevádzkovanie zariadení a systémov s ukončenou technickou podporou, pre ktoré výrobca už nevydáva bezpečnostné aktualizácie. V roku 2025 bolo možné pozorovať nárast počtu takýchto systémov, čo súvisí s rastúcou komplexnosťou technológií, ich prepojenosťou, s nedostatočným dodržiavaním základných kyberbezpečnostných zásad a v niektorých sektoroch aj s nedostatočným financovaním prevádzky a rozvoja IT infraštruktúry. Tento trend rapídne zvyšuje riziko zneužitia zraniteľností útočníkmi.

Bezpečnosť dodávateľských reťazcov

Skúsenosti z roku 2025 potvrdili, že kybernetický incident u dodávateľa môže mať vplyv na desiatky ďalších organizácií v dodávateľskom reťazci. Viaceré incidenty v 2025 ukázali, že narušenie informačného systému dodávateľa môže paralyzovať kľúčové podniky a organizácie naraz vo viacerých sektoroch a krajinách. Úniky citlivých údajov z kompromitovaných systémov dodávateľa, ktoré sa týkajú rôznych organizácií v priestore EÚ vytvárajú riziko ich sekundárneho zneužitia na paralelné útoky, či už na priamy prienik do systémov alebo realizáciu cielených phishingových kampaní.

AI ako príležitosť ale aj riziko

AI sa stala neoddeliteľnou súčasťou každodenného života a pre jednotlivcov, firmy aj štáty priniesla nové príležitosti pre zefektívnenie najrôznejších procesov a zrýchlenie mnohých činností. Zároveň však predstavovala výzvu z pohľadu kybernetickej bezpečnosti, keďže možnosti jej zneužitia vytvárajú mnohé riziká, z ktorých mnohé ešte ani nepoznáme. Najviditeľnejším príkladom zneužívania AI bolo generovanie deepfake obsahu a dezinformačných kampaní, ktoré sú čoraz presvedčivejšie a využívané na impersonáciu osôb a šírenie škodlivého obsahu. Nekontrolované používanie alebo zneužívanie AI môže viesť k mnohým iným rizikám, od nepozorovaného úniku citlivých údajov až po vzdialené vykonanie kódu a získanie úplnej kontroly nad systémom. Je nevyhnutné túto technológiu využívať efektívne, ako aj zabezpečiť jej ochranu tak, aby sa nestala zdrojom bezpečnostných rizík. Cesta k cieľu, akým je riadený bezpečný vývoj, nasadzovanie a používanie AI, nevedie iba cez jej urýchlenú reguláciu, ale najmä cez jej spoznávanie, teda vedu, výskum a vzdelávanie.

Nedostatok odborných kapacít

Nedostatok odborných kapacít patrí dlhodobo medzi významné výzvy v oblasti kybernetickej bezpečnosti, a to nielen na Slovensku. Tento problém sa opakovane objavuje aj vo výsledkoch prieskumov a analýz, ktoré poukazujú na pretrvávajúci nedostatok kvalifikovaných odborníkov a potrebu systematického rozvoja odborných kapacít, ktoré sú nevyhnutné pre obsadzovanie pracovných pozícií v oblasti kybernetickej bezpečnosti.

1. 3. Povedomie o kybernetickej bezpečnosti v spoločnosti

Kybernetická bezpečnosť je nielen doménou národnej bezpečnosti, ale aj celospoločenskou témou. Dlhodobo tvorí súčasť bežného života spoločnosti a vďaka médiám sa čoraz viac dostáva do povedomia širokej verejnosti. Ľudia si uvedomujú, že časť ich bežného života sa odohráva v kybernetickom priestore, kde čelia hrozbám, ktoré môžu negatívne ovplyvniť ich digitálne aktíva – teda údaje, súkromie, ale aj peniaze. Je zrejmé, že čím vyššie je povedomie o kybernetických rizikách a o spôsobe ochrany pred nimi, tým sú spoločnosť a štát odolnejšie voči kybernetickým bezpečnostným hrozbám.

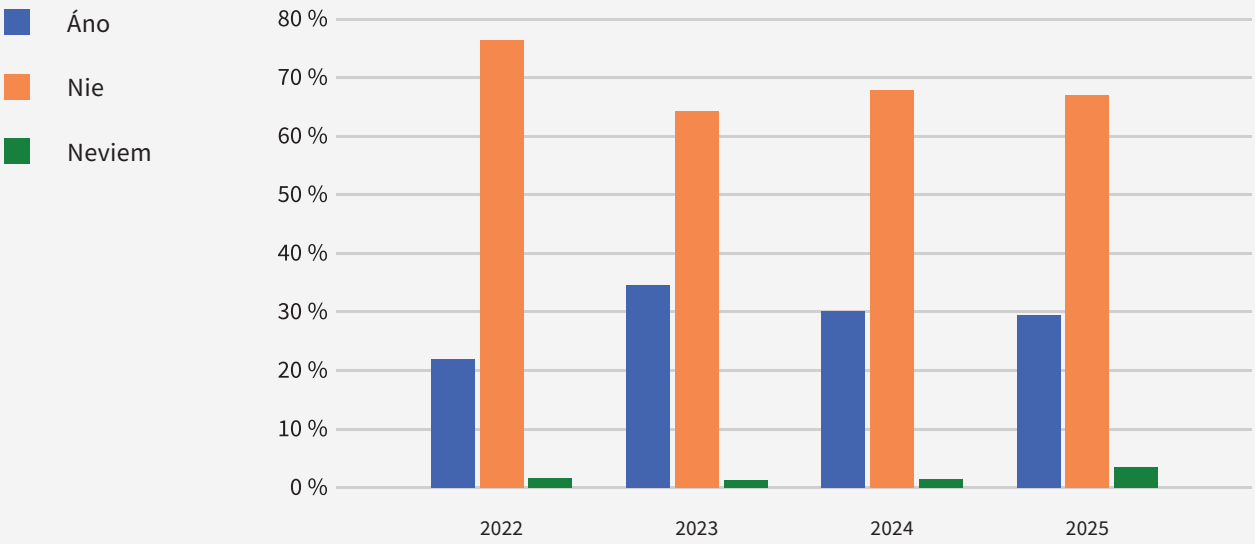
Aké sú vedomosti a návyky pri používaní digitálnych zariadení a služieb a aká je miera poznania kybernetickej bezpečnosti mali za cieľ zistiť reprezentatívne prieskumy realizované pre Kompetenčné a certifikačné centrum kybernetickej bezpečnosti.[1] Prieskum, ktorý sa uskutočnil v dňoch 10.-16.10.2025 na reprezentatívnej vzorke tisíc respondentov, potvrdzuje, že väčšina spoločnosti využíva iba základné formy kybernetickej ochrany a o hrozbách digitálneho prostredia má nedostatočné informácie. Do prieskumu boli zahrnuté aj otázky o nových technologických trendoch, napríklad o používaní umelej inteligencie či postkvantovej kryptografii. Štruktúra prieskumu bola zvolená zámerne tak, aby pokrývala čo najväčší rozsah relevantných tém.

[1] Reprezentatívny prieskum kybernetickej bezpečnosti za rok 2025, SCIO, október 2025
Reprezentatívny prieskum kybernetickej bezpečnosti za rok 2024, AKO, júl 2024

Bezpečnosť detí v digitálnom priestore

Väčšina rodičov neprijíma dostatočné opatrenia na ochranu detí v online priestore. Až dve tretiny opýtaných nepoužívajú žiadnu formu rodičovskej kontroly, čo možno považovať za vážne riziko. Deti sa tak môžu jednoduchšie dostať k nevhodnému obsahu, môžu byť vystavené kyberšikane, online predátorom alebo iným formám zneužitia. Zabezpečenie digitálnej ochrany detí by malo byť súčasťou základnej digitálnej výchovy rodičov, podporenej školskými programami, ale aj inými štátnymi a neštátnymi preventívnymi aktivitami.

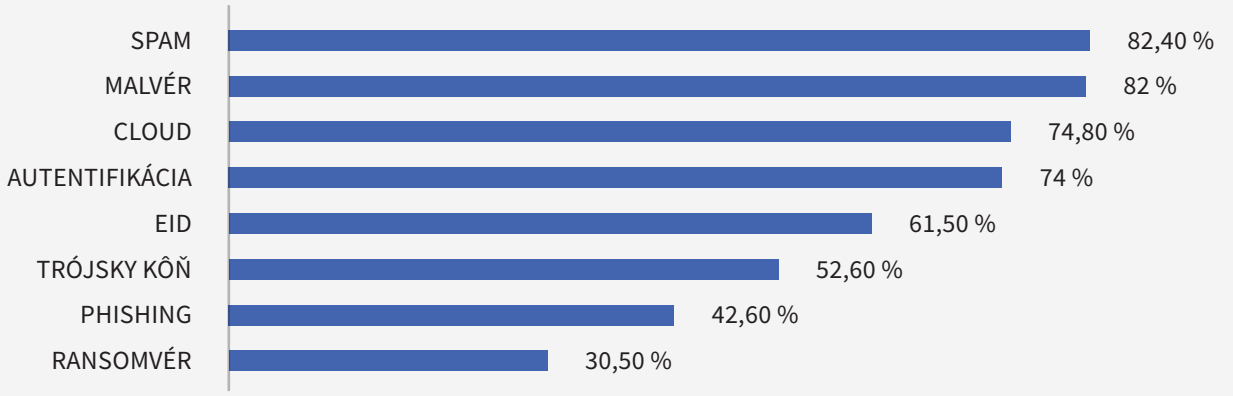
Používate nástroje rodičovskej kontroly?



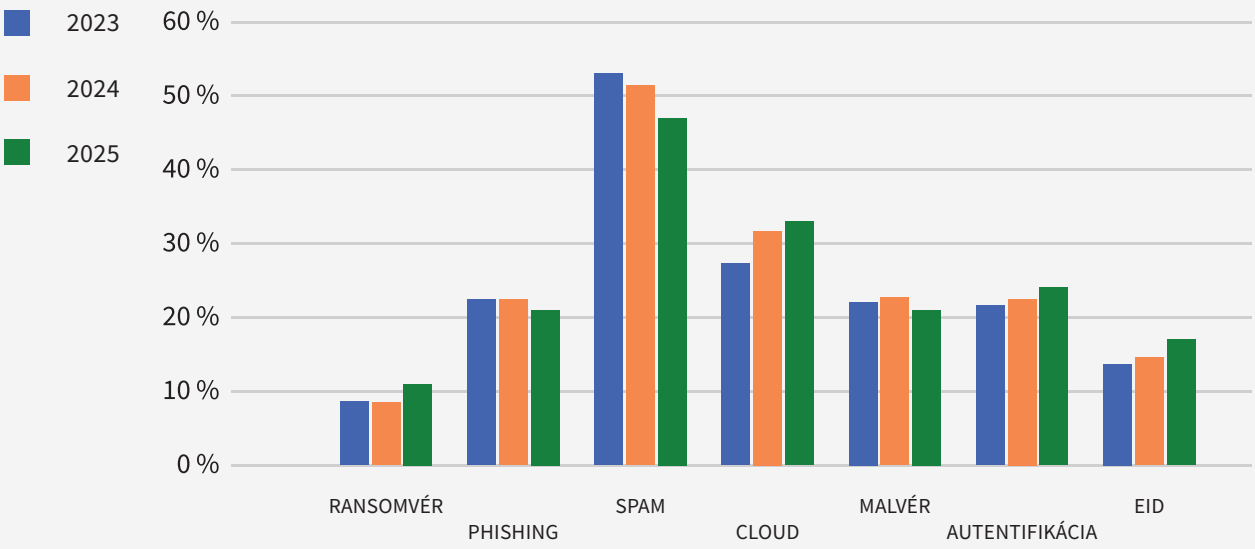
Znalosť rizík spojených s IT technológiami

Znalosť základných IT pojmov je v spoločnosti pomerne nízka. Z pohľadu kybernetickej bezpečnosti ide o základný prvok odolnosti spoločnosti, pretože informovaná osoba je menej náchylná sa stať obeťou útoku. Neznalosť týchto pojmov zvyšuje riziko správania, pri ktorom používatelia nedokážu rozpoznať hrozbu ani prijať adekvátne opatrenia na svoju ochranu. Výnimku tvorí pojem spam, ktorý je známy väčšine populácie. Naopak, pojmy ako phishing, ransomvér či autentifikácia sú väčšine skúmanej populácie neznáme. Iba štyria z desiatich respondentov poznajú pojem ransomvér, čo možno považovať za kritické zistenie. Výsledky prieskumov naznačujú, že vo väčšine pojmov je trend nastavený pozitívne, avšak tempo rastu nie je výrazné. Tieto zistenia poukazujú na potrebu systematického vzdelávania a popularizácie kybernetických pojmov.

Analýza otvorených odpovedí – správne definície pojmov



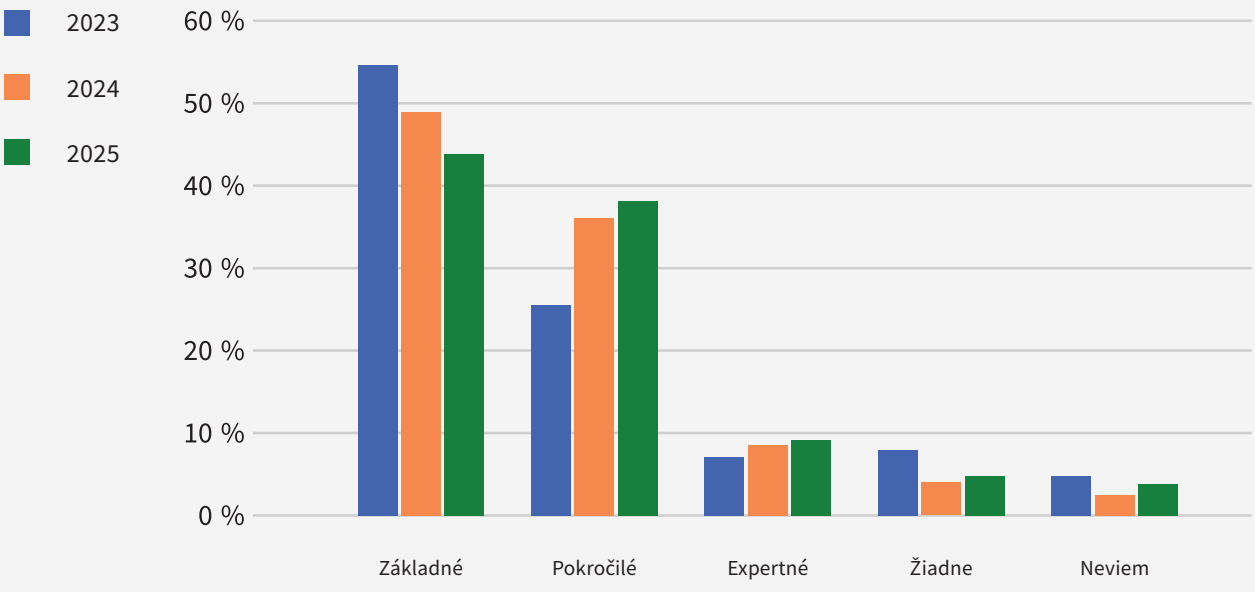
Poznateľnosť pojmu



Digitálne zručnosti obyvateľstva

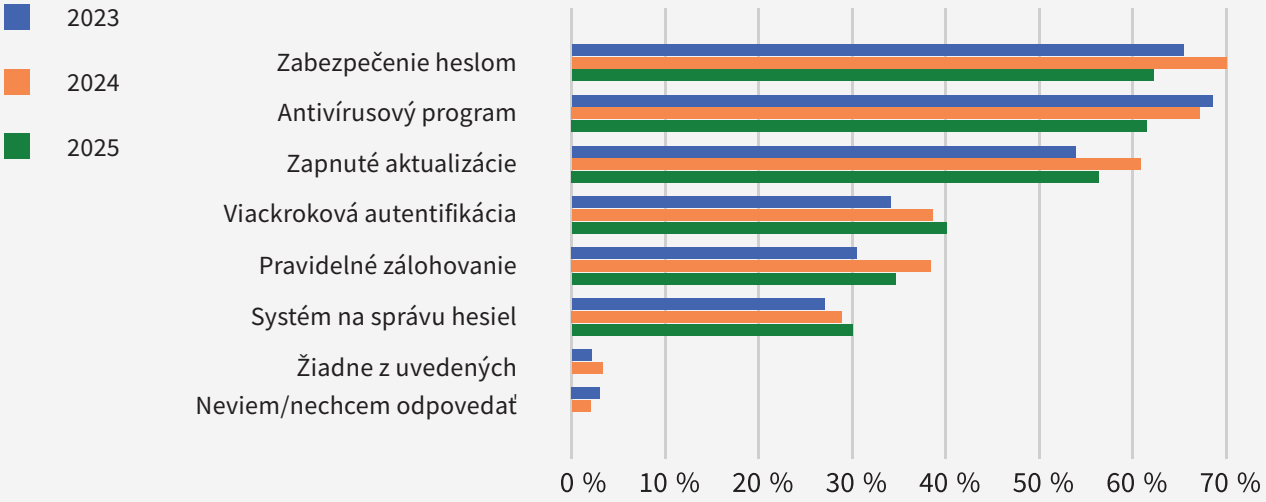
Vzhľadom na to, že práve ľudský faktor predstavuje významný prvok kybernetickej bezpečnosti, je postupná zmena štruktúry obyvateľstva v oblasti digitálnych zručností pozitívnym zistením. Klesá podiel osôb s iba základnými zručnosťami a súčasne rastie podiel spoločnosti s pokročilými a expertnými kompetenciami. Priaznivým trendom je pokles osôb bez digitálnych zručností, čo naznačuje postupné znižovanie priepastných rozdielov v spoločnosti. Napriek tomu úroveň digitálnych zručností slovenskej populácie zostáva prevažne na základnej úrovni. Z pohľadu kybernetickej bezpečnosti je dôležité vnímať digitálnu negramotnosť ako vážne systémové riziko.

Aké sú vaše digitálne zručnosti?



Údaje za obdobie 2023 – 2025 naznačujú relatívne stabilné používanie základných bezpečnostných prvkov a nástrojov, pričom najčastejšie používanými zostáva heslo a antivírusový program. Je zrejmé, že zvyšujúce sa bezpečnostné povedomie pozitívne vplýva na používanie vhodných bezpečnostných opatrení.

Ktoré z nasledujúcich opatrení počítačovej bezpečnosti používate?

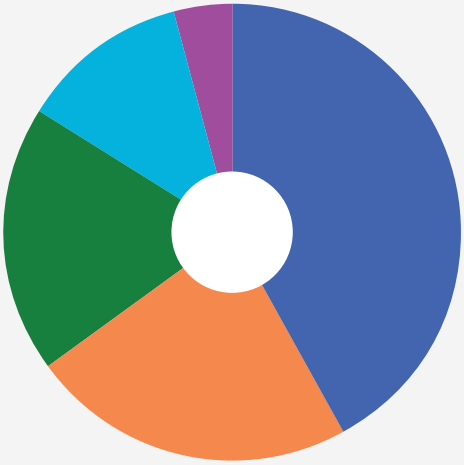


Bezpečné používanie hesiel

Používanie rovnakého hesla zostáva v populácii pomerne rozšíreným javom. Len pätina respondentov uviedla, že pre každý účet používa unikátne heslo. Tento návyk predstavuje jedno z najväčších rizík v oblasti osobnej kybernetickej bezpečnosti. Kompromitácia jedného účtu môže viesť k ohrozeniu ďalších služieb. Zistenia poukazujú na potrebu systematického vzdelávania v oblasti správy hesiel.

Používate rovnaké heslo pre rôzne systémy?

Niektoré účty	42 %
Nikdy nepoužívam rovnaké heslá	23 %
Väčšina účtov	19 %
Neviem	12 %
Všetky účty	4 %



Používanie AI

AI sa stala prirodzenou súčasťou života spoločnosti, hoci mnohí si jej prítomnosť v digitálnom prostredí a jej pravidelné používanie pravdepodobne ani neuvedomujú. Viac ako polovica populácie využíva aspoň jeden AI systém, čo si vyžaduje neustále zvyšovanie informovanosti o benefitoch, ale aj rizikách AI systémov, osobitne v kontexte dynamického technologického vývoja, ktorý je charakteristický pre posledné obdobie.

Používate systémy s umelou inteligenciou?

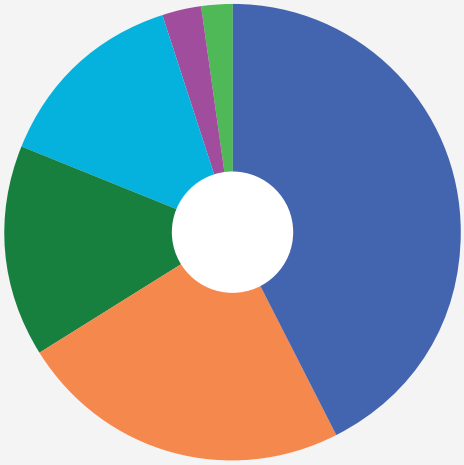
Používa aspoň jeden AI systém	52 %
Nepoužíva	48 %

Kvantové počítače a postkvantová kryptografia

Povedomie o kvantových technológiách, ako aj o postkvantovom šifrovaní je veľmi nízke. Spoločnosť na Slovensku momentálne nedisponuje dostatočnou mierou pripravenosti na technologické zmeny súvisiace s rozvojom kvantovej informatiky, osvetové aktivity by sa preto mali zamerať aj na túto oblasť.

Používate systémy s umelou inteligenciou?

Nikdy nepočul/a	43 %
Počul/a, nerozumie	24 %
Základná predstava	15 %
Nevie	14 %
Oboznámený/á	3 %
Plánuje používať	2 %



Výsledky prieskumu naznačujú, že úroveň povedomia obyvateľov o kybernetickej bezpečnosti sa síce postupne zlepšuje, avšak pretrvávajú výrazné medzery v oblasti bezpečnostných návykov a poznania hrozieb. Digitálne zručnosti populácie zostávajú prevažne na základnej úrovni a len malá časť respondentov disponuje pokročilými zručnosťami. Hoci väčšina respondentov používa základné bezpečnostné opatrenia, pokročilejšie nástroje sú využívané v podstatne nižšej miere. Úroveň povedomia o kybernetických hrozbách, umelej inteligencii či kvantových technológiách je značne obmedzená, avšak v krátkodobom horizonte je možné očakávať jeho rozvoj. Informovanosť je základným predpokladom účinnej ochrany pred kybernetickými hrozbami. Z dlhodobého hľadiska je preto nevyhnutné kontinuálne rozvíjať vzdelávanie v kybernetickej bezpečnosti.

2. NAJVÝZNAMNEJŠIE UDALOSTI V SLOVENSKEJ REPUBLIKE ZA ROK 2025

Znefunkčnenie služieb slovenského katastra nehnuteľností

Začiatkom roka 2025 bol ÚGKK terčom ransomvérového útoku, ktorý spôsobil významný výpadok kľúčových informačných systémov. Kompromitácia informačných systémov bola rozsiahla. Incident mal priamy vplyv na takmer všetky služby geodézie a katastra, ktorých nedostupnosť ovplyvnila prevádzku samospráv, štátnej správy a subjektov v súkromnom sektore.

Nefunkčné služby výrazne obmedzovali prístup k údajom o vlastníckych právach, parcelách, mapových podkladoch a k funkciám spojeným so zápisom zmien do katastra, ale tiež ku geodetickej dátovej sade a dátam, ktoré využívajú geolokalizačné služby. To spôsobilo oneskorenia v agende územného plánovania, stavebného konania, verejných obstarávaní, ako aj trhu s nehnuteľnosťami a poskytovaním hypotekárnych úverov. Narušená bola činnosť geodetov aj niektorých služieb a zariadení založených na geolokácii.

Incident bol identifikovaný v rámci niekoľkých hodín, pričom okamžite nasledovalo odpojenie kľúčových systémov od verejnej siete a spustenie štandardizovaného postupu riešenia KBI. Na miesto boli prizvané odborné tímy, ktoré koordinovali technickú forenznú analýzu a proces obnovy. Do procesu boli zapojené všetky jednotky CSIRT a ďalšie relevantné subjekty, pričom incident bol eskalovaný aj na Bezpečnostnú radu SR. V rámci riešenia incidentu bolo kľúčovým zistením, že dáta informačných systémov katastra je možné obnoviť zo zálohy a že tieto dáta nevykazovali žiadne známky narušenia ich integrity. Expertom sa podarilo dáta obnoviť i keď celková obnova infraštruktúry ÚGKK a jeho služieb si vyžiadala niekoľko mesiacov práce. Bezprostredne po incidente boli prijaté viaceré opatrenia na posilnenie kybernetickej odolnosti, a to nielen na ÚGKK, ale aj v ostatných orgánoch verejnej správy.

Incident tiež podčiarkol význam včasnej aplikácie bezpečnostných aktualizácií na odstránenie známych zraniteľností a potrebu nepretržitého bezpečnostného monitoringu prostredníctvom pokročilých riešení, ako aj detekcie a reakcie na hrozby na koncových zariadeniach.

Skenovanie siete a pokusy o prienik do systémov

Po kompromitácii systémov ÚGKK pristúpilo viacero štátnych inštitúcií k aktívnemu zhodnoteniu kybernetickej odolnosti svojej IT infraštruktúry, najmä verejne dostupných zariadení, systémov a služieb. Realizovali sa opatrenia ako penetračné testovanie, kontrola verejne dostupných služieb a audit pripojených zariadení na známe zraniteľnosti. To aj z dôvodu, že NASES dlhodobo eviduje vysoký objem skenov vládnej siete Govnet z internetu, pričom časť z nich môže byť výsledkom penetračných testov či iných aktivít, ktoré neboli riadne nahlásené alebo oznámené, a preto sú zachytené bezpečnostným dohľadom ako incidenty. Paralelne s legitímnymi aktivitami bol zaznamenaný všeobecný nárast útokov spojených so skenovaním a pokusmi o prienik do verejne dostupných sietí.

Výhražné bombové správy

Začiatkom roku 2025 bola zaznamenaná vlna výhražných e-mailových kampaní obsahujúcich bombové hrozby zameraná na školy a iné verejné inštitúcie. V reakcii na situáciu vydal NBÚ odporúčanie na elimináciu týchto hrozieb, predovšetkým odporúčal blokovanie prichádzajúcich e-mailových správ zo serverov, ktoré slúžia na skrytie identity odosielateľov týchto hrozieb. V rámci zvýšenia pripravenosti na podobné incidenty vydala SIS v spolupráci s MV SR, PZ a NBÚ metodiku pre vyhodnocovanie rizika bombových hrozieb. V nasledujúcich kvartáloch bol zaznamenaný pokles počtu hlásení výhražných správ, čo mohlo súvisieť s prijatými opatreniami či s kombináciou viacerých externých faktorov. V poslednom kvartáli 2025 boli zaznamenané bombové vyhrážky rozposlané na viacero nemocníc spadajúcich pod rovnakého prevádzkovateľa. Táto vlna výhražných správ poukázala na význam ich dôsledného zabezpečenia a taktiež podmienenia odoslania správy overením identity odosielateľa.

Zvýšený výskyt ransomvérových útokov

V priebehu roka 2025 bolo hlásených niekoľko ransomvérových útokov, ktorých cieľom bolo široké spektrum spoločností naprieč rôznymi sektormi. Tieto incidenty potvrdili pretrvávajúci trend, podľa ktorého ransomvérové skupiny cielia nielen na veľké organizácie, ale aj na menšie subjekty s nižšou úrovňou zabezpečenia. Vektorom prieniku sa najčastejšie stali nedostatočne zabezpečené služby vzdialeného prístupu alebo verejne dostupné zariadenia a systémy, ktoré neboli pravidelne aktualizované resp. boli závislé od špecifických softvérových riešení.

Počas roka bol zachytený aj prípad, ktorý nebol včas nahlásený NBÚ. Subjekt s útočníkom komunikoval a zaplatil výkupné podľa pokynov. Po zaplatení výkupného bol poskytnutý dešifrovací nástroj iba na časť zašifrovaných súborov. Útočník následne zvýšil požadovanú sumu za sprístupnenie zvyšných dát. Napokon sa ukázalo, že subjekt disponuje funkčnými zálohami. Spomínaný incident poukazuje na význam pravidla „nikdy neplatiť útočníkovi“, ktoré NBÚ neustále prízvukuje, nakoľko obeť nemá akékoľvek záruku, že útočník splní, čo prisľúbil.

Zneužívanie nedostatočne zabezpečených zariadení

V máji rezonovala informačným prostredím správa o zneužívaní nedostatočne zabezpečených kamier v kybernetickom priestore SR, ktoré mali zneužívať ruskí štátom sponzorovaní aktéri. Útok cielil nielen na kamery priamo prístupné z internetu, ale aj na kamery nepriamo dostupné prostredníctvom nesprávne nakonfigurovaných routerov, firewallov a media serverov. Útočníci zneužívali prístup ku kamerám na špionáž a sledovanie verejných priestranstiev, dopravných koridorov a zariadení alebo pohraničných oblastí. Skupina tieto aktivity vykonávala najmenej od roku 2022.

Phishingové kampane

Spomedzi podvodných phishingových útokov vzbudila v apríli 2025 pozornosť hlasovacia kampaň vo falošnej súťaži alebo ankete. Útok začal prijatím správy v aplikácii WhatsApp od niektorého z uložených kontaktov. Odosielateľ prijímateľa v správe vyzýval na hlasovanie v súťaži, v ktorej mohla dcéra alebo príbuzná odosielateľa získať štipendium alebo inú cenu. Podvodná správa mala charakter URL linku s falošnou fotografiou malej tanečníčky/baletky, ktorej malo údajné hlasovanie pomôcť v súťaži. Po kliknutí na URL odkaz v správe sa prijímateľ dostal do falošného hlasovacieho portálu, ktorý vyžadoval autentifikáciu hlasujúceho formou telefónneho čísla a overovacieho kódu. Tieto údaje umožnili útočníkovi prístup do aplikácie obete a jej spárovanie so zariadením útočníka. Okrem kompromitácie obsahu aplikácie útočník ďalej rozosielal podvodnú kampaň v mene obete. Na riešenie problému bolo potrebné manuálne odpárovať všetky zariadenia napojené na aplikáciu.

Zachytené boli aj prípady phishingových kampaní zneužívajúcich kompromitované e-mailové účty a cloudové platformy na zdieľanie súborov. Princíp podvodu spočíval v tom, že podvodník v mene kontaktu z adresára obete zaslal informáciu o zdieľaní PDF súboru, ktorý mohol byť maskovaný ako faktúra. Súbor následne naviedol obeť na odkaz falošného prihlasovacieho okna do aplikácie Microsoft 365, ktorý už bol pod kontrolou útočníka. Obeť v domnienke zadávania prihlasovacích údajov do svojho účtu zadala údaje priamo útočníkovi, ktorý takto získal prístup k účtu obete a zároveň ďalší kanál, ktorým mohol rozposielať škodlivú kampaň. Tento druh phishingu je nebezpečný najmä preto , že jeho pôvodcom je legitímna e-mailová adresa a škodlivý obsah je umiestnený na skutočnej adrese úložiska, čím útočník obchádza všetky bezpečnostné protokoly, ktoré majú obeť chrániť pred phishingom.

Narušenie dodávateľského reťazca v dôsledku KBI

Hlavnou udalosťou tretieho kvartálu 2025 bol jeden z najvážnejších kybernetických incidentov posledných rokov. Spoločnosť Jaguar Land Rover (JLR) bola koncom augusta nútená odstaviť výrobu a centrálne IT systémy vo viacerých krajinách po tom, ako sa stala obeťou cieleného útoku. Incident paralyzoval procesy výroby, fakturácie, registrácie vozidiel a logistiky náhradných dielov. Firma musela prejsť na postupný kontrolovaný reštart, ktorý trval niekoľko týždňov a spôsobil vážne ekonomické škody. Britská vláda dokonca poskytla garančný rámec vo výške 1,5 miliardy libier, aby stabilizovala dodávateľský reťazec a ochránila menších subdodávateľov pred kolapsom. Spoločnosť potvrdila exfiltráciu časti dát, hoci zdôraznila, že nemá dôkaz o úniku zákazníckych informácií. Podľa dostupných informácií mohol incidentu podstatne napomôcť aj fakt, že JLR nemala dostatočne oddelené IT a výrobné OT systémy. V dôsledku toho sa útok rozšíril rýchlejšie a zasiahol celé prostredie výrobných závodov.

Dopady boli okamžité aj na Slovensku. Závod JLR v Nitre, ktorý zamestnáva približne 5-tisíc ľudí, musel zastaviť výrobu. Nitriansky závod preventívne odstavil lokálne systémy, aby sa útok nešíril ďalej. Obnovenie výroby na Slovensku sa oproti iným krajinám výrazne oneskorilo. JLR začal finančné a logistické systémy (fakturácie, registrácie vozidiel, distribúciu náhradných dielov) zapínať postupne, nitrianska továreň sa však do plnej prevádzky dostala až v októbri. Pre Slovensko to znamenalo nielen okamžitý výpadok produkcie, ale aj narušenie subdodávateľského reťazca. Lokálni dodávatelia dielov čelili oneskorenej fakturácii a nedostatku transparentných informácií, čo vytvorilo výrazný tlak na ich likviditu.

Tento prípad ilustruje efekt prelievania – incident, ktorý vznikol mimo Slovenska, okamžite a priamo ochromil jednu z najväčších zahraničných investícií v krajine a spôsobil sekundárne škody v dodávateľskej sieti. Pre slovenský kybernetický priestor je to dôležité poznanie. Naša infraštruktúra je plne previazaná s medzinárodnými systémami. To znamená, že aj útoky cielené primárne na zahraničné centrály, môžu mať okamžitý vplyv na naše podniky, zamestnancov a ekonomiku. Kybernetickú bezpečnosť je preto potrebné chápať ako súčasť medzinárodne prepojeného ekosystému, v ktorom nestačí zabezpečovať len lokálnu ochranu, ale je nevyhnutné budovať odolnosť aj v širšom cezhraničnom kontexte.

Vishing – podvody prostredníctvom telefonických hovorov

V treťom kvartáli bol zaznamenaný výrazný nárast počtu podvodných schém výhodného investovania spojeného s kryptomenami, v ktorom sa útočníci vydávali za pracovníkov investičných spoločností. Podvodníci si v tomto prípade svoje obete pravdepodobne vopred identifikovali v uniknutých dátových zoznamoch.

Vishing má podobu telefonického hovoru, v ktorom podvodníci tvrdia, že kontaktovaná osoba má u nich založený investičný alebo kryptomenový účet a vyzývajú ju na výber finančných prostriedkov. Útočníci sa zvyčajne vydávajú za skutočné investičné platformy a obeti často zasielajú e-mail s prihlasovacími údajmi do podvodnej mobilnej alebo webovej aplikácie, prípadne URL adresu alebo screenshot s údajným ziskom, ktorý v skutočnosti nikdy nevznikol. Útočníci od obete naliehavým slovníkom žiadajú výber zisku, za ktorý vyžadujú zaplatiť finančný poplatok, stiahnuť si nebezpečnú aplikáciu na vzdialený prístup alebo poskytnutie citlivých údajov obete.

NCKB zaznamenalo aj niekoľko prípadov, v ktorých podvodníci ponúkali zhodnotenie vlastných úspor formou investovania do trhov a kryptomien. Aj v tomto prípade podvodníci kontaktovali obeť prostredníctvom e-mailu, v ktorom ponúkali výhodné investovanie s veľkou finančnou návratnosťou. Podvodníci používali na komunikáciu Gmail účty a aplikáciu WhatsApp. Falošné investovanie spočívalo v registrácii na podozrivej platforme, ktorá od obetí žiadala osobné a finančné údaje, prípadne zaplatenie registračných poplatkov.

Zaznamenané boli aj prípady volaní od falošných vyšetrovateľov. Išlo o podvod, v ktorom sa útočníci vydávali za príslušníkov PZ a kontaktovali vopred vybrané obete s cieľom získania citlivých údajov a v úspešných prípadoch aj peňazí. Podvodníci kontaktovali ľudí s odôvodnením, že sa môžu stať obeťou úverového podvodu alebo že niekto v ich mene požiadal o úver, ktorému sa údajne snažia predísť. V zaznamenaných prípadoch sa podvodníci dožadovali osobných a bankových údajov. Aby zvýšili svoju dôveryhodnosť, obeti zaslali e-mail s fotografiami falošných policajných preukazov, prípadne s fotografiou podozrivej osoby, ktorá sa snažila vykonať úverový podvod. Hoci polícia evidovala aj úspešné prípady takýchto podvodov, NCKB vo viacerých prípadoch zaznamenalo obozretnosť potenciálnych obetí, za čo možno vďačiť neustálemu zvyšovaniu povedomia o podobnom type hrozieb, na ktorom sa aktívne podieľa NBÚ, policajný zbor ale aj komerčné spoločnosti, ktoré sú častým terčom impersonifikácie podvodníkov.

Incidenty vo verejnej správe a sieťovej infraštruktúre

Najdôležitejšou udalosťou štvrtého kvartálu 2025 bol sofistikovaný kybernetický útok, ktorý viedol ku kompromitácii systémov subjektu v sektore verejná správa. Na základe informácií o spôsobe vedenia útoku, získaných technickou a forenznou analýzou, možno túto aktivitu s vysokou dôveryhodnosťou asociovať s aktivitami skupiny podporovanej Ruskou federáciou. Incident bol včas odhalený a rýchla odozva zahŕňajúca úplnú izoláciu IT infraštruktúry od vonkajšieho internetu zabránila vážnejším následkom. Útočníkovi sa podarilo získať prihlasovacie údaje k legitímnej e-mailovej schránke. Platné prihlasovacie údaje boli následne zneužité na rozposlanie e-mailu so škodlivou prílohou špecificky zvolenej podmnožine zamestnancov. E-mailová správa aj príloha obsahovali sledovacie prvky, ktoré útočníkovi umožnili sledovať interakciu obetí a celý priebeh kampane. Príloha obsahovala Visual Basic makrá slúžiace na vytvorenie viacerých súborov a skriptov spúšťaných v pravidelných intervaloch pomocou plánovaných úloh. Po otvorení prílohy jedným z adresátov došlo ku kompromitácii pracovného zariadenia, ktoré aktér následne zneužil na prístup k ďalším serverom a laterálne šírenie po sieti.

V rámci vzájomnej výmeny informácií so zahraničnými partnermi bola sprostredkovaná informácia o kompromitovanom TP-Link routeri v rámci Slovenskej republiky. Celosvetovo malo ísť o viacero kompromitovaných zariadení v rôznych štátov. Aktér hrozby bližšie nešpecifikovaným spôsobom získal prihlasovacie údaje, ktoré zneužil na získanie prístupu do systému a vzdialené vykonanie kódu vedúceho k získaniu úplnej kontroly nad zariadením. Kompromitované zariadenia skupina primárne zneužívala ako súčasť anonymizačnej infraštruktúry na maskovanie svojej činnosti, ďalší prieskum sieťovej infraštruktúry alebo prienik do interných sietí.

Narušenie infraštruktúry škodlivého softvéru

Koncom septembra 2025 sa nemeckým OČTK v spolupráci s Europolom a Eurojustom v rámci medzinárodnej akcie Operation Endgame podarilo narušiť infraštruktúru škodlivého nástroja Rhadamanthys. Tento malvér sa špecializoval na zber a exfiltráciu citlivých údajov obetí, ako sú napríklad prihlasovacie údaje do rôznych služieb, bankové údaje alebo história webového prehliadania. Forenznou analýzou zaistených serverov sa podarilo identifikovať dodatočné údaje o samotných používateľoch služby a taktiež zoznam obetí, ktoré OČTK zdieľali s národnými jednotkami CSIRT.

Dátová sada prijatá NCKB obsahovala údaje, ktoré boli odcudzené z približne 900 zariadení aktívnych v kybernetickom priestore SR. Bližšou analýzou bolo identifikovaných približne 770 konkrétnych obetí zo Slovenska, ktorým boli zaslané adresné upozornenia na kompromitáciu zariadení a únik citlivých údajov, a taktiež aj odporúčania a kroky, ktoré je potrebné vykonať na zabezpečenie systémov a mitigáciu rizika zneužitia uniknutých údajov. Pri riešení incidentov tohto typu je dôležité vykonať zmenu všetkých prihlasovacích údajov, ktoré mohli uniknúť a vykonať reinštaláciu zariadenia.

Zneužívanie uvoľnených domén

V novembri NCKB identifikovalo aktéra, ktorý skupuje uvoľnené slovenské domény a umiestňuje na ne pornografický obsah. Ide o viac ako 30 domén s názvami slovenských obcí, e-shopov alebo známych ľudí, o ktoré už predchádzajúci majiteľ nemal záujem alebo za ne ďalej nezaplatil rezerváciu. Kampaň bola zaznamenaná aj v zahraničí, pričom aktér rovnakým spôsobom registroval uvoľnené domény aj v iných krajinách. Aktivity tohto aktéra zároveň poukazujú na riziká spojené s blížiacou sa exspiráciou webových domén. V prípade, že vlastník domény neuhradí registračný poplatok včas, môže doména po uplynutí registračného obdobia prejsť do registrácie iného záujemcu.

Neaktualizované IKT a IKT s ukončenou podporou

Za dlhodobú hrozbu možno označiť používanie neaktuálnych verzií softvérov v štátnych a vládnych organizáciách, v ktorých neboli opravené najnovšie objavené zraniteľnosti. Používaním starších a neaktuálnych verzií softvérov sa zvyšuje riziko ich kompromitácie potenciálnymi útočníkmi. NCKB v tomto kontexte upozorňovalo špeciálne na zastarané verzie webového redakčného systému WordPress a sieťové prvky dostupné z internetu. Tento trend potvrdzujú aj výsledky bezpečnostných skenov vládnej jednotky CSIRT. V hodnotenom období sa opakovane vyskytovali závažné nedostatky, ktoré neboli opravené ani po opakovaných upozorneniach. NBÚ sa tento problém snaží riešiť zvyšovaním bezpečnostného povedomia, a taktiež rozposielaním adresných varovaní na zraniteľné alebo nesprávne nakonfigurované zariadenia a systémy.

Iné významné udalosti

Politickým rozhodnutím sa v apríli 2025 program CVE, ktorý predstavuje medzinárodný štandard na evidenciu a identifikáciu kybernetických zraniteľností, ocitol v kritickej situácii v dôsledku rizika prerušenia financovania zo strany americkej agentúry CISA. Program spravovaný organizáciou MITRE je kľúčovým nástrojom pre koordinované zverejňovanie zraniteľností, keďže každému bezpečnostnému problému priraďuje unikátny identifikátor, ktorý umožňuje jeho jednotnú identifikáciu naprieč systémami a bezpečnostnými nástrojmi. CISA napokon kontrakt s MITRE dočasne predĺžila o jedenásť mesiacov, čím zabezpečila fungovanie programu do apríla 2026. Situácia poukázala na potrebu dlhodobej reformy a stabilného modelu správy programu CVE. Odborná komunita však upozorňuje, že ide len o dočasné riešenie a diskutuje sa o vytvorení nezávislej CVE Foundation, ktorá by mala zabezpečiť dlhodobú stabilitu a financovanie systému.

3. AKTÉRI HROZIEB

3.1. Štátom sponzorované skupiny

APT skupiny v roku 2025 pokračovali v realizácii operácií zameraných predovšetkým na kybernetickú špionáž, infiltráciu cieľových prostredí a systematický zber citlivých politických, technologických a ekonomických informácií. Pre SR predstavovali tieto aktivity hrozbu najmä pre štátnu správu, obranný a bezpečnostný sektor, energetiku, dopravu, výskumné inštitúcie a technologické spoločnosti. Slovensko je cieľom nielen priamych operácií, ale aj sekundárnych kompromitácií v rámci dodávateľských reťazcov a medzinárodných organizácií, ktorých je súčasťou. Zvlášť rizikové sú dlhodobé operácie a prieniky bez okamžitého viditeľného vplyvu, ktoré môžu zostať neodhalené mesiace až roky a byť aktivované v čase zvýšeného bezpečnostného napätia.

V roku 2025 sa prevažne ruské, čiastočne čínske a tiež APT skupiny prepojené na ďalšie krajiny zameriavali na inštitúcie štátnej správy, súkromné spoločnosti a subjekty kritickej infraštruktúry spadajúce do sféry ich záujmu a pôsobnosti. Okrem spearphishingových kampaní v snahe o kompromitáciu cieľových systémov využívali napr. aj techniky password spraying či manipuláciu s oprávneniami Microsoft Exchange. Na vykonávanie kybernetických útokov využívali aj známe aplikácie, ako sú WhatsApp, Signal, ale aj Microsoft Teams.

Ruská skupina vykonávala dlhodobú kampaň, ktorej cieľom boli západné logistické firmy, technologické spoločnosti a štátne inštitúcie, a subjekty podporujúce Ukrajinu. Časť kompromitovanej infraštruktúry bola identifikovaná aj v priestore SR.

NBÚ v spolupráci s partnermi v kybernetickom priestore identifikoval malvér, ktorý vykazoval známky totožné so širšou kampaňou vykonávanou ruskou APT skupinou v eurázijskom priestore. Malvér bol preventívnou činnosťou včasne identifikovaný, čím bol zamedzený vznik potenciálnych kompromitácií.

3.2. Hacktivistické skupiny

Aktivity hacktivistických skupín majú prevažne politický motív a často sú naviazané na geopolitické udalosti. V priestore SR dochádza v posledných rokoch k poklesu útokov týchto skupín. NBÚ identifikoval niekoľko typov jednotlivcov a skupín z domáceho aj zahraničného prostredia, ktorí vykonávali prevažne DDoS útoky voči inštitúciám SR, najmä z politického presvedčenia. Išlo hlavne o útoky vykonané na bankové inštitúcie a subjekty štátnej a verejnej správy. NBÚ identifikoval aj aktéra, ktorý aktívne vyhľadával zraniteľnosti na súkromných a štátnych slovenských webových stránkach so zámerom ich zneužitia pri budúcich útokoch.

3.3. Kyberkriminálne skupiny

Ransomvér predstavuje jeden z najzávažnejších problémov z pohľadu dopadu aktivít kybernetických kriminálnych skupín. Z dlhodobého hľadiska eviduje NBÚ nárast ransomvérových útokov v kybernetickom priestore SR. Kompromitácie systémov ransomvérom známych kriminálnych skupín boli identifikované u viacerých subjektov, od výroby, cez zdravotníctvo až po inštitúcie verejnej správy. Vo väčšine prípadov išlo o tradičný scenár, kedy boli obete požiadané o zaplatenie výkupného, aby im kriminálnici umožnili odšifrovanie systémov. Objavilo sa však aj niekoľko prípadov kompromitácií kriminálnych aktérov, ktoré zdieľali podobnosti s aktivitami APT skupín, čo by zodpovedalo narastajúcej spolupráci medzi štátnymi a kriminálnymi aktérmi pri určitých typoch útokov.

V priestore SR boli identifikovaní aj tzv. petty criminals a scam call centrá, ktoré sa zameriavali najmä na vykonávanie finančných podvodov voči jednotlivcom a menším organizáciám. Tieto skupiny využívajú kombináciu telefonických podvodov, SMS správ, e-mailov a falošných online reklám, pričom čoraz častejšie nasadzujú automatizované nástroje, skripty a umelú inteligenciu na zvýšenie objemu a presvedčivosti útokov.

Profesionalizácia a systematizácia aktivít kriminálnych skupín sa v posledných rokoch zintenzívňuje. Ich aktivity sa stávajú sofistikovanejšími a ťažšie odlíšiteľnými od legitímnej komunikácie, čo vedie k vyššej úspešnosti ich operácii. V roku 2025 sa objavili aj útoky typu pure data theft, ktoré pozostávajú z exfiltrácie dát, bez potreby ich šifrovania. Tento model sa čoraz častejšie objavuje v priemysle a službách, vrátane spoločností mimo kritickej infraštruktúry, a vytvára tlak na obete najmä v kontexte reputačných škôd a ohrozenia duševného vlastníctva.

4. ŠTATISTICKÝ PREHĽAD INCIDENTOV

NCKB v rámci svojej činnosti monitorovalo slovenský kybernetický priestor, zhromažďovalo a analyzovalo informácie z prijatých hlásení kybernetických bezpečnostných incidentov. Štatistické vyhodnotenie vychádza výlučne z prijatých hlásení KBI evidovaných NCKB. Tieto hlásenia sú prijímané rôznymi informačnými kanálmi ako telefonické hovory, e-mailové správy či prostredníctvom webového formulára. Primárnym bodom nahlasovania by však mal byť JISKB. Prípadné odchýlky v sledovaných údajoch je možné pripísať postupnému prechodu na hlásenia cez JISKB, ktorého používanie vyplýva zo ZoKB, a s tým spojeným nárastom aktivity subjektov v tomto systéme.

Typ nahláseného incidentu	Počet
Sociálne inžinierstvo	1067
Podozrenie na úspešný prienik do systému vrátane APT	126
Nedostupnosť (DoS, DDoS útok, sabotáž, výpadok služby)	106
Zraniteľnosť (ich existencia)	66
Škodlivý kód (vírus, malvér, ransomvér)	62
Vyhrážanie	42
Iné	41
Nevyžiadaná pošta (spam)	38
Pokus o prienik do systému	34
Neoprávnený prístup k informáciám, únik informácií, poškodenie informácií	32
Skenovanie siete	17
Podvod (neautorizované využitie prostriedkov, porušenia autorských práv)	15
Obťažovanie	4

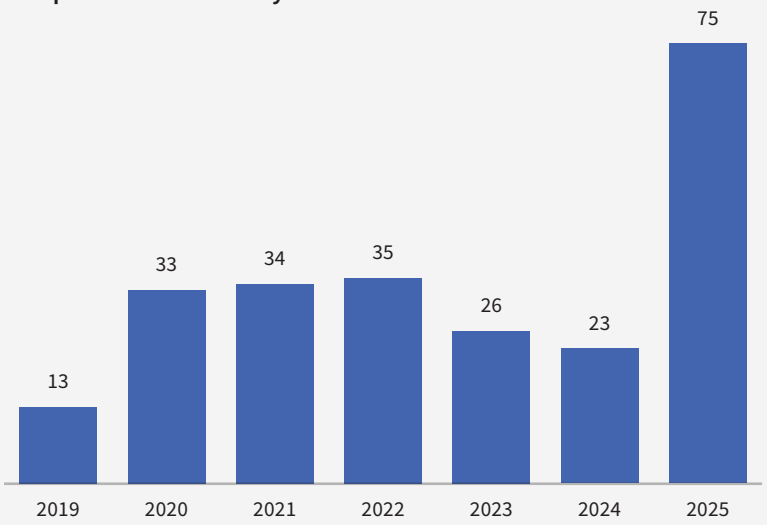
V roku 2025 výrazne dominovali útoky sociálneho inžinierstva s cieľom získať prístup k údajom či informačným systémom. Útočníci využívali presvedčivé techniky a s pomocou AI sa pokúšali zneužívať dôveru, nepozornosť a nedostatočné bezpečnostné povedomie používateľov.

V prípade útokov sociálneho inžinierstva sa ako najefektívnejší prístup dlhodobo považuje prevencia a proaktívne zvyšovanie bezpečnostného povedomia používateľov. NBÚ preto o aktuálnych kampaniach a hrozbách informuje prostredníctvom sociálnych sietí a webového sídla. Súčasťou preventívnych aktivít sú aj školenia a vzdelávacie aktivity zamerané na zvyšovanie bezpečnostného povedomia a schopnosti rozpoznať podvodné alebo manipulatívne aktivity.

Vývoj kybernetických bezpečnostných incidentov

Počet nahlásených incidentov dlhodobo rastie. V roku 2025 bolo nahlásených 1650 incidentov, čo v porovnaní s predchádzajúcim rokom predstavuje medziročný nárast približne o 40 %. Zvýšený počet hlásení však automaticky neznamená, že kybernetický priestor SR je nebezpečnejší. Je možné ho čiastočne pripísať legislatívnym zmenám, ktoré prirodzene viedli k zvýšeniu počtu regulovaných subjektov.

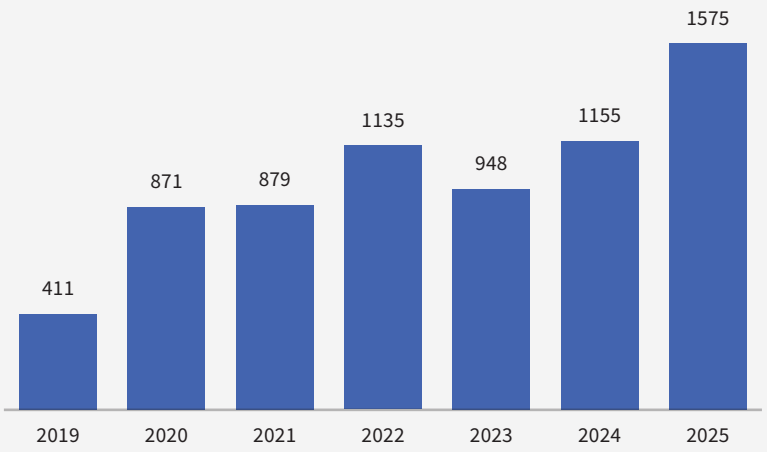
Závažné kybernetické bezpečnostné incidenty



Pri hláseniach dobrovoľných a závažných KBI je potrebné zohľadniť faktory, ktoré môžu ovplyvňovať ich počet, a to najmä prijatie legislatívy a už spomínané zvýšenie počtu regulovaných subjektov. V rámci závažných incidentov sú v období od roku 2019 – 2024 do analýzy zahrnuté všetky incidenty z kategórii I, II aj III. V dôsledku novely zákona o kybernetickej bezpečnosti účinnej v roku 2025 došlo k úprave metodiky hlásenia incidentov. Incidenty sa už nerozdeľujú do troch úrovní závažnosti, ale rozlišujú sa na závažné KBI hlásené na základe zákonnej povinnosti a incidenty nahlásené dobrovoľne. V roku 2025 sa v praxi naplno prejavili zmeny vyplývajúce z novely ZoKB. Počet dobrovoľných hlásení sa oproti predchádzajúcemu roku zvýšil približne o 36 %.

V predchádzajúcich rokoch počet hlásení závažných KBI nevykazoval jednoznačný rastúci trend, keďže povinné subjekty z dôvodu náročnosti presného kvantifikovania dopadu incidentu často uprednostňovali dobrovoľné hlásenia. Dobrovoľné hlásenia tak v praxi neraz zahŕňali aj incidenty, ktoré by vzhľadom na svoj charakter mohli byť klasifikované ako povinné.

Dobrovoľné hlásenia



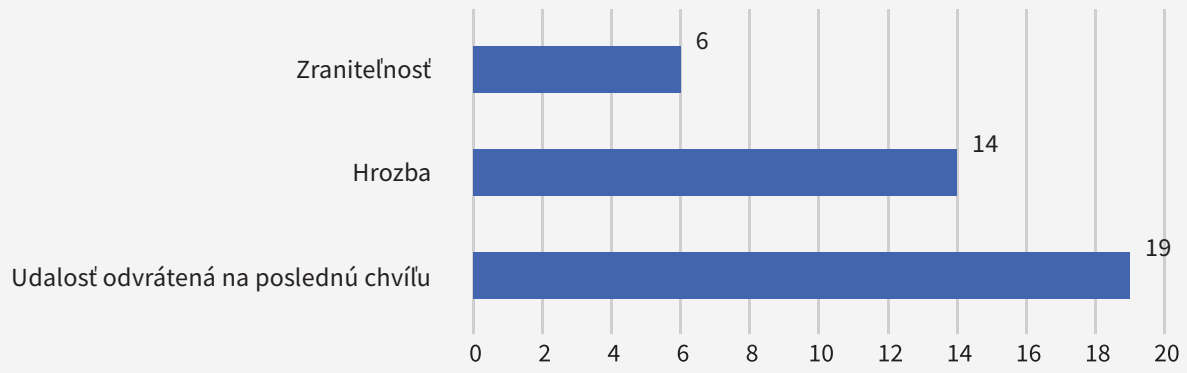
V oboch sledovaných rokoch bol v druhej polovici roka zaznamenaný nárast počtu hlásení kybernetických incidentov, pričom v roku 2025 je tento trend výraznejší.

Počet hlásených kybernetických bezpečnostných incidentov z časového hľadiska

Mesiac	2024	2025
Január	75	146
Február	77	119
Marec	82	123
Apríl	103	120
Máj	92	136
Jún	117	135
Júl	100	154
August	91	131
September	101	170
Október	119	173
November	116	138
December	105	102

Podľa ZoKB sa prostredníctvom systému JISKB hlásia aj ďalšie dôležité udalosti. Ide o významnú kybernetickú hrozbu, o ktorej sa subjekt dozvie; udalosť, ktorá mohla spôsobiť závažný KBI, no bola odvrátená na poslednú chvíľu; ako aj zraniteľnosť, ktorá môže byť zneužitá na spôsobenie závažného kybernetického bezpečnostného incidentu a ktorú subjekt nemohol v primeranom čase odstrániť alebo zmierniť prijatím vhodných opatrení.

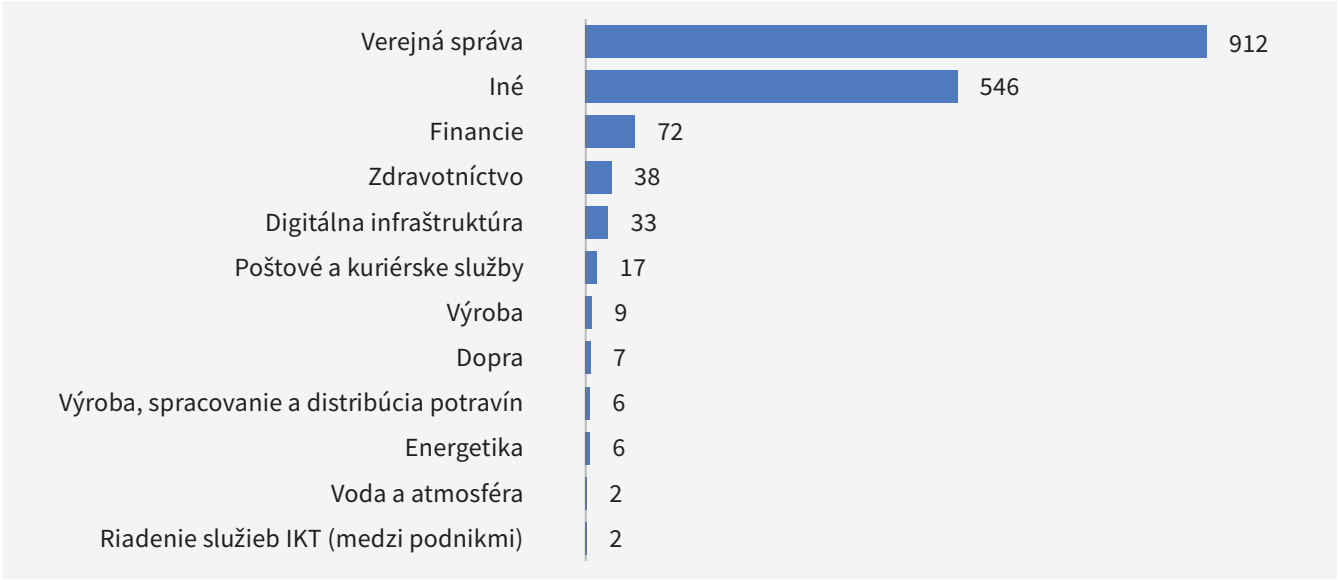
Počet hlásených kybernetických bezpečnostných incidentov z časového hľadiska



5. KYBERNETICKÁ BEZPEČNOSŤ V SEKTOROCH

5.1. Hlásenia kybernetických bezpečnostných incidentov podľa sektorov

Prehľad výskytu kybernetických bezpečnostných incidentov v jednotlivých sektoroch vychádza z analýzy hlásených incidentov NCKB. Počet hlásených incidentov sa medzi sektormi výrazne líši, čo poukazuje na rozdielnu mieru organizačnej zrelosti, úroveň bezpečnostných opatrení a regulačného rámca, ako aj na rozdielnu mieru investícií do kybernetickej bezpečnosti. V sektoroch odpadové hospodárstvo, poskytovatelia digitálnych služieb, vesmír, výroba a distribúcia chemických látok a výskum, neboli v sledovanom období zaznamenané žiadne hlásené incidenty.



5.2. Stav súladu s požiadavkami zákona o kybernetickej bezpečnosti

Audity kybernetickej bezpečnosti slúžia na overenie plnenia povinností podľa ZoKB a na posúdenie zhody prijatých bezpečnostných opatrení s požiadavkami ZoKB, jeho vykonávacích predpisov, ako aj s požiadavkami osobitných predpisov v oblasti kybernetickej bezpečnosti. Tie sa vzťahujú na bezpečnosť sietí a informačných systémov prevádzkovateľa základnej služby, ako aj na prostriedky podporujúce poskytovanie týchto služieb.

Cieľom auditu je overiť dosahovanie požadovanej úrovne kybernetickej bezpečnosti, identifikovať nedostatky pri zabezpečovaní ochrany sietí a informačných systémov, a navrhnúť opatrenia na ich odstránenie s cieľom predchádzať kybernetickým bezpečnostným incidentom.

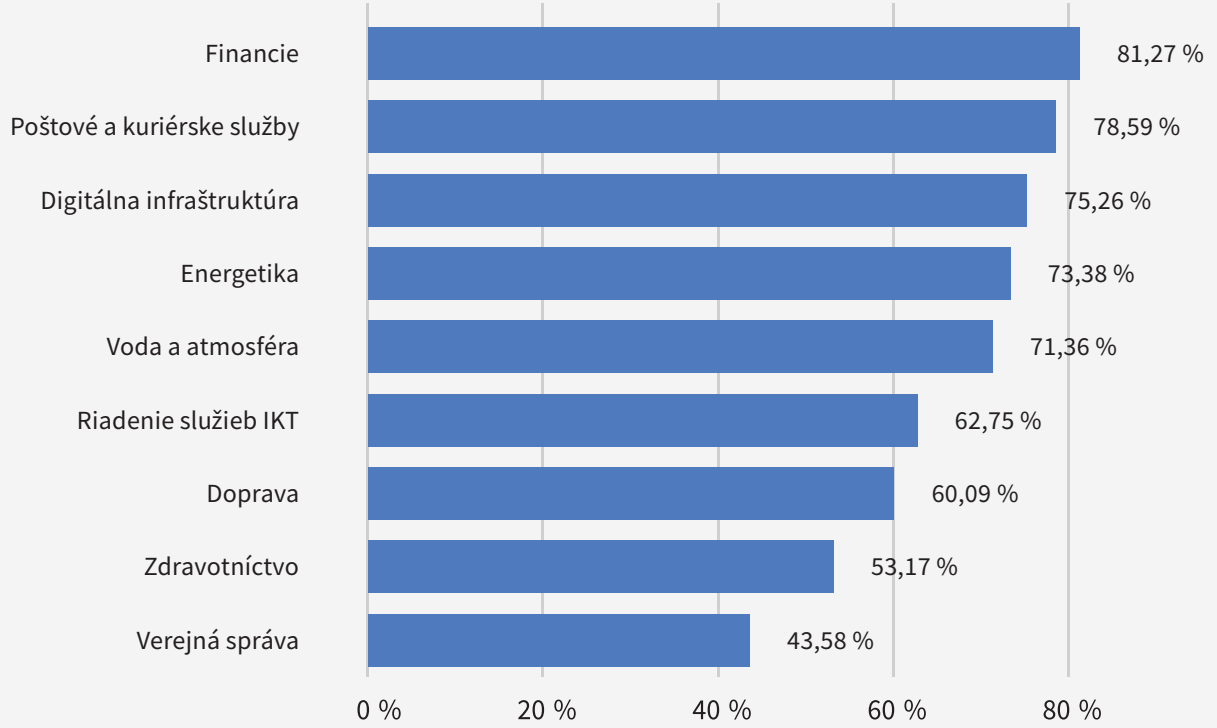
Z metodologického hľadiska je prehľad zistení z auditných správ založený na priemernej miere súladu, pričom využitie absolútnych čísel je v tomto kontexte obmedzené. Počty auditovaných subjektov v jednotlivých sektoroch sa medziročne menia, čo súvisí s dvojročným cyklom povinných auditov. V rámci jedného kalendárneho roka tak auditné správy predkladá len určitá časť subjektov. V roku 2025 bolo NBÚ doručených 112 auditných správ a 673 samohodnotení od prevádzkovateľov základnej služby, ktorí využili prechodné ustanovenie § 34b ods. 8 a 9 ZoKB.

Sektor	Počet doručených auditných správ
Verejná správa	51
Zdravotníctvo	22
Energetika	14
Digitálna infraštruktúra	8
Doprava	5
Financie	5
Voda a atmosféra	4
Poštové a kuriérske služby	2
Riadenie služieb IKT	1

Vplyv novej vyhlášky NBÚ č. 227/2025 Z. z. o bezpečnostných opatreniach, ktorá nadobudla účinnosť 01.09.2025, bude možné vyhodnotiť až po roku 2027. Od tohto obdobia budú všetky subjekty povinne prijímať bezpečnostné opatrenia výlučne podľa tejto vyhlášky. Novozaradené subjekty budú postupne podliehať prvým auditom kybernetickej bezpečnosti.

V roku 2025 bolo vplyvom novely ZoKB do registra prevádzkovateľov základnej služby novozaradených 1486 subjektov.

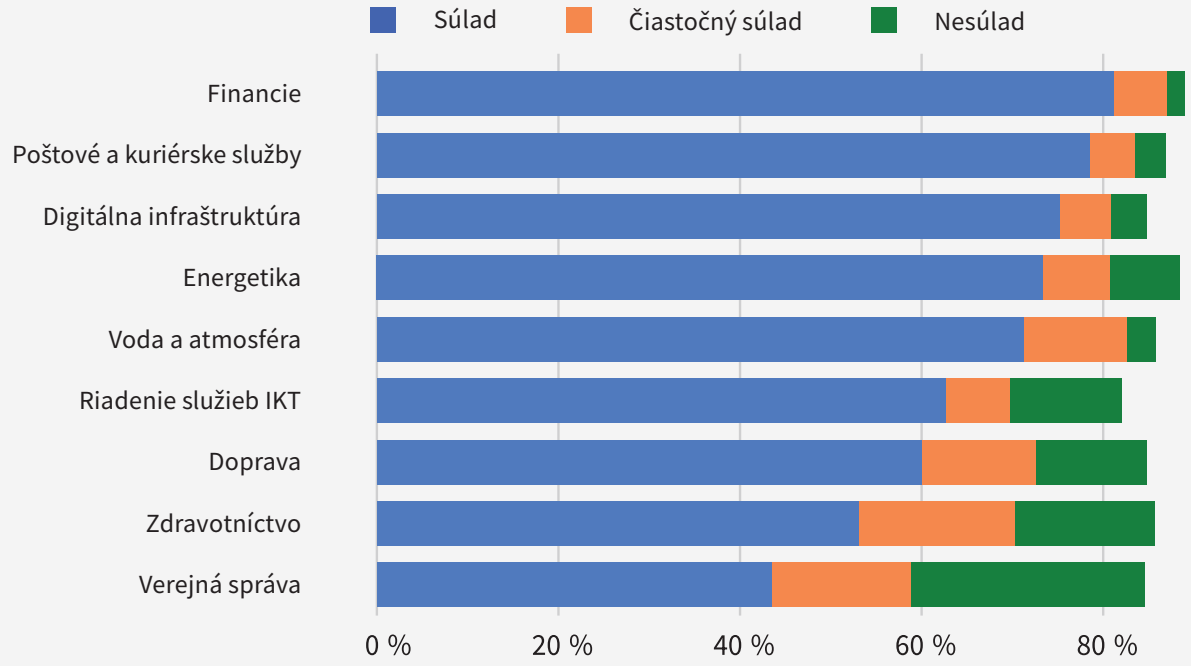
Porovnanie sektorov z hľadiska priemernej miery súladu v percentách



Porovnanie sektorov z hľadiska celkovej priemernej percentuálnej miery súladu poskytuje prehľad o úrovni plnenia požiadaviek kybernetickej bezpečnosti v jednotlivých sektoroch a umožňuje identifikovať rozdiely v miere implementácie bezpečnostných opatrení, ako aj potenciálne oblasti vyžadujúce ďalšie zlepšenie.

Prehľad auditných zistení v jednotlivých sektoroch prináša porovnanie úrovne súladu, čiastočného súladu a nesúladu, pričom poukazuje na výraznú prevahu súladu v auditných zisteniach naprieč jednotlivými sektormi.

Stav súladu v sektoroch



V rámci dohľadovej činnosti bolo vykonaných 19 kontrol u prevádzkovateľa základnej služby, pričom kontrolné zistenia boli zistené u 14 prevádzkovateľov základnej služby. K februáru 2026 neboli ukončené kontroly v štyroch subjektoch, ktoré boli začaté v roku 2025.

Najčastejšie kontrolné zistenia spočívali v nedostatočnej úprave vzťahu s treťou stranou, najmä absencia analýzy rizík dodávateľského vzťahu. Opakovane bolo identifikované, že prevádzkovatelia základnej služby nevykonávali bezpečnostný monitoring alebo mali implementovaný nástroj na bezpečnostný monitoring, ktorý však nebol riadený a výstupy z neho neboli vyhodnocované.

5.3. Stav kybernetickej bezpečnosti v sektoroch na základe prieskumu Najvyššieho kontrolného úradu SR

V prvej polovici roku 2025 realizoval Najvyšší kontrolný úrad SR dotazníkový prieskum o stave, manažmente a financovaní kybernetickej bezpečnosti u vybraných prevádzkovateľov základnej služby. V rámci prieskumu bolo oslovených 110 subjektov, pričom odpovede poskytlo 97 subjektov. Do prieskumu boli zaradené organizácie z viacerých sektorov (energetika, financie, zdravotníctvo, doprava, verejná správa, digitálna infraštruktúra a iné), a napriek tomu, že neobsahuje celé spektrum subjektov má vzhľadom na návratnosť vysokú informačnú hodnotu.

Prieskum priniesol viaceré zaujímavé zistenia, pričom niektoré z nich sa často opakujú u väčšiny subjektov. Z faktorov, ktoré ovplyvňujú stav kybernetickej bezpečnosti, boli najvýraznejšími nedostatok ľudí a finančných prostriedkov, nejednotnosť regulačného prostredia a potreba napĺňania vyšších požiadaviek bez zabezpečenia systémovej schémy financovania. Spoločným zistením v oblasti koordinácie, riadenia IT a digitalizačných projektov bolo, že napriek vyžadovaniu ukazovateľov výkonnosti, ich merateľnosť často nie je správne nastavená a subjekty vykazujú ich naplnenie na úrovni orientačných odhadov, čo znemožňuje efektívne vyhodnotenie a kvalifikované riadenie. Ako pozitívny aspekt je možné považovať fakt, že väčšina opýtaných má zavedené základné procesy a opatrenia a uvedomuje si dôležitosť kybernetickej bezpečnosti. Zistenia vo viacerých špecifických oblastiach, na ktoré sa prieskum zameral v kombinácii s výsledkami auditov a samohodnotení dávajú ucelenejší obraz o prístupe verejných a súkromných organizácií ku kybernetickej bezpečnosti, ale tiež odhaľujú niektoré nedostatky a problémy.

Financovanie

V oblasti financovania kybernetickej bezpečnosti, približne polovica respondentov nedisponuje samostatným rozpočtom na kybernetickú bezpečnosť oddeleným od IT. Výraznejšie oddelenie rozpočtov je možné pozorovať najmä vo väčších organizáciách verejnej správy a v sektore energetiky. Pozitívnym trendom je, že až 78 % opýtaných subjektov plánuje v najbližších rokoch navýšenie finančných prostriedkov v oblasti kybernetickej bezpečnosti. Pretrvávajúcim problémom však zostáva nedostatočná transparentnosť vo finančnom plánovaní prostriedkov na kybernetickú bezpečnosť a vysoká miera závislosti od externých zdrojov. To v konečnom dôsledku vedie k neudržateľnosti systémového financovania, a tiež znižuje porovnateľnosť medzi jednotlivými subjektmi.

Máte samostatne rozpočtované prostriedky na kybernetickú bezpečnosť?

Áno	25 %
Nie	29 %
Nevieme odčleniť od rozpočtu na IT	46 %

Onboarding

Ľudský faktor predstavuje v oblasti kybernetickej bezpečnosti jedno z najvýznamnejších rizík, pričom viac ako polovica subjektov nedisponuje systematicky zavedenými procesmi pre prehodnocovanie rizík spojených s nástupom nových zamestnancov. Základné preverenie bezúhonnosti pracovníkov je pomerne rozšírené, avšak komplexné procesy pri nástupe nových zamestnancov a pravidelné prehodnocovanie rizík zostávajú skôr výnimkou než štandardom.

Máte pravidlá určujúce proces preverovania personálneho rizika pri onboardingu?

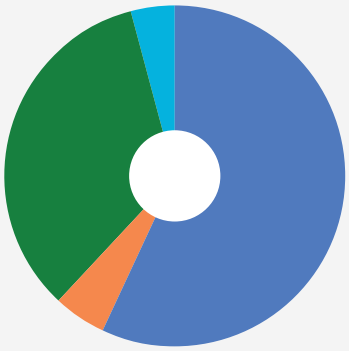
Áno	40 %
Nie	60 %

Interné vzdelávanie o kybernetickej bezpečnosti

Interné vzdelávanie v oblasti kybernetickej bezpečnosti síce v organizáciách prebieha, avšak často v nedostatočnom rozsahu a intenzite. Celkové výsledky naznačujú, že školenia sú stále vnímané skôr formálne, než ako kľúčový nástroj budovania odolnosti organizácie. Výrazné rozdiely medzi sektormi poukazujú na absenciu jednotného metodického usmernenia a nedostatočne rozvinutú kultúru kybernetickej bezpečnosti. Zatiaľ čo vo viacerých sektoroch pôsobia výsledky nevyrovnane, sektor energetiky vykazuje najvyššiu mieru systematického a zodpovedného prístupu.

Ako často prebiehajú školenia zamestnancov v oblasti kybernetickej bezpečnosti?

Raz ročne	57 %
Raz za polrok	5 %
Len pri nástupe / podľa potreby	34 %
Vôbec	4 %

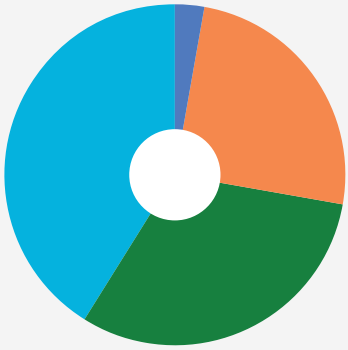


Využívanie AI

Využívanie AI uviedlo približne 25 % opýtaných subjektov, pričom najpokročilejší je sektor financií. V praxi ide najmä o aplikácie založené na AI, ako sú chatboty, dátová analytika či veľké jazykové modely (LLM). V ostatných sektoroch je jej nasadzovanie prevažne fragmentované a často len na experimentálnej úrovni. Pri využívaní AI subjekty kladú skôr dôraz na monitorovanie a dodržiavanie legislatívneho rámca než na reálnu implementáciu bezpečnostných opatrení na elimináciu rizík spojených s používaním AI.

Využívate vo Vašej organizácii AI aplikácie?

Áno, vo viacerých procesoch	3 %
Áno, ale len v obmedzenom rozsahu	25 %
Nie, zvažujeme	31 %
Nie	41 %



Plán reakcie na KBI

Najvyššiu úroveň pripravenosti, vrátane existencie a reálneho využívania plánov reakcie na incidenty a cvičení, vykazuje sektor financií. Relatívne lepšiu úroveň možno pozorovať aj v doprave a čiastočne v energetike, kde sa zároveň systematickejšie uplatňuje primárna prevencia, napríklad bezpečnostné testovania a riadenie zraniteľností. Naopak, zdravotníctvo, verejná správa a sektory voda a atmosféra vykazujú nižšiu úroveň systematického prístupu, najmä v oblasti pravidelných cvičení a konzistentného testovania. Hoci formálnym plánom reakcie na KBI disponuje približne 66 % opýtaných subjektov, jeho praktické uplatňovanie zostáva otázne.

Máte formálny plán reakcie na kybernetické incidenty?

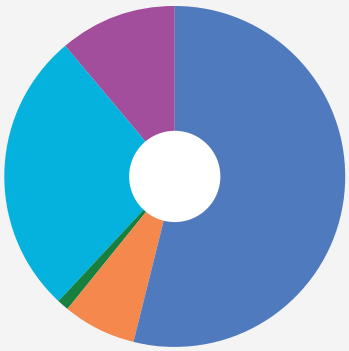
Áno	66 %
Nie	34 %

Riadenie rizík a kontinuita činností

Väčšina opýtaných subjektov disponuje metodikou riadenia rizík, avšak nástroje kontinuity činností, ako plán kontinuity činností (Business Continuity Management) a plán obnovy (Disaster Recovery Plan), sú často zamerané výlučne na IT oblasť. Krízový komunikačný plán má zavedený približne polovica subjektov. Pozitívnym zistením je, že väčšina subjektov pravidelne aktualizuje register rizík.

Ako často aktualizujete register rizík?

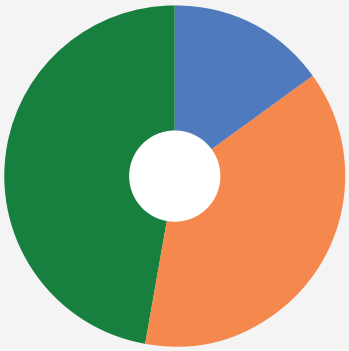
Raz ročne	54 %
Dvakrát ročne	7 %
Štvrťročne	1 %
Ad hoc	27 %
Nevedieme register rizík	11 %



Riadenie rizík a plánovanie kontinuity činností sú pritom dôležité procesné nástroje pre rýchlu obnovu kľúčových činností počas krízových situácií. Z hľadiska sektorového porovnania vykazuje najvyššiu úroveň implementácie sektor financií, spolu s energetikou a digitálnou infraštruktúrou. Na strednej úrovni sa nachádzajú doprava a verejná správa, ktorých výsledky sú nevyrovnané, zatiaľ čo zdravotníctvo a sektor voda a atmosféra patria medzi najslabšie, pričom v nich prevažuje skôr formálny prístup nad funkčným.

Máte zavedený plán kontinuity činností?

Áno, pre všetky kľúčové procesy	15 %
Áno, len pre časť IT	38 %
Nie, zvažujeme	47 %

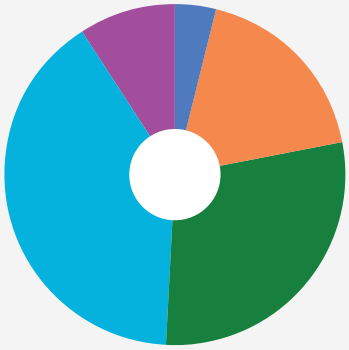


Bezpečnosť údajov a zálohovanie

Napriek tomu, že subjekty zálohujú, bezpečnosť a spoľahlivosť záloh je otázna. Zálohovanie je v mnohých prípadoch vnímané skôr ako technický proces než opatrenie kybernetickej bezpečnosti. Výsledky poukazujú na to, že hoci je technologická infraštruktúra na zálohovanie vo väčšine organizácií zavedená, procesy a disciplína pri jej využívaní sú často nedostatočné. V prípade rozsiahlejšieho KBI by veľká časť organizácií nemusela byť schopná obnoviť svoju prevádzku včas a spoľahlivo. Prieskum poukázal na fakt, že iba málo organizácií pravidelne testuje použiteľnosť záloh na obnovu systému.

Ako často testujete obnovu dát zo zálohy?

Raz za mesiac	4 %
Raz za štvrťrok	18 %
Raz za rok	29 %
Iné	40 %
Nikdy	9 %



Bezpečnosť dodávateľského reťazca

Analýza poukazuje na to, že najslabším sektorom v oblasti dodávateľského riadenia je zdravotníctvo, kde často absentujú certifikácie aj systematické hodnotenie rizík. Verejná správa vykazuje výraznú nejednotnosť, niektoré subjekty disponujú vyspelými procesmi zatiaľ čo u iných absentujú základné nastavenia. Naopak, medzi najsilnejšie sektory patria energetika a financie, ktoré systematicky uplatňujú certifikácie, zmluvné požiadavky a disponujú zavedenými procesmi eskalácie. Sektory doprava a voda síce pracujú s vysokým počtom dodávateľov, avšak nedostatky eskalačných mechanizmov zvyšujú ich celkovú rizikovosť. Sektory digitálna infraštruktúra a vesmír vykazujú vyššiu úroveň pripravenosti, najmä v oblasti riadenia väčšieho počtu dodávateľov.

6. HODNOTENIE STAVU KYBERNETICKEJ BEZPEČNOSTI ZO STRANY ÚSTREDNÝCH ORGÁNOV

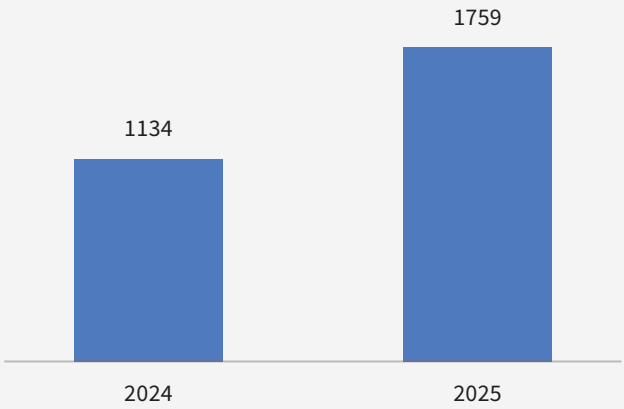
6.1. Stav v sektoroch z pohľadu ústredných orgánov

6.1.1 Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky

I. Vnímanie hrozieb a rizík v roku 2025

V roku 2025 VJ CSIRT, pôsobiaca v rámci MIRRI, zaznamenala až 55 % nárast počtu incidentov v porovnaní s predošlým rokom. Medzi hlavné hrozby patrili sociálne inžinierstvo a phishing (vrátane ich automatizovaných foriem podporených umelou inteligenciou), ktoré často slúžia ako vstupný vektor útoku. Ďalej to boli ransomvérové kampane, škodlivý kód, zneužívanie známych zraniteľností a útoky typu DDoS, ktoré predstavujú významné riziko pre organizácie vo verejnej správe.

Počet incidentov riešených CSIRT.SK [2]



II. Čo považujete za najväčšie riziko pre vašu oblasť?

Jedným z najvýznamnejších identifikovaných rizík je pretrvávajúci falošný pocit bezpečnosti, ktorý môže viesť k podceneniu aktuálnych hrozieb a k nedostatočnej priorizácii bezpečnostných opatrení. Tento stav sa často prejavuje absenciou systematického a dlhodobo udržateľného prístupu k riadeniu kybernetickej bezpečnosti na úrovni organizácie, ktorý je realizovaný prevažne reaktívnym spôsobom. Organizáciám chýba ucelená bezpečnostná stratégia, jasne definovaný rámec riadenia rizík, ako aj prepojenie technických, procesných a organizačných opatrení. Zavádzané kontrolné mechanizmy sú často izolované, bez pravidelného vyhodnocovania ich efektívnosti a bez väzby na celkový rizikový profil organizácie a na jej biznis procesy. Z dlhodobého hľadiska takýto nesystematický prístup zvyšuje pravdepodobnosť vzniku bezpečnostných incidentov a obmedzuje schopnosť organizácie včas identifikovať, analyzovať a primerane reagovať na meniace sa kybernetické hrozby.

[2] Štatistika obsahuje incidenty, ktoré boli hlásené VJ CSIRT

Napriek technologickému pokroku a implementácii rôznych bezpečnostných nástrojov zostáva najčastejším a najviac zneužívaným vektorom kybernetických útokov ľudský faktor. Používatelia predstavujú kritický prvok bezpečnostného reťazca. Ich správanie má priamy vplyv na celkovú úroveň bezpečnosti organizácie. Nedostatočne nastavené alebo nepravidelné vzdelávanie v oblasti kybernetickej bezpečnosti zvyšuje riziko kompromitácie prístupových údajov, neoprávneného prístupu k informačným systémom a úniku citlivých údajov.

Systém riadenia zraniteľností je vo viacerých organizáciách riadený nesystematickým a nejednotným spôsobom. Procesy zamerané na identifikáciu, hodnotenie, priorizáciu a odstraňovanie zraniteľností nie sú definované ani formálne ukotvené v interných politikách a postupoch. Nesystematické riadenie zraniteľností zvyšuje pravdepodobnosť úspešného zneužitia zo strany útočníkov. Vďaka registrácii organizácií do systému plošného hodnotenia zraniteľností VJ CSIRT, Achilles, je možné odoberať informácie o známych zraniteľnostiach detegovaných na prvkoch dostupných z internetu.

III. Ako hodnotíte aktuálnu úroveň kybernetickej bezpečnosti vo vašej oblasti/sektore?

Úroveň kybernetickej bezpečnosti vo verejnej správe nie je možné zovšeobecniť, medzi jednotlivými inštitúciami sa výrazne líši. Kým niektoré organizácie jej venujú systematickú pozornosť, iné k nej pristupujú prevažne formálne alebo nedostatočne. Tieto rozdiely sa odrážajú najmä v kvalite technického zabezpečenia, úrovni modernizácie infraštruktúry, efektívnosti riadenia bezpečnostných aktualizácií, dôslednosti uplatňovania bezpečnostných princípov, ako aj v oblasti vzdelávania zamestnancov a vzdelanostnej úrovne zamestnancov v oblasti kybernetickej a informačnej bezpečnosti. Medzi ďalšie veľké slabiny patrí nedostatok komunikácie smerom k VJ CSIRT poskytujúcej služby, ktoré môžu organizácie využívať na zvýšenie úrovne svojej kybernetickej bezpečnosti.

IV. Aktivity realizované v roku 2025

Jednou z priorít sekcie kybernetickej bezpečnosti bolo vzdelávanie, najmä zriadenie a koordinácia šiestich kompetenčných centier kybernetickej bezpečnosti na vysokých školách, ktoré sa zameriavajú na zvyšovanie odbornosti zamestnancov verejnej správy a vyškolenie manažérov kybernetickej bezpečnosti. Bolo spustené špecializované technicko-expertízne laboratórium, ktoré významne posilní technické možnosti VJ CSIRT v oblasti hardvérovej bezpečnosti, forenznej a dátovej analýzy. S cieľom podporiť súlad verejnej správy s legislatívou bolo zabezpečené dodanie dokumentácie Jednotného metodického rámca. Zároveň prebiehala spolupráca na novele zákona o ITVS, ktorá upravuje naviazané ustanovenia ZoKB. Bol iniciovaný legislatívny proces novelizácie vyhlášky o obsahu bezpečnostných opatrení pre subjekty verejnej správy využívajúce ITVS. Taktiež bol implementovaný Systém včasného varovania na viacerých orgánoch verejnej moci, ktoré boli pripojené k SOC MIRRI. Prebiehala príprava Národného projektu kybernetickej a informačnej bezpečnosti pre obce do 6-tisíc obyvateľov zameraného na posilnenie kybernetickej bezpečnosti. V oblasti osvety sa uskutočnilo osem konferencií, na ktorých boli predstavené riešenia, plány a novinky z oblasti kybernetickej bezpečnosti pre zamestnancov verejnej správy. Zároveň sa MIRRI zameriavalo na kontrolnú činnosť dodržiavania ustanovení zákona o ITVS a mnohé iné aktivity.

Medzi proaktívne aktivity jednotky CSIRT.SK patrí systém Achilles, určený na pravidelné, neinvazívne skenovanie a overovanie zraniteľností verejne dostupných služieb a zariadení IT infraštruktúry organizácií prístupných z internetu. Do tohto programu bolo zapojených 341 organizácií, čo predstavuje medziročný nárast o 21 % oproti roku 2024. Do služby Afrodita, zameranej na prevenciu, detekciu a zdieľanie indikátorov kompromitácie, sa zapojilo sedem organizácií, pričom dve z nich disponujú vlastným SOC. Táto služba je kľúčová, keďže predstavuje jednotné kontaktné miesto pre výmenu informácií o činnostiach aktérov hrozieb, preto je dôležité do nej prispievať vlastnými vstupmi, ako aj využívať existujúce. V prevádzke bol zároveň aj systém Domino, ktorý slúži na monitorovanie dostupnosti vybraných webových domén. V priebehu roka 2025 vykonala VJ CSIRT v rámci služby ARES celkovo 16 penetračných testov. VJ CSIRT sa významne zameriavala aj na vzdelávacie aktivity, ako napr. Kyberaréna, v ktorej absolvovalo odborné školenia viac ako 120 technických pracovníkov a IT špecialistov verejnej správy. Popri odborných školeniach organizovala VJ CSIRT edukačné prednášky zamerané na kybernetickú a informačnú bezpečnosť.

Najvýznamnejšie incidenty, ktoré riešila VJ CSIRT zahŕňali ransomvérový útok na ÚGKK, ale aj útoky typu DDoS na rôzne webové služby a bruteforce e-mail bombing na viacero štátnych organizácií, VšZP, LESY SR š.p., MV, Ústavný súd SR. Evidované boli aj výhražné e-maily adresované slovenským univerzitám a závažný bezpečnostný incident na MH.

6.1.2 Ministerstvo vnútra Slovenskej republiky

I. Vnímanie hrozieb a rizík v roku 2025

Situáciu v roku 2025 ovplyvnila najmä legislatívna zmena, predovšetkým implementácia smernice NIS2 a prijatie vyhlášky NBÚ č. 227/2025 Z. z., ktorá zvýšila požiadavky na zabezpečenie systémov verejnej správy a ich odolnosť. Došlo taktiež k rozšíreniu pôsobnosti a kompetencií MV v oblasti kybernetickej bezpečnosti, keďže sa stalo ústredným sektorovým orgánom pre tri sektory – digitálna infraštruktúra, verejná správa a vesmír. V roku 2025 boli ako najvážnejšie identifikované ransomvérové útoky na štátne organizácie. Z pohľadu počtu hlásených incidentov od zamestnancov MV došlo medziročne k poklesu, čo pravdepodobne súvisí s nasadením ochrany koncových zariadení. Za rok 2025 boli zaznamenané celkovo dva DDoS útoky.

II. Čo považujete za najväčšie riziko pre vašu oblasť?

Za najväčšie riziko v oblasti kybernetickej bezpečnosti rezortu MV sa považuje kombinácia troch faktorov: prepojenosť informačných systémov verejnej správy a vysoké požiadavky na ich dostupnosť, rýchlo sa meniace hrozby a obmedzené odborné kapacity. Prepojenosť systémov zvyšuje pravdepodobnosť, že incident zasiahne viacero služieb súčasne, pričom staršie IS sú zaťažené technologickým dlhom. Zároveň rastie riziko ransomvérových útokov a pokusov o kompromitáciu digitálnej identity používateľov a rastúce využívanie AI útočníkmi zvyšuje nároky na efektívnu ochranu. Dôležitým rizikom je aj vznik nových zraniteľností, ktoré si vyžadujú permanentné monitorovanie a včasné prijímanie nápravných opatrení. Pretrvávajúcim rizikom je nedostatok odborných pracovníkov na trhu práce a ich nedostatočné finančné ohodnotenie, čo znižuje schopnosť dlhodobo udržať rastúce požiadavky na prevádzku a riešenie incidentov.

III. Ako hodnotíte aktuálnu úroveň kybernetickej bezpečnosti vo vašej oblasti/sektore?

Úroveň kybernetickej bezpečnosti v rezorte MV v roku 2025 možno hodnotiť ako postupne sa zlepšujúcu. Došlo k zvýšeniu ochrany a bezpečnosti koncových zariadení a sietí vďaka zavedeniu nových bezpečnostných nástrojov a postupnej implementácii centrálneho monitorovacieho riešenia, do ktorého boli postupne zapájané prvky infraštruktúry. Zlepšila sa schopnosť riešiť bezpečnostné incidenty aj vďaka automatizácii reakcií, skrátil sa reakčný čas. Kapacity bezpečnostného tímu sa posilnili účasťou na medzinárodných cvičeniach a pravidelným odborným vzdelávaním. Boli zavedené účinnejšie nástroje na skenovanie zraniteľností. V súvislosti s novou legislatívou kybernetickej bezpečnosti boli aktualizované interné smernice, postupy a procesy. V roku 2025 bol zabezpečený 24/7 kontakt na nahlasovanie incidentov.

IV. Aktivity realizované v roku 2025

Zamestnanci MV sa v roku 2025 priamo podieľali na riešení incidentu na kataster, po ktorom sa na základe poznatkov implementovali nové bezpečnostné opatrenia. Dôležitou súčasťou preventívnych aktivít bola oblasť vzdelávania vyvinutá vlastnými kapacitami bez nároku na rozpočet. Kurz Základy kybernetickej bezpečnosti absolvovalo 29 920 zamestnancov a kurz Návody a upozornenia ďalších 707. Pre správcov IKT bol určený odborný kurz, v ktorom bolo vyškolených 364 osôb. Okrem toho rezort zorganizoval konferenciu Cyber Security Days. Zamestnanci sa počas roka 2025 zúčastnili odborných kurzov organizovaných Univerzitou Komenského. Tieto aktivity predstavovali významný krok smerom k zvyšovaniu povedomia aj odbornosti v rezorte. V roku 2025 sa vykonávali audity v oblasti kybernetickej bezpečnosti, hodnotenia bezpečnosti informačných systémov a posilňovali sa personálne a materiálne kapacity.

6.1.3 Ministerstvo obrany Slovenskej republiky

I. Vnímanie hrozieb a rizík v roku 2025

V súvislosti s neustále sa meniacim bezpečnostným prostredím bol zaznamenaný výrazný nárast škodlivých činností rôznych hacktivistických skupín zameriavajúcich sa na subjekty súkromného aj verejného sektora. Ich činnosti sú zamerané od útokov s cieľom DDoS, pokusy o zneužívanie prihlasovacích údajov až po ransomvérové útoky a demonštráciu možnosti ovládania nedostatočne zabezpečených priemyselných rozhraní, ktoré sú dostupné zo siete internet. V rámci pôsobenia sofistikovaných kybernetických aktérov, štátnych alebo štátom podporovaných, bol zaznamenaný vývoj taktík, techník a metód využívaných pri kybernetických operáciách. Posun týchto aktérov do oblasti využívania umelej inteligencie pri tvorbe škodlivého kódu alebo zvýšení úrovne automatizácie a obchádzaniu bezpečnostných prvkov prináša výzvy na poli kybernetickej obrany a ochrany informačných systémov.

II. Čo považujete za najväčšie riziko pre vašu oblasť?

Z pohľadu sektora obrany je možné konštatovať že SR ako členská krajina NATO a EÚ je už tradičným predmetom záujmu štátnych aktérov vykonávajúcich operácie v kybernetickom priestore, ktoré ohrozujú národné záujmy SR, ako aj bezpečnostné záujmy NATO a EÚ. Okrem už tradičných zdrojov hrozieb v podobe štátnych aktérov bol rok 2025 pre sektor obrany významným zdrojom hrozieb ozbrojený konflikt na Ukrajine a s tým spojená nestabilita v medzinárodnom prostredí, činnosť APT skupín zameraná voči vojenským a ekonomický záujmom SR, ako aj rozsiahle používanie zastaraných technológií v produkčných častiach informačných systémov v kybernetickom priestore.

III. Ako hodnotíte aktuálnu úroveň kybernetickej bezpečnosti vo vašej oblasti/sektore?

VS v rámci rezortnej a mimorezortnej spolupráce zaznamenáva výrazný posun nielen v oblasti bezpečnostného povedomia technického a používateľského personálu, ale zároveň aj v schopnostiach relatívne rýchlo a efektívne reagovať aj na novovzniknuté kybernetické hrozby. Realizovaná spolupráca, napríklad v prípade incidentu v infraštruktúre ÚGKK, poukázala na vysokú mieru flexibility a expertnej úrovne. Priebežná inovácia technológií a odborný rozvoj personálu umožňujú v dostatočnej miere reagovať aj na stále nové techniky využívané kybernetickými aktérmi.

IV. Aktivity realizované v roku 2025

VS na základe žiadostí iných orgánov ústrednej štátnej správy poskytlo pomoc pri riešení kybernetických incidentov v komunikačnej a informačnej infraštruktúre ich rezortov. Svojou expertnou činnosťou prispelo k analýze kybernetického incidentu v infraštruktúre ÚGKK. VS spolupracovalo s viacerými zahraničnými partnermi v preverovaní možných negatívnych dopadov na SR v rôznych kybernetických incidentoch, ako napr. po úniku osobných a prihlasovacích údajov, ktoré boli šírené na verejnej sieti internet. Zároveň sa aktívne podieľalo na riešení kybernetických incidentov presahujúcich hranice SR. 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 NCIA, NATO CCD COE a EDA. Konkrétne išlo o cvičenia CROSSED SWORDS 2025, CYBER COALITION 2025, EDA milCERT exercise 2025, NATO CMX 2025 a národných veliteľsko–štábnych cvičení zameraných na preverenie obrany štátu v kybernetickom priestore. Medzi najvýznamnejšie patrí cvičenie LOCKED SHIELDS 2025, kde SR obsadila celkovo 4. miesto spomedzi 24 zúčastnených tímov z približne 30 krajín NATO a EÚ. Medzinárodný slovensko-maltský tím, tvorený zástupcami štátneho, súkromného a akademického sektora, svojim umiestnením opätovne potvrdil pripravenosť a preukázal kľúčové spôsobilosti SR v oblasti kybernetickej obrany.

6.1.4 Ministerstvo financií Slovenskej republiky

I. Vnímanie hrozieb a rizík v roku 2025

Rok 2025 potvrdil, že kybernetické hrozby sú ekonomickým aj geopolitickým faktorom, ktorý významne ovplyvňuje chod organizácií. Najväčšie riziká predstavuje ransomvér, dodávateľský reťazec a AI-podporované útoky. V podmienkach MF boli za relevantné hrozby a riziká vnímané najmä hrozby kybernetického útoku a narušenia alebo zničenia kritickej infraštruktúry.

Dynamicky sa meniaca legislatíva zvyšuje technické, personálne, odborné, organizačné a procesné nároky na organizácie verejnej správy, pričom tieto požiadavky často nie sú sprevádzané primeraným finančným krytím v rámci rozpočtu SR. Legislatívna prax ukazuje, že pri prijímaní zákonov, príslušných vyhlášok a ich novelizáciách býva v dôvodových správach často deklarovaný nulový finančný a personálny dopad na štátny rozpočet. Tento rozpor medzi legislatívnymi požiadavkami a reálnymi kapacitami organizácií vedie k systémovému podfinancovaniu, prevádzkovému napätiu a vytváraniu investičného dlhu, ktoré ohrozuje efektívne plnenie povinností v oblasti kybernetickej bezpečnosti. Riadenie kontinuity činností v rámci kritickej infraštruktúry na Slovensku čelí zásadným systémovým problémom, najmä v oblasti koordinácie spolupráce medzi OVM a inými subjektmi kritickej infraštruktúry, pripravenosti a distribúcii krízových plánov medzi príslušné organizácie. Rovnako vnímame ako potrebné pripraviť odporúčania pre jednotlivé organizácie, ako sa vysporiadať a čeliť novým typom hrozieb v podobe dronov (špionáž, útok), implementácie AI nástrojov a ich zneužitia z pohľadu dát na vstupe a na výstupe. V kontexte kybernetickej bezpečnosti je tento problém obzvlášť závažný, keďže výpadky a incidenty v digitálnom prostredí majú okamžitý a často kaskádový vplyv na fungovanie štátu a poskytovanie služieb občanom.

II. Čo považujete za najväčšie riziko pre vašu oblasť?

Ransomvérové útoky sú považované za najzávažnejšie hrozby pre štát a najmä sektor financie. V roku 2025 zasiahli viacero kľúčových štátnych aj podnikových systémov. Za najväčší štátny incident považujeme útok na systémy ÚGKK. Incident zásadne ovplyvnil finančné procesy štátu aj bánk, nakoľko napadnutý systém je integrálnou súčasťou úverových procesov bánk (záložné práva, verifikácia vlastníctva). Útok spôsobil výrazné spomalenie schvaľovania hypoték, notárskych úkonov a procesov na Finančnom riaditeľstve SR. Dopad pre sektor financie bol z tohto hľadiska doposiaľ bezprecedentný. Aj incident mimo bankového ekosystému môže paralyzovať kľúčové procesy, ak je naviazaný na štátne registre (kataster, RPO, RFO, eGov komponenty).

Trendy v SR, čo sa týka sociálneho inžinierstva a AI-generovaných podvodov kopírujú európsky vývoj s rastom AI-posilnených útokov, ako napríklad generované deepfake videá manažérov, vishing s AI hlasom, presvedčivé e-maily imitujúce regulátora, poisťovňu, daňový úrad a podobne.

Finančný sektor patrí dlhodobo medzi najodolnejšie sektory z pohľadu kybernetickej bezpečnosti, avšak ako hrozbu vnímame jeho previazanosť na iné, menej odolné sektory ako je napríklad štátna správa či energetika. Krízové riadenie nie je dostatočne koordinované medzi štátom, bankami a kritickými dodávateľmi. Na národnej úrovni absentuje testovanie pripravenosti na rôzne krízové scenáre a koordinácia zainteresovaných zložiek prvkov kritickej infraštruktúry pri jednotlivých krízových scenároch. Ako príklad môžu poslúžiť rozsiahle blackouty na Pyrenejskom polostrove, alebo v Českej republike, ktoré sa odohrali v roku 2025. Štát by mal byť pripravený na obdobné krátkodobé, ale aj strednodobé výpadky a mal by mať pripravené a rozdistribuované plány reakcie na ne.

Personálna poddimenzovanosť je vážnym problémom verejnej správy. Udržanie kvalitných odborníkov v dostatočnom počte v oblasti informačnej a kybernetickej bezpečnosti je náročné, keďže súkromný sektor im dokáže poskytnúť lepšie platové podmienky.

III. Ako hodnotíte aktuálnu úroveň kybernetickej bezpečnosti vo vašej oblasti/sektore?

Sektor financie patrí tradične medzi najregulovanejšie a technologicky najvyspelejšie oblasti ekonomiky. Rok 2025 ukázal špecifické slabiny, ktoré by mohli vplývať na jeho celkovú odolnosť. Bankový podsektor má dlhodobo nadštandardnú mieru regulácie (NBS, EBA, DORA), čo sa prejavuje v technických opatreniach. Banky využívajú moderné systémy, majú robustné IAM, segmentáciu, bezpečnostné dohľady a pokročilé monitorovanie. Ako vážne riziká bankového podsektora sa považuje najmä zraniteľnosť štátnych systémov, čo má priame dopady na banky. Kataster, registre a e-Gov komponenty sú kritické pre úverové a AML (Anti-Money Laundering) procesy. Útok na ÚGKK preukázal, že slabiny mimo bankového prostredia môžu mať priamy vplyv na finančné služby. Po incidente MF pristúpilo k výraznému zvýšeniu pozornosti na oblasť kyberbezpečnosti súvisiacej so správou a prevádzkou informačných systémov v oblasti riadenia verejných financií. Rast AI-posilnených útokov, deepfake a vishing kampane zasiahli aj finančné procesy. Rastúci počet podvodov na klientoch a zraniteľnosť koncových zariadení klientov má takisto negatívny vplyv na odolnosť bankového sektora.

IV. Aktivity realizované v roku 2025

V roku 2025 bol v podmienkach MF externým audítorom realizovaný audit kybernetickej bezpečnosti s výsledkom súladu s legislatívnymi požiadavkami na 88 %, čo predstavuje pozitívny posun oproti ostatnému auditu. V hodnotenom období sa vykonala aktualizácia informačných aktív a analýza rizík, kde významná časť rizík bola v porovnaní s predchádzajúcim stavom s nižšou závažnosťou. Zostávajúcim rizikám s nižšou závažnosťou sa dlhodobo venuje primeraná pozornosť. V roku 2025 MF pristúpilo k prebudovaniu oddelenia bezpečnostného monitoringu SOC na oddelenie CSIRT. Zároveň sa začali prípravné práce na akreditácii oddelenia CSIRT v rámci medzinárodného združenia CSIRT tímov - TF CSIRT. V podmienkach MF boli realizované opatrenia zahŕňajúce kontinuálne zlepšovanie vybudovaného systému bezpečnostného monitoringu, analýzy rizík a pravidelné audity a skeny zraniteľností v spolupráci s oddelením CSIRT a externými dodávateľmi. V roku 2025 MF s ohľadom na incident na portáli ÚGKK venovalo zvýšenú pozornosť testovaniu plánov obnovy informačných systémov MF. V rámci hodnoteného obdobia boli realizované aktivity týkajúce sa schváleného IT projektu Posilnenie informačnej a kybernetickej bezpečnosti MF (PIKB), ktorého cieľom je pokračovať v posilnení kybernetickej bezpečnosti ministerstva, a to prostredníctvom zavádzania nových bezpečnostných technológií a zabezpečenia informačných systémov v rámci rezortu financií. Projektom PIKB bude riešená aj bezpečnosť prístupových infraštruktúr, kde sa plánuje podpis zmlúv s rezortnými organizáciami opisujúcimi rozsah poskytovaných služieb CSIRT. Na záver roka 2025 sa spustilo verejné obstarávanie na dodávku tovarov a služieb potrebných pre naplnenie cieľov projektu PIKB. Hlavné aktivity projektu PIKB sa začali vykonávať pomocou interného personálu od 15. októbra 2025. Osveta zamestnancov a verejnosti v oblasti IKB v roku 2025 zo strany MF sa realizovala prostredníctvom odborných prednášok zamestnancov SIT. Organizované boli prednášky a školenia pre zamestnancov MF, Štátnej pokladnice a študentov Žilinskej univerzity v Žiline. Zamestnancom sú na pravidelnej báze zasielané e-maily týkajúce sa aktuálnych hrozieb a trendov v oblasti IKB.

6.1.5 Ministerstvo zdravotníctva Slovenskej republiky

I. Vnímanie hrozieb a rizík v roku 2025

V roku 2025 bol zaznamenaný výrazný nárast intenzity a sofistikovanosti kybernetických hrozieb. Nárast ransomvérových incidentov, sprevádzaný zvyšujúcou sa technickou vyspelosťou útočníkov a rastúcou mierou ich úspešnosti, preukázal schopnosť narušiť prevádzku dotknutých organizácií na obdobie niekoľkých dní až týždňov. Prevádzka zastaraných a neaktualizovaných informačných systémov, technologický dlh a rozsiahla závislosť od informačno-komunikačných technológií významne zvyšujú pravdepodobnosť úspešného narušenia a predlžujú čas obnovy po incidente, čím sa zvyšuje riziko narušenia kontinuity poskytovania zdravotnej starostlivosti. Významným aspektom vývoja v roku 2025 bol tiež nárast útokov podporovaných umelou inteligenciou. Útočníci vo zvýšenej miere využívali AI nástroje na tvorbu presvedčivých phishingových kampaní, čo zásadne zvyšovalo úspešnosť sociálneho inžinierstva, ktoré je významným rizikom najmä pre zdravotnícke zariadenia, ktoré pracujú s veľkým počtom používateľov s rôznorodou úrovňou digitálnych zručností. Každodenný kontakt personálu s citlivými údajmi zvyšuje pravdepodobnosť úspechu manipulatívnych techník útočníkov.

II. Čo považujete za najväčšie riziko pre vašu oblasť?

Najvýznamnejšie riziko pre poskytovateľov zdravotnej starostlivosti predstavujú útoky, ktoré môžu narušiť prevádzkovú kontinuitu, najmä ransomvérové incidenty. Zdravotníctvo patrí medzi sektory s najvyššou závislosťou od nepretržitej dostupnosti informačných systémov. Úspešný ransomvérový útok môže spôsobiť obmedzenie poskytovania zdravotnej starostlivosti, a tým ohroziť život a zdravie pacientov. Ďalším zásadným rizikom je technologický dlh – zastarané systémy, chýbajúce aktualizácie, obmedzená kompatibilita a vysoká miera integrácie s externými riešeniami, vrátane dodávateľského reťazca. Riziko zvyšujú aj manipulatívne techniky sociálneho inžinierstva, ktoré sú v zdravotníctve mimoriadne účinné vzhľadom na prevádzkovú záťaž a rôznorodosť používateľov.

III. Ako hodnotíte aktuálnu úroveň kybernetickej bezpečnosti vo vašej oblasti/sektore?

Úroveň kybernetickej bezpečnosti v zdravotníctve je možné hodnotiť ako postupne sa zlepšujúcu, avšak stále nedostatočnú vo vzťahu k rozsahu hrozieb. Pretrváva technologický dlh, limitované personálne kapacity, chýbajúci nepretržitý monitoring a nerovnomerné zavádzanie bezpečnostných štandardov. Používatelia disponujú rozdielnou úrovňou digitálnych zručností, čo zvyšuje celkovú zraniteľnosť poskytovateľov zdravotnej starostlivosti. Pozitívnym trendom je zlepšovanie procesov v dôsledku legislatívnych požiadaviek a rastúce povedomie o rizikách.

IV. Aktivity realizované v roku 2025

V roku 2025 bol v sektore zdravotníctva zahájený proces akreditácie jednotky CSIRT pre sektor zdravotníctva, ktorej úlohou je posilniť koordináciu, riešenie incidentov a odbornú podporu. V nadväznosti na Európsky akčný plán pre kybernetickú bezpečnosť nemocníc a poskytovateľov zdravotnej starostlivosti bol iniciovaný proces tvorby národného akčného plánu, ktorého cieľom je posilniť pripravenosť sektora na odhaľovanie kybernetických hrozieb a zlepšenie reakcie na KBI. V rámci tejto iniciatívy bolo taktiež zriadené Národné centrum na podporu kybernetickej bezpečnosti pre nemocnice a poskytovateľov zdravotnej starostlivosti, ktoré má poskytovať metodickú pomoc, špecializované služby, nástroje a odborné usmernenia v súlade s Európskym centrom podpory kybernetickej bezpečnosti pre zdravotnícky sektor. Tieto aktivity predstavujú zásadný krok smerom k systematickému posilneniu kybernetickej odolnosti zdravotníckeho sektora a vytvárajú rámec pre efektívnejšiu koordináciu, zdieľanie informácií a riešenie incidentov v budúcnosti.

6.2. Stav kybernetickej bezpečnosti z pohľadu ostatných ústredných orgánov

6.2.1 Ministerstvo zahraničných vecí a európskych záležitostí SR

Úroveň kybernetickej bezpečnosti v rezorte MZVEZ zodpovedá platným legislatívnym požiadavkám a je zabezpečovaná pri maximálnom možnom využití dostupných rozpočtových, technických a personálnych kapacít rezortu. Rezort priebežne prijíma technické a organizačné opatrenia zamerané na znižovanie rizík vyplývajúcich z aktuálnych kybernetických hrozieb, najmä z hľadiska ochrany informačno-komunikačných technológií, systémov a spracúvaných informácií.

Za kľúčové riziko možno považovať možnosť infiltrácie informačno-komunikačných technológií a systémov škodlivým kódom prostredníctvom zraniteľností, ktorých zneužitie by mohlo viesť k neoprávnenému získavaniu informácií z prostredia rezortu. Z tohto dôvodu boli prijaté viaceré opatrenia technického charakteru s cieľom eliminovať identifikované vektory možných kybernetických útokov a posilniť ochranu informačných systémov.

MZVEZ v sledovanom období realizovalo viacero technicko-bezpečnostných opatrení, vrátane plnej implementácie dvojfaktorovej autentifikácie pre prístup do neutajovaných informačných systémov. Bola zrealizovaná migrácia služieb do cloudu, čo rovnako prispelo k zvýšeniu úrovne bezpečnosti a dostupnosti služieb. Prebiehali pravidelné preškolenia v oblasti kybernetickej bezpečnosti a bol zavedený e-learningový kurz. Zároveň boli realizované školenia v oblasti kybernetickej diplomacie ako súčasť predvýjazdovej prípravy pri vysielaní diplomatov na ZÚ v zahraničí.

Napriek prijatým opatreniam pretrvávajú viaceré systémové výzvy. Medzi najvýznamnejšie patrí nedostatok špecializovaných personálnych kapacít v oblasti bezpečnosti IT systémov a obmedzené možnosti finančného ohodnotenia odborníkov v štátnej správe v porovnaní so súkromným sektorom. Významným faktorom sú aj vysoké finančné náklady spojené so zabezpečovaním a priebežným zvyšovaním úrovne kybernetickej bezpečnosti.

Z pohľadu rezortu je potrebné naďalej posilňovať technické, personálne a finančné predpoklady kybernetickej bezpečnosti, vrátane rozvoja systémov včasnej detekcie, pravidelného vyhodnocovania rizík, zvyšovania kybernetickej hygieny a zabezpečenia primeranej technickej a administratívnej podpory. Celkovo možno stav kybernetickej bezpečnosti v rezorte hodnotiť ako stabilizovaný a primeraný dostupným kapacitám, pričom ďalšie zvyšovanie odolnosti bude závisieť najmä od schopnosti posilniť odborné kapacity, zabezpečiť udržateľné financovanie a priebežne reagovať na meniace sa hrozby v kybernetickom priestore.

6.2.2 Slovenská informačná služba

Rok 2025 priniesol do oblasti kybernetickej bezpečnosti potrebu pokračovať v prispôsobovaní sa novým výzvam. V globálnom meradle možno za najvýznamnejší trend označiť postupujúce „dozrievanie“ modelov agentickej umelej inteligencie, spojené s rapídnym nárastom tokov vykonávaných s jej asistenciou. To prispieva k znižovaniu technologickej bariéry a umožňuje automatizáciu útokov, obchádzanie tradičných detekčných mechanizmov, vytváranie škodlivého kódu a generovanie phishingových správ za vynaloženia minimálnej námahy. Výsledkom je dramatický nárast efektivity ich malígneho pôsobenia. Súčasne napreduje rozvoj deepfake obsahu, komplikujúci odhaľovanie dezinformačných kampaní a narúšajúci dôveru verejnosti v digitálne informácie. Medzi najvýznamnejšie riziká je možné zaradiť taktiež aj pokračujúcu profesionalizáciu kybernetickej kriminality, spojenú s rozširovaním modelov ransomvér ako služba a malvér ako služba, ktorá znižuje vstupnú bariéru pre útočníkov a umožňuje rýchlu škálovateľnosť útokov.

Znepokojujúcim faktorom je taktiež pokračujúci nárast počtu ransomvérových a APT skupín spojený so zdokonaľovaním techník vydierania obetí a prieniku do cieľových systémov. Útočníci čoraz častejšie cielia na dodávateľské reťazce, priemyselné riadiace systémy a prevádzkové technológie, pričom je evidentná intenzívna snaha predovšetkým čínskych a ruských APT skupín o dlhodobé, nenápadné pôsobenie v kompromitovaných sieťach. Zlepšenie situácie v tejto oblasti je dlhodobo obmedzované pretrvávajúcim nedostatkom kvalifikovaných odborníkov na kybernetickú bezpečnosť, ktorý predstavuje významný limitujúci faktor ovplyvňujúci schopnosť organizácií adekvátne reagovať na bezpečnostné incidenty. Tento deficit zároveň znižuje úroveň pripravenosti organizácií/subjektov, spomaľuje implementáciu ochranných opatrení a zvyšuje ich celkovú zraniteľnosť‘ voči dynamicky sa vyvíjajúcim kybernetickým hrozbám.

Globálny vývoj disponuje potenciálom zásadným spôsobom ovplyvniť aj bezpečnostné prostredie SR. Kybernetické hrozby sa stávajú komplexnejšími, rýchlejšími a ťažšie predvídateľnými, pričom sú často prepojené s geopolitickým napätím. V uplynulom roku sa pritom priamou formou potvrdilo, že útoky cieliace na kľúčové informačné systémy majú potenciál zásadným spôsobom ovplyvniť chod štátu, a kľúčovým faktorom úspešného útoku je ľudský prvok.

Kým v roku 2024 bola SR cieľom výhražných e-mailových kampaní, koncom roka 2024 a začiatkom roka 2025 adekvátne aplikovanie opatrení na zabezpečenie kybernetickej bezpečnosti štátu pri výhražných e-mailových kampaniach prispelo k ich rapídnemu zníženiu. V roku 2025 v SR naopak významne vzrástlo riziko sofistikovaných phishingových a spearphishingových kampaní a iných foriem sociálneho inžinierstva, ktoré zneužívajú nedostatočnú kybernetickú hygienu používateľov a slabé overovanie identity. Pretrváva ich pomerne vysoká incidencia ako aj úspešnosť, a to často aj v oblasti kritickej infraštruktúry SR. Výsledkom boli v uplynulom roku okrem iného aj viaceré incidenty úspešných ransomvérových útokov cieliacich na elektronické systémy verejnej správy.

Za najväčšiu výzvu uplynulého roka možno považovať pretrvávajúcu prítomnosť zraniteľností v tejto oblasti. Kybernetický útok na ÚGKK z januára 2025 sa vyznačoval širokými systémovými presahmi, pričom odhalil slabé miesta digitálnej infraštruktúry SR. Zároveň však podstatným spôsobom urýchlil odbornú diskusiu a významne posilnil spoluprácu na rezortnej, národnej, ako aj medzinárodnej úrovni. Prostredie verejnej správy SR je dlhodobo charakteristické suboptimálnym financovaním kybernetickej bezpečnosti, ktoré obmedzuje schopnosť organizácií implementovať adekvátne technické a organizačné opatrenia. Výzvou zároveň zostáva relatívne nízke povedomie úradníkov o problematike, slabé zabezpečenie prihlasovacích údajov a absencia pokročilejších autentifikačných mechanizmov, ako aj nesprávne zaobchádzanie s citlivými údajmi. Zosilňovačom asociovaného rizika je pretrvávajúci nedostatok školení a všeobecného bezpečnostného povedomia. Hoci sa pravidelne realizujú vzdelávacie kampane a odborné podujatia, je mimo ich dosahu plne odstrániť identifikované slabé miesta v správaní používateľov.

Celková úroveň kybernetickej bezpečnosti SR je v súčasnosti nižšia ako želateľná, pričom medzi jednotlivými sektormi naďalej pretrvávajú významné rozdiely. Kritická infraštruktúra a digitálne služby sú naďalej vystavované rastúcim tlakom. Napriek tomu je však možné pozorovať kontinuálne zlepšovanie úrovne kybernetickej bezpečnosti v SR.

7. VYHODNOTENIE PLNENIA AKČNÉHO PLÁNU REALIZÁCIE NÁRODNEJ STRATÉGIE KYBERNETICKEJ BEZPEČNOSTI NA ROKY 2021-2025

Rok 2025 bol posledným rokom Národnej stratégie kybernetickej bezpečnosti SR pre roky 2021 až 2025. Preto bol aj rokom, v ktorom bolo vyhodnotené plnenie Akčného plánu národnej stratégie. Vyhodnotenie poskytlo prehľad o naplnení strategických cieľov štátu v oblasti kybernetickej bezpečnosti. Implementácia stratégie prebiehala prostredníctvom konkrétnych úloh rozdelených do tematických kategórií, pričom ich plnenie bolo pravidelne monitorované a vyhodnocované.

V hodnotenom období došlo k výraznému pokroku najmä v oblasti legislatívy, metodického usmerňovania, budovania inštitucionálnych kapacít a rozvoja medzinárodnej spolupráce. Väčšina úloh bola splnená resp. čiastočne splnená, pričom sa podarilo vytvoriť základné systémové rámce riadenia kybernetickej bezpečnosti na národnej úrovni.

V kategórii **Dôveryhodný štát pripravený na hrozby** boli aktualizované právne predpisy vrátane prípravy na implementáciu smernice NIS2, vypracované metodiky riadenia rizík a posilnené analytické a detekčné kapacity. Nedostatky pretrvávajú najmä v oblasti ekonomického modelovania politík, systematického hodnotenia rizík a certifikácie výrobkov a služieb.

V oblasti **efektívneho odhaľovania a objasňovania počítačovej kriminality** došlo k posilneniu odborných kapacít orgánov činných v trestnom konaní, k rozvoju vzdelávacích programov a metodickej podpory. Čiastočne však ostali nedokončené opatrenia týkajúce sa jednotného štatistického vykazovania počítačovej kriminality a komplexných legislatívnych úprav v tejto oblasti.

V kategórii **odolný súkromný sektor** bol zavedený jednotný systém hlásenia kybernetických incidentov a vytvorený právny rámec pre testovanie odolnosti subjektov. Obmedzený pokrok bol zaznamenaný pri budovaní podporných mechanizmov, najmä grantových schém a inkubátorov pre malé a stredné podniky.

V oblasti **kybernetickej bezpečnosti vo verejnej správe** boli vytvorené metodické rámce, šablóny dokumentácie, zavedené nástroje na testovanie zraniteľností a posilnené mechanizmy monitorovania a reakcie na incidenty. Rezervy pretrvávajú najmä v jednotnom uplatňovaní metodík a v systematickom budovaní odborných kapacít.

V oblasti **silných partnerstiev** Slovenská republika aktívne participovala na tvorbe politík EÚ, NATO a ďalších medzinárodných organizácií, a súčasne rozvíjala sektorovú spoluprácu. Priestor na ďalší rozvoj spočíva v oblasti kybernetickej diplomacie a hlbšej integrácie do obranných iniciatív.

V kategórii **vzdelávania a rozvoja odborníkov** došlo k začleneniu kybernetickej bezpečnosti do kurikulárnej reformy, vzniku nových študijných programov a metodických materiálov. Chýba však jednotný systém merania kompetencií a dlhodobý, koordinovaný rámec hodnotenia výsledkov.

Najslabšie výsledky boli zaznamenané v oblasti **výskumu a vývoja**, kde sa síce podarilo rozbehnúť grantové schémy a normalizačné aktivity, avšak nepodarilo sa vytvoriť koordinované výskumné konzorcium, spoločnú infraštruktúru ani systematický mechanizmus zdieľania dát.

Vyhodnotenie plnenia Národnej stratégie kybernetickej bezpečnosti tak ukázalo, že Slovenská republika v období 2021 – 2025 významne posilnila svoje základné kapacity a rámce kybernetickej bezpečnosti. Do budúceho obdobia bude nevyhnutné zamerať sa na prehĺbenie strategickej koordinácie, zavedenie merateľných ukazovateľov výkonnosti, systematické budovanie odborných kapacít a vytvorenie udržateľného a prepojeného systému podpory výskumu, vzdelávania a inovácií v oblasti kybernetickej bezpečnosti.

8. AKTIVITY A OPATRENIA NBÚ

8.1 Národná legislatíva

Slovenská republika zavŕšila proces transpozície smernice 28. novembra 2024, kedy Národná rada Slovenskej republiky schválila zákon č. 366/2024 Z. z., 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 zákony. ZoKB nadobudol účinnosť 1. januára 2025. Slovenská republika sa tak stala piatou krajinou, ktorá si splnila transpozičnú povinnosť a len treťou krajinou s úplnou transpozíciou smernice NIS2.

V roku 2025 došlo k prijatiu podzákonných právnych predpisov v oblasti kybernetickej bezpečnosti, ktoré nadväzujú na novelu ZoKB. Národný bezpečnostný úrad vydal dve nové vyhlášky. Prvou je Vyhláška Národného bezpečnostného úradu č. 226/2025 Z. z., ktorou sa ustanovujú podrobnosti o hláseniach. Vymedzuje kritéria závažného narušenia fungovania prevádzkovateľa základnej služby, náležitosti hlásenia závažného kybernetického bezpečnostného incidentu a hlásenia významnej kybernetickej hrozby či udalosti odvrátenej v poslednej chvíli. Druhou je Vyhláška Národného bezpečnostného úradu č. 227/2025 Z. z., ktorá ustanovuje obsah bezpečnostných opatrení, rozsah všeobecných bezpečnostných opatrení pre siete a informačné systémy a operačné technológie a obsah a štruktúru bezpečnostnej dokumentácie.

Národný bezpečnostný úrad zároveň vydal novú metodiku analýzy rizík, podľa ktorej majú prevádzkovatelia základnej služby vykonávať riadenie rizík. Ide o kľúčový dokument pri aplikovaní zákona a najmä pri implementácii opatrení.

8.2 Európska únia

V oblasti kybernetickej bezpečnosti sa rok 2025 niesol najmä v znamení implementácie už prijatej legislatívy v národnom prostredí, predovšetkým kľúčovej horizontálnej smernice NIS2. Jej cieľom je, aby tieto subjekty mali jasne stanovené procesy riadenia rizík, zavedené primerané bezpečnostné opatrenia a včas hlásili významné kybernetické incidenty.

Implementácia sa ďalej týkala nariadenia CRA, ktoré sa sústreďuje na samotné produkty s digitálnym prvkom – softvér, hardvér, IoT a iné. Stanovuje výrobcom povinnosť navrhovať produkty bezpečne v súlade s princípom secure by design, pravidelne ich aktualizovať, riešiť zraniteľnosti počas celého životného cyklu a transparentne informovať o rizikách. Na národnej úrovni sa preto vytvoril systém, ktorý má umožniť požadovanú certifikáciu a následný dohľad nad certifikovanými produktmi.

Pozornosť bola venovaná aj implementácii nariadenia eIDAS2, ktorým sa zavádza európska peňaženka digitálneho občana. Národné riešenie peňaženky musí spĺňať spoločne dohodnuté technické špecifikácie, aby bolo vzájomne interoperabilné s ostatnými členskými štátmi EÚ, čomu bude predchádzať náležitá certifikácia riešenia a jeho partnerské preskúmanie.

V priebehu roka 2025 sa konali technické výbory na úrovni Európskej komisie, ktorých výsledkom bolo vydanie niektorých implementačných nariadení EK vo vestníku EÚ. Zavedením aktualizovaných pravidiel elektronickej identifikácie vrátane európskej peňaženky digitálnej identity sa vytvoril právne nespochybniteľný základ spoločného chráneného digitálneho priestoru v EÚ. Slovensko počas celého roka aktívne zasielalo pripomienky a komentáre, ktoré slúžili na zefektívnenie a racionalizáciu prerokovávaných právnych noriem. Na nariadenie eIDAS2 koncom novembra 2025 nadviazalo nariadenie EBW, ktorého cieľom je umožniť firmám a iným právnym subjektom jednoduchú, rýchlu a bezpečnú komunikáciu, výmenu dokumentov a overovanie totožnosti naprieč EÚ.

Vo februári 2025 z dôvodu administratívneho korigenda vstúpilo do účinnosti nariadenie CySOLa, ktoré sa sústredilo na spoločnú ochranu a reakciu EÚ pri kybernetických incidentoch väčšieho rozsahu. Zavádza celoeurópsky systém detekcie hrozieb, sieť cezhraničných cyber hubov, mechanizmy koordinovanej reakcie a tzv. európsku kybernetickú rezervu – skupinu odborníkov a kapacít, ktoré môžu byť nasadené pri útokoch. Jeho cieľom je zlepšiť pripravenosť štátov a umožniť rýchlu, koordinovanú reakciu na incidenty presahujúce hranice jedného štátu. Záverom roka 2025 požiadalo Moldavsko o pomoc z rezervy na účely kybernetickej bezpečnosti. Komisia po posúdení žiadosti predložila Rade EÚ návrh na prijatie vykonávacieho aktu, ktorým by sa povoľovalo poskytnutie podpory Moldavsku.

Rada EÚ prijala v júni 2025 aktualizované odporúčanie, ktoré definuje, ako má EÚ a členské štáty EÚ reagovať na rozsiahle kybernetické incidenty alebo kybernetické krízy. Tzv. Blueprint stanovuje jednotný postup v rámci celej EÚ od detekcie, analýzy, eskalácie, reakcie až po zotavenie po incidente. Zároveň zdôrazňuje potrebu koordinácie medzi jednotlivými aktérmi. Na jeseň 2025 sa v Rade EÚ na úrovni pracovnej skupiny uskutočnilo praktické cvičenie, ktoré prenieslo návrhy do praxe.

V oblasti kybernetickej diplomacie, ktorá obsahovo presahuje do domén Spoločnej zahraničnej a bezpečnostnej politiky EÚ a Spoločnej bezpečnostnej a obrannej politiky EÚ sa aktivity v prvej polovici roka sústredili prevažne na koordináciu spoločných pozícií EÚ pre rokovania OEWG, kde vrcholili diskusie o založení permanentného mechanizmu, ktorý by pokrýval globálnu koordináciu aspektov kybernetickej bezpečnosti. Tzv. Globálny mechanizmus OSN má začať fungovať v marci 2026.

Slovensko sa tiež zapojilo do kybernetických dialógov s tretími partnerskými krajinami a zúčastnilo sa cvičenia aplikácie „Súboru nástrojov kybernetickej diplomacie v praxi“. V kontexte vyhodnocovania neustálych kybernetických hrozieb Slovensko spolupracovalo s ostatnými členskými štátmi EÚ, svojimi strategickými partnermi, EEAS (INTCEN), EK, ENISA, ECCC, ECSO, Europolom, či CERT-EU, a zúčastňovalo sa prípravy ďalších sankčných kyberbezpečnostných zoznamov pre dotknuté fyzické osoby na žiadosť Estónska, či nášho strategického partnera, Veľkej Británie. Slovensko sa tiež zapojilo do procesu prípravy strategického materiálu k zaujatiu pozície EÚ voči škodlivým aktivitám pochádzajúcim z tretích krajín.

Slovensko v rámci svojich medzinárodných aktivít usporiadalo začiatkom júla 2025 konferenciu na pôde Stáleho zastúpenia v Bruseli venovanú digitálnym a kyberbezpečnostným zručnostiam, či získavaniu nových talentov určenú pre odbornú verejnosť, priemysel a zástupcov inštitúcií a členských štátov EÚ.

NBÚ sa aktívne zúčastňoval zasadnutí na úrovni Skupiny pre spoluprácu (NIS Cooperation Group), ktoré sú organizované na základe smernice NIS2. Cieľom Skupiny pre spoluprácu je 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 súčasťou viacerých pracovných skupín a iniciatív zameraných na budovanie spoločného rámca kybernetickej bezpečnosti. Medzi najvýznamnejšie aktivity patrí účasť v CyCLONe, sieti zástupcov členských štátov na zvládanie kybernetických kríz.

SK-CERT pôsobil aj v rámci medzinárodných organizácií, združujúcich jednotky CSIRTov. V rámci CSIRT Network si s členskými štátmi EÚ vymieňal operatívne informácie o hrozbách a incidentoch. Vzhľadom na pretrvávajúcu vojenskú situáciu na východe Európy si štáty vymieňali aj informácie súvisiace s vojnou na Ukrajine a poskytovali si vzájomnú pomoc podľa potreby. SK-CERT si v rámci CSIRT Network v roku 2025 udržal najvyšší status vyspelosti CSIRT jednotky „Advanced“, ktorý sa udeľuje po tzv. peer-review procese.

8.3 Organizácia pre bezpečnosť a spoluprácu v Európe

Zorganizované stretnutia účastníckych štátov OBSE podčiarkli dôležitosť medzinárodnej spolupráce v oblasti kybernetickej bezpečnosti a zdieľania informácií o existujúcich a potenciálnych hrozbách. Činnosti a fungovanie OBSE boli v roku 2025 ovplyvnené nestabilnou geopolitickou situáciou, najmä prebiehajúcou vojnou Ruskej federácie proti Ukrajine, čo sa následne premietlo aj na priebehu rokovaní o kybernetickej bezpečnosti a bezpečnosti IKT.

V uplynulom roku sa uskutočnili štyri zasadnutia IWG. Stretnutie kontaktných bodov OBSE pre oblasť IKT sa konalo súbežne s druhým zasadnutím IWG v júni 2025. Obsah zasadnutí tvorili diskusie o prebiehajúcej implementácii existujúcich iniciatív v zmysle opatrení na budovanie dôvery zúčastnených štátov OBSE, pričom vývoj CBM v rámci OBSE prebiehal paralelne s aktivitami Prvého výboru OSN s dôrazom na význam regionálnych organizácií pri implementácii záväzkov v oblasti kybernetickej bezpečnosti. Prebiehali tiež diskusie o národných iniciatívach (pripravované národné stratégie kybernetickej bezpečnosti a príslušné akčné plány ich implementácie) a vnútroštátnom vývoji v oblasti kybernetickej/IKT bezpečnosti. Krajiny tiež upriamili pozornosť na národné procesy venujúce sa novým technológiám, viedli odborné diskusie o naliehavých kybernetických výzvach ako napríklad vývoj umelej inteligencie, vplyvy kvantových technológií a o iných relevantných kybernetických a IKT hrozbách.

Výročná konferencia OBSE, ktorá sa konala súbežne s tretím zasadnutím IWG v októbri 2025, opätovne potvrdila kľúčovú úlohu OBSE ako fóra pre inkluzívny dialóg o kybernetickej bezpečnosti a bezpečnosti IKT. Jednotlivé diskusné panely poukázali na potrebu zosúladenia politických záväzkov s praktickými opatreniami a na význam koordinovanej spolupráce medzi štátmi, súkromným sektorom a medzinárodnými partnermi.

Sekretariát OBSE sa dlhodobo venuje činnostiam, ktoré podporujú činnosti pracovných skupín na úrovni OSN. Jednou z najdôležitejších aktivít Sekretariátu OBSE a Oddelenia pre nadnárodné hrozby bola podpora aktivít OEWG, a to najmä príspevky k tvorbe Dohovoru OSN proti počítačovej kriminalite a podpora transformácie OEWG na permanentný mechanizmus kybernetickej bezpečnosti, už spomínaný Globálny mechanizmus.

Prostredníctvom zasadnutí IWG NBÚ zdieľal informácie o implementačných procesoch transpozície smernice NIS2 do národnej legislatívy, o stave kybernetickej bezpečnosti, ako aj o aktuálnych aktivitách a pokrokoch pri implementácii opatrení na budovanie dôvery.

NBÚ vníma prínos zasadnutí OBSE v bezpečnom zdieľaní informácií na regionálnej úrovni, posilňovaní medzinárodnej spolupráce, upevňovaní svojho postavenia ako spoľahlivého medzinárodného hráča a v rozširovaní svojej siete kontaktných bodov v kybernetickej a IKT oblasti i mimo členských štátov EÚ. V spojitosti s aktivitami OBSE, je veľmi pozitívne hodnotená koordinácia spolupráce na národnej úrovni so zástupcami MZVEZ.

Z perspektívy úradu boli kľúčové najmä témy týkajúce sa vzájomného informovania účastníckych štátov OBSE a budovania dôvery, medziregionálnej spolupráce OBSE s inými regionálnymi organizáciami (UAS, ECOWAS) a medzinárodnými organizáciami (OSN), stratégií boja proti aktuálnym kybernetickým a hybridným hrozbám (ich prevencia, reakcia na takéto hrozby a nástroje stabilizácie kybernetického priestoru) a zamedzenia zneužívania nových a vznikajúcich technológií hlavne v kontexte podvratných aktivít vykonávaných nielen štátnymi ale aj neštátnymi aktérmi.

8.4 Organizácia Severoatlantickej zmluvy

Počas roka 2025 sa uskutočnili rokovania Bezpečnostného výboru NATO, ktoré prebehli vo všetkých svojich formátoch – vo formáte bezpečnostných politík, bezpečnosti komunikačných a informačných systémov a na úrovni riaditeľov bezpečnostných úradov členských štátov. Predsedajúcim výboru bol riaditeľ NOS Galen Nace, ktorý diskutoval s predstaviteľmi bezpečnostných autorít o rôznych bezpečnostných témach, a to nielen v kontexte súčasnej geopolitickej situácie.

Udalosťou roka NATO v oblasti kybernetickej bezpečnosti bola konferencia Cyber Defence Pledge, ktorá sa uskutočnila v máji vo Varšave. Účastníci tak mohli prvýkrát po rozsiahlej úprave dotazníka (2023) reflektujúceho na dynamiku v kyberpriestore zhodnotiť dosiahnutý pokrok aliancie v oblasti kybernetickej obrany v oblasti kritickej infraštruktúry, a bezpečnosti dodávateľského reťazca a vesmírnych systémov. Na vypracovaní dotazníka spolupracoval úrad s VS (Centrom kybernetickej obrany) a MV.

Tretia výročná konferencia o kybernetickej obrane NATO sa uskutočnila v októbri v Tirane 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 NBÚ a Centra kybernetickej obrany.

8.5 Regionálna spolupráca

V roku 2025 Národné centrum kybernetickej bezpečnosti Maďarska na základe rotácie predsedníctva krajín predsedalo CECSP. Zástupcovia NBÚ sa aktívne zúčastnili rokovaní platformy spolu s ďalšími kolegami zastúpenými krajinami Vyšehradskej štvorky (Česká republika, Maďarsko, Poľsko), Rakúska a Slovinska, ktoré sa stalo regulárnym členom platformy. Predmetom rokovaní boli aktuálne témy, v rámci ktorých sa partneri pokúšali nájsť spoločné prieniky a podporu. Maďarské predsedníctvo pokračovalo s aktualizáciou zakladajúcich dokumentov. Medzi najdôležitejšie témy stretnutia patrili: „Aktuálny stav procesu transpozície smernice NIS 2.0 v jednotlivých členských štátoch a informácie o významných kybernetických bezpečnostných incidentoch z posledného obdobia.“; „Kybernetická bezpečnosť a činnosť Národných kompetenčných centier“ „AI v kontexte kybernetickej bezpečnosti“ a „Využívanie umelej inteligencie v súvislosti so systémom „Honeypot“. Experti sa zhodli, že pri aproximácii sa vyžaduje adaptívny, koordinovaný a inovatívny prístup, ktorým sa dosiahne najširšia harmonizácia naprieč celou EÚ.

Rok 2025 sa niesol v duchu stretnutí s našimi najbližšími partnermi. Česká republika organizovala už šiesty ročník Prague Cyber Security Conference, ktorá sa uskutočnila v marci 2025. Témou konferencie boli „Invisible frontlines“ (Neviditeľné hranice) - kybernetický priestor ako miesto, kde dochádza ku konfliktom, ktoré síce môžu byť neviditeľné, no ich dopady sú viac než reálne.

V priebehu roka sa uskutočnilo niekoľko stretnutí so zástupcami NÚKIB k otázkam transpozície smernice NIS2, atribúcie a iných kyberbezpečnostných tém.

8.6 Bilaterálne vzťahy

Zo strany NBÚ boli bilaterálne vzťahy aktívne rozvíjané naprieč všetkými pracovnými platformami a formátmi, či už pri osobnom kontakte počas zasadnutia pracovných skupín, alebo ad hoc pri plnení úloh na bilaterálnej úrovni.

S cieľom ďalej rozvíjať a prehlbovať spoluprácu v oblasti kybernetickej bezpečnosti sa v Kenskej republike uskutočnil prvý ročník kyberbezpečnostnej hry CyberGame.

Príslušníci NBÚ pravidelne komunikovali o aktuálnych právnych predpisoch na národnej úrovni, zraniteľnostiach, hrozbách a incidentoch; zdieľali informácie o osvedčených postupoch a o dobrej praxi so zahraničnými partnermi; zúčastňovali sa rôznych medzinárodných cvičení kybernetickej bezpečnosti, ako aj bilaterálnych rokovaní a zahraničných prijatí.

O nadviazanie spolupráce v oblasti kybernetickej bezpečnosti prejavila záujem Brazílska federatívna republika. Rokovania vyústili do podpísania Memoranda o spolupráci v oblasti kybernetickej bezpečnosti medzi NBÚ a Kabinetom pre inštitucionálnu bezpečnosť Kancelárie prezidenta Brazílskej federatívnej republiky v máji 2025. Na memorandum nadviazalo decembrové pracovné stretnutie, na ktorom sa prediskutovalo aktuálne nastavenie kompetencií úradov a orgánov štátnej správy pri riešení kybernetických záležitostí. Implementácia memoranda ostáva významným mementom pri budovaní vzájomnej úzkej spolupráce a je dôležité v nastolenom trende pokračovať.

V októbri 2025 bolo podpísané Memorandum o porozumení medzi NBÚ a Národným úradom pre kybernetickú bezpečnosť Rwandskej republiky o posilnení spolupráce v oblasti kybernetickej bezpečnosti. Návšteva bola finančne podporená rozvojovým nástrojom SlovakAid – Sharing Slovak Expertise. Rwandská delegácia ocenila stav kybernetickej bezpečnosti v Slovenskej republike. Identifikovala viacero oblastí, v ktorých vidí perspektívu vzájomnej spolupráce, ako napríklad zriadenie Národného bezpečnostného úradu Rwandy, podporu budovania kyberkomunity, podporu vzdelávania, proces certifikácie audítorov a manažérov, proces vykonávania auditov, založenie Rady audítorov, riadenie kybernetického útoku alebo účasť na CyberGame.

8.7 Certifikačný orgán NBÚ

Ako súčasť opatrení vyplývajúcich z novely zákona č. 69/2018 o kybernetickej bezpečnosti s cieľom znížiť riziká súvisiace s rýchlym technologickým vývojom a digitalizáciou, zvýšiť celkovú úroveň kybernetickej bezpečnosti v podmienkach SR a podporiť domácich výrobcov a dodávateľov IT riešení, zriadil NBÚ orgán pre posudzovanie zhody v oblasti kybernetickej bezpečnosti. Ako prvý v SR tak preukázal spôsobilosť vykonávať akreditovanú činnosť plnením akreditačných požiadaviek normy ISO/IEC 17065: 2012 na vykonávanie certifikácie v oblasti hodnotenia kybernetickej bezpečnosti IKT produktov podľa EUCC. Tým sa SR ako siedma členská krajina EÚ (po Nemecku, Švédsku, Francúzsku, Španielsku, Holandsku a Taliansku) plnohodnotne zapojila do programu zabezpečujúceho automatické uznávanie certifikátov kybernetickej bezpečnosti vydaných certifikačnými orgánmi pôsobiacimi v EÚ vo všetkých krajinách Európskeho hospodárskeho priestoru.

Certifikačný orgán je akreditovaný podľa požiadaviek normy ISO/IEC 17065: 2012 a notifikovaný v systéme NANDO na výkon certifikácie v oblasti hodnotenia kybernetickej bezpečnosti IKT produktov.

8.8 Vydávanie varovaní, bulletinov a adresných varovaní

NCKB v priebehu roka 2025 monitorovalo otvorené, ale aj uzavreté zdroje so špecifickým zameraním na vyhľadávanie informácií o bezpečnostných zraniteľnostiach a s nimi súvisiacich aktivitách, najmä o ich aktívnom zneužívaní alebo zneužívaní nedostatočného zabezpečenia či nesprávnej konfigurácie verejne dostupných inštancií IKT zariadení a systémov. Následne prebiehalo zhodnotenie závažnosti zraniteľností a aktivít na základe multikriteriálneho hodnotenia.

V závislosti od závažnosti sú informácie komunikované prostredníctvom výstupov na webovom sídle SK-CERT, bezpečnostných varovaní alebo bulletinov. Bezpečnostné bulletiny sú rozposielané prostredníctvom e-mailu na adresy v zozname prihlásených odberateľov.

NCKB pripravuje adresné varovania, ktoré rozposiela subjektom so zraniteľnými alebo nedostatočne zabezpečenými inštanciami identifikovanými na základe voľne dostupných zdrojov a nástrojov.

Štatistický prehľad vydaných bezpečnostných bulletinov a varovaní

Mesiac	JAN	FEB	MAR	APR	MÁJ	JÚN	JÚL	AUG	SEP	OKT	NOV	DEC
Varovanie	62	55	69	56	53	63	59	50	39	54	35	22
Bulletin	4	4	4	5	4	4	5	4	5	4	4	3
Zraniteľnosť	107	109	126	132	109	129	147	125	116	80	55	44

NCKB priebežne pracuje na zlepšovaní procesu vyhodnocovania závažnosti informácií o bezpečnostných zraniteľnostiach a s nimi súvisiacimi aktivitami. Regulované subjekty a subjekty prihlásené na odber bezpečnostných varovaní a bulletinov môžu prispieť ku zlepšeniu kvality informácii zdieľaním údajov o využívaných technológiách ako aj pravidelnou aktualizáciou kontaktných údajov. Je žiadúce, aby mali neregulované subjekty implementovaný mechanizmus zodpovedného oznamovania zraniteľností podľa akceptovaného štandardu poskytovania bezpečnostných informácií webových stránok. NCKB dlhodobo sleduje negatívny trend ignorovania bezpečnostných varovaní adresovaných subjektom. Niektoré subjekty naďalej vychádzajú z presvedčenia, že z hľadiska potenciálnych útočníkov nepredstavujú atraktívny cieľ. Takýto prístup často vedie k ľahko odvrátiteľným incidentom. Organizácie pristúpia k riešeniu situácie až po opakovaných varovaniach od viacerých bezpečnostných zložiek štátu.

8.9 Cvičenia

Cvičenia v oblasti kybernetickej bezpečnosti sú kľúčové pre overenie pripravenosti, zlepšenie reakčných schopností a identifikáciu nedostatkov v procesoch a systémoch. V roku 2025 sa uskutočnilo cvičenie BlueOLEX, ktoré sa zameralo na simuláciu eskalácie rozsiahleho kybernetického bezpečnostného incidentu na dopravný 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 preveriť schopnosť riešiť tieto krízy.

NBÚ participoval na cvičení NATO CMX2025, v rámci ktorého bolo možné precvičiť politicko-vojenské konzultácie a rozhodovanie pri komplexnej civilno-vojenskej kríze v širokom spektre situácií. Cvičenie umožnilo preveriť pripravenosť NATO a jednotlivých štátov na súčasné bezpečnostné výzvy, vrátane kybernetických útokov.

V roku 2025 sa tiež uskutočnilo cvičenie CySOPex 2025, ktorého sa zúčastnili zástupcovia väčšiny členských štátov EÚ. Cvičenie bolo zamerané na dopravný sektor a prvky kritickej infraštruktúry. Pri tomto cvičení sa overovala rýchlosť reakcie, pripravenosť na rozsiahle kybernetické bezpečnostné incidenty a efektívnosť výmeny informácií na národnej ale aj medzinárodnej úrovni.

Odborníci z NCKB nechýbali ani na Locked Shields, najväčšom cvičení kybernetickej obrany na svete, ktoré sa konalo pod záštitou NATO CCDCoE. Zástupcovia NBÚ sa rozdelili do dvoch tímov. Jeden tvorili odborníci zo Slovenska a z Malty, a umiestnil sa na piatom mieste. Ďalší kolegovia boli v tíme NATO.

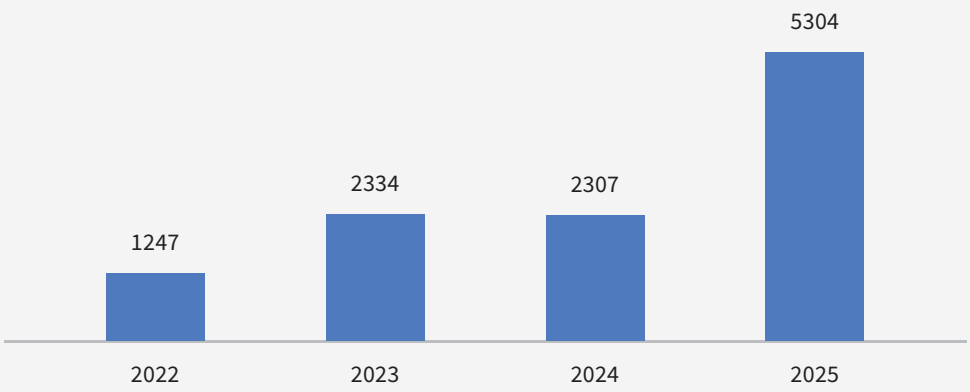
8.10 CyberGame

Z medzinárodnej hry CyberGame, zameranej na kybernetickú bezpečnosť, sa už stala tradícia. V roku 2025 sa definitívne zaradila medzi jeden z praktických formátov zameraných na rozvoj kyberbezpečnostných zručností. Hra trvá 10 týždňov a prináša úlohy rôznych úrovní náročnosti - od úloh pre začiatočníkov, ktorí sa vďaka CyberGame dostali k téme kybernetickej bezpečnosti, až po zložité úlohy pre skúsených profesionálov.

Štvrtý ročník priniesol výraznú zmenu. Vďaka rozvojovej spolupráci SR pod značkou SlovakAid a podpísanému memorandu o spolupráci medzi Slovenskom a Keňou sa tento rok otvorili tri verzie hry: národná verzia pre hráčov zo Slovenska, svetová a samostatná verzia pre hráčov z Kene. Kenská edícia sa stretla s veľmi pozitívnym ohlasom a počíta sa s jej pokračovaním aj v budúcnosti.

Počet hráčov sa oproti predošlému roku viac ako zdvojnásobil. Stúpol aj počet úspešných riešiteľov úloh.

Počet účastníkov CyberGame v jednotlivých ročníkoch



V roku 2025 hráčov potrápili úlohy v šiestich vetvách - malvérová analýza, forenzná analýza, kryptografia, OSINT, ofenzívna bezpečnosť a procesy a riadenie bezpečnosti. V národnej verzii sa súťažilo o vecné ceny v kategóriách celkový víťaz, najlepšia hráčka, študent, junior, najlepší hráč verejného sektora a učiteľ. Okrem toho boli odovzdané ocenenia víťazom jednotlivých hracích vetiev.

CyberGame, z dielne NCKB, konkrétne SK-CERT, je ukážkou, že štátna inštitúcia dokáže aj prostredníctvom praktických aktivít zvyšovať povedomie o kybernetickej bezpečnosti nielen na Slovensku, ale aj v zahraničí.

8.11 Bezpečnostné povedomie

V roku 2025 sa NBÚ systematicky venoval šíreniu povedomia o kybernetickej bezpečnosti prostredníctvom všetkých dostupných komunikačných kanálov s cieľom osloviť odbornú ale aj širšiu verejnosť.

Národný bezpečnostný úrad v spolupráci s partnermi pripravil dve konferencie zo série Kyber2025 na tému novej legislatívy a umelej inteligencie, ako aj ďalšie odborné podujatia. V rámci týchto podujatí prezentovali široké spektrum tém vrátane problematiky ransomvérových útokov, nahlasovania incidentov, certifikácie kybernetickej bezpečnosti, či aktuálneho stavu kybernetickej bezpečnosti na Slovensku.

Prednáškami, workshopmi, ako aj aktívnou účasťou experti prispeli do odborného programu viacerých významných konferencií v oblasti kybernetickej bezpečnosti, ako sú ITAPA, EPI konferencia Kybernetická bezpečnosť, OpenCamp 2025, SlovakiaTech Fórum-Expo, Cyber Security Bratislava, Kybernetická bezpečnosť v doprave a nová smernica NIS2. Zástupcovia NCKB sa podieľali aj na tvorbe programu konferencie FIRSTCON25 v Kodani.

Okrem osobných stretnutí, odborných podujatí a konferencií úrad aktívne využíval svoje oficiálne účty na sociálnych sieťach. Zároveň bol NBÚ pravidelne oslovovaný novinármi z tlačených a online médií, ako aj z televízneho a rozhlasového prostredia. NBÚ mal počas roka 2025 svoje zastúpenie v najsledovanejších ranných aj večerných mediálnych formátoch. V porovnaní s predchádzajúcimi rokmi zaznamenala mediálna prítomnosť úradu nárast, čo prispelo k tomu, že sa informácie o aktuálnych kybernetických hrozbách a preventívnych opatreniach dostali k širšej skupine ľudí.

V rámci mediálnej a komunikačnej činnosti sa NBÚ zameriaval najmä na témy ochrany zariadení a realizoval osvetové kampane zamerané na zvýšenie povedomia o rizikách spojených s využívaním umelej inteligencie, phishingovými útokmi a ransomvérom. Osobitná pozornosť bola venovaná aj témam určeným laickej verejnosti, ako napríklad odporúčaniam pre bezpečné správanie sa v online priestore počas letných dovoleniek či v zahraničí a ochrane osobných zariadení.

Úrad sa zároveň venoval komunikácii tém zameraných na rodičov, s cieľom podporiť ich schopnosť chrániť deti v digitálnom prostredí a viesť ich k bezpečnému používaniu internetu, ako aj k rozpoznávaniu a vyhýbaniu sa kybernetickým hrozbám. NBÚ v roku 2025 podpísal Deklaráciu o spolupráci pri ochrane seniorov pred podvodmi.

Dôležitou súčasťou komunikácie NBÚ boli odborné a legislatívne témy, najmä smernica NIS2, novela zákona o kybernetickej bezpečnosti a nové vyhlášky z dielne NBÚ. Prostredníctvom médií a sociálnych sietí úrad zároveň informoval verejnosť a dotknuté subjekty o možnostiach čerpania finančných príspevkov z fondov Európskej únie v oblasti kybernetickej bezpečnosti.

8.12 Vzdelávanie v oblasti kybernetickej bezpečnosti

Príslušníci a zamestnanci NBÚ sa podieľali na výučbe viacerých predmetov na vysokých školách. V rámci Fakulty informatiky a informačných technológií STU zabezpečovali výučbu predmetov Bezpečnosť informačných technológií (zameraného na softvérové zraniteľnosti), Bezpečnosť operačných systémov a Forenzná analýza. Na Fakulte elektrotechniky a informatiky STU v Bratislave zabezpečovali výučbu predmetu Manažment bezpečnostných incidentov. Spolupodieľali sa na zabezpečení odborného obsahu pre Vzdelávací program Bezpečnostné štúdia na Právnickej fakulte Univerzity Komenského. Na Katedre žurnalistiky Filozofickej fakulty Univerzity Komenského viedli jednosemestrálny predmet Bezpečnosť novinárov v online prostredí. Osvetu v oblasti kybernetickej bezpečnosti úrad realizoval aj prostredníctvom prednášok a diskusií na stredných školách.

Odborníci z NBÚ sa v akademickom prostredí pohybovali pomerne často, o čom svedčí aj účasť odbornom seminári Kybernetické bezpečnostné incidenty, ransomvér a trestnoprávna zodpovednosť. NCKB ako partner podporovalo Slovak Cyber Team, národnú reprezentáciu mladých talentov, a podieľalo sa na realizácií tréningových bootcampov.

V rámci oblasti kybernetickej bezpečnosti sa Slovensko snaží čoraz viac snaží zapojiť ženy o čom svedčí aj národná kapitola Women4Cyber, v rámci ktorej pôsobili odborníci z SK-CERT ako mentori v polročnom mentoringovom programe zameranom na prehlbovaní odborných znalostí.

V oblasti certifikácie kybernetickej bezpečnosti sa podieľal NOKC na vyhľadávaní, výbere a vzdelávaní expertov Národnej autority pre certifikáciu kybernetickej bezpečnosti (NCCA). Do tejto databázy sa v priebehu roka podarilo zaradiť 10 odborníkov. Zároveň NOKC v roku 2025 zorganizoval odborné školenie s účasťou medzinárodných lektorov pre expertov NCCA, ktorí získali kompetencie hodnotiteľa podľa EUCC, ako aj webinár na tému Certifikácia kybernetickej bezpečnosti pre IKT produkty.

9. ČINNOSŤ KCCKB

Štátna príspevková organizácia Kompetenčné a certifikačné centrum kybernetickej bezpečnosti plní úlohu Národného koordinačného centra 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.

EÚ projekty

V máji 2025 uzavrelo KCCKB prvý NCC projekt, ktorý úspešne obhájilo v auguste. Projekt bol venovaný zvyšovaniu povedomia o kybernetickej bezpečnosti, vytvoreniu Kyberkomunity, organizácii odborných podujatí a podpore malých a stredných podnikov v budovaní kapacít. Zároveň je od júna 2025 spustený nový projekt NCC 2.0 na roky 2025-2029.

KCCKB ako koordinátor je súčasťou projektu NIS2 spolu s NBÚ a Ministerstvom dopravy Slovenskej republiky. V júli prebehlo úspešné obhájenie všetkých vykonaných aktivít v polovici obdobia pred expertmi z Európskej komisie.

V rámci aktivít Národného koordinačného centra bola v roku 2025 ukončená a vyhodnotená výzva FSTP-Kaskádové financovanie ako súčasť projektu NCC, ktorej cieľom bolo významne prispieť k posilneniu kyberbezpečnostných kapacít zapojených subjektov. Predmetom výzvy bolo vypracovanie bezpečnostnej dokumentácie. Podporu získalo 44 subjektov so svojimi projektmi.

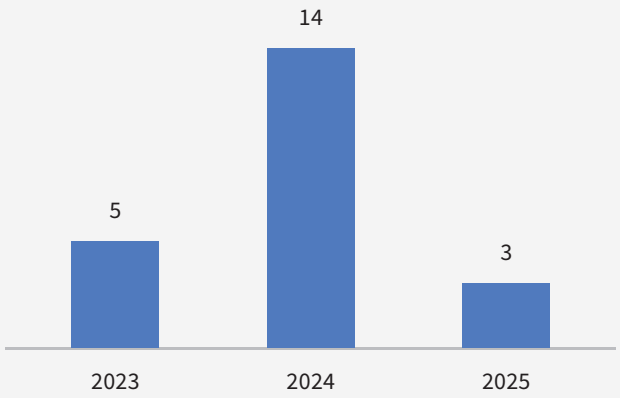
Súčasťou cieľov KCCKB v roli Národného koordinačného centra v roku 2025 bolo aj intenzívne budovanie odbornej kyberkomunity. Toto úsilie viedlo k vytváraniu silných partnerstiev, zdieľaniu osvedčených postupov a zvýšeniu povedomia o dôležitosti kybernetickej bezpečnosti medzi podnikmi, akademickou sférou a verejným sektorom. Členmi európskej komunity kybernetickej bezpečnosti podľa Nariadenia (EÚ) č. 2021/887 sa prostredníctvom NCC-SK stalo už 197 slovenských subjektov.

KCCKB k EÚ projektom zorganizovalo viacero vzdelávacích a networkingových aktivít, ako boli: Cyberbrunch, Cyberbreakfast, séria online webinárov NIS2, stretnutia pracovných skupín Audítorov a Manažérov kybernetickej bezpečnosti, semináre s témou transpozície smernice NIS2, webináre s témou Ako správne napísať projekt a získať európske financovanie. Celkovo sa na uvedených aktivitách počas roku 2025 zúčastnilo vyše 3-tisíc účastníkov.

Významným aspektom Národného koordinačného centra v medzinárodnom pôsobení bola účasť v riadiacich štruktúrach na európskej úrovni, najmä prostredníctvom participácie na zasadnutiach Správnej rady ECCC a stretnutiach siete NCC. KCCKB sa v úlohe NCC aktívne zapájalo aj do činností pracovných skupín ECCC, v rámci ktorých prispievalo k výmene informácií, koordinácii aktivít a zdieľaniu skúseností v oblastiach relevantných pre rozvoj kybernetickej bezpečnosti na európskej úrovni. Osobitná pozornosť bola venovaná bilaterálnej spolupráci s českým národným koordinačným centrom NCC-CZ. V roku 2025 bola táto spolupráca formalizovaná podpisom memoranda o porozumení, ktoré vytvorilo rámec pre systematickú výmenu informácií, koordináciu aktivít a prípravu spoločných iniciatív.

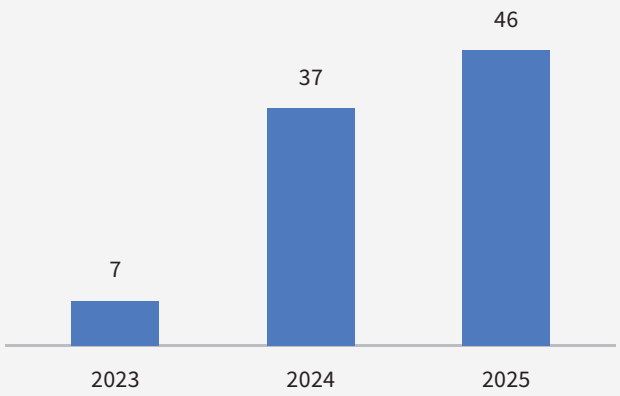
Vývoj počtu certifikovaných audítorov a manažérov kybernetickej bezpečnosti

Medziročný nárast počtu certifikovaných audítorov



Počet certifikovaných osôb sa prostredníctvom Kompetenčného centra v roku 2025 navýšil o troch certifikovaných audítorov (celkový počet 80) a 46 certifikovaných manažérov (celkový počet 100).

Medziročný nárast počtu certifikovaných manažérov



KCCKB v roku 2025 nepredĺžilo akreditáciu na certifikáciu manažérskych systémov.

Expertné činnosti

V rámci expertných činností pre verejnú správu vykonalo KCCKB 39 auditov kybernetickej bezpečnosti, tri konzultačné projekty a boli vykonané NEV merania u viac ako 50 subjektov.

Znalecká organizácia KCCKB v roku 2025 vytvorila spolu 20 znaleckých posudkov.

Kompetenčné centrum bolo úspešné aj v oblasti vzdelávania dospelých ako Certifikovaná vzdelávacia inštitúcia. Vzhľadom na novelu zákona o kybernetickej bezpečnosti a príslušných vyhlášok, boli aktualizované sylaby takmer všetkých vzdelávacích produktov. Do portfólia vzdelávania pribudli nové špecializované kurzy, workshop Riešenie incidentov a kurz a workshop Bezpečnosť AI.

Za rok 2025 bolo realizovaných celkovo 34 školení, ktorých sa zúčastnilo 438 účastníkov. Portfólio odborných školení zahŕňalo kurzy:

- Základy KB
- Manažér KB 1 a 2
- Audítor KB
- 7 špecializačných kurzov a workshopov
- Kurz manažérstva informačnej bezpečnosti podľa ISO/IEC 27001:2022
- Webinár Prehľad kybernetickej bezpečnosti

Odborné a informačné aktivity

Kompetenčné centrum sa aktívne zúčastňovalo na konferenciách a podujatiach na Slovensku aj v zahraničí. Celkovo jeho zástupcovia v roku 2025 KCCKB uskutočnili vyše 50 odborných prednášok na odborných konferenciách, workshopoch, seminároch, ako aj na pôde vysokých škôl, v SR aj v zahraničí. V rámci publikačných aktivít vydávalo Kompetenčné centrum odborné články, sylaby a letáky na účely zvyšovania bezpečnostného povedomia. V rámci adventu 2025 bola vydaná séria článkov pre občanov SR v kooperácii so Slovenskou bankovou asociáciou na ochranu pred najčastejšími útokmi, ktoré cielia na financie obyvateľov:

- Investičný podvod – lákavá ilúzia rýchleho zisku
- Phishing - ako funguje, ako ho rozpoznať a ako sa chrániť
- Whatsapp podvod – hlasujte za tanečnicu
- Útoky na online bazároch – aj predaj môže byť nebezpečný

Kompetenčné centrum vydalo v roku 2025 knihu Návrh vzdelávacích osnov pre II. st. ZŠ pre oblasť informačnej a kybernetickej bezpečnosti a odporúčané moderné didaktické metódy s príkladmi. Kniha nastavila základ vzdelávacích osnov pre druhý stupeň základných škôl.

V rámci odbornej činnosti KCCKB podporilo NBÚ vytvorením Metodiky analýzy rizík kybernetickej bezpečnosti a Odporúčaní pre kryptografické algoritmy.

Už každoročne sú na základe zadania KCCKB spracované prieskumy stavu kybernetickej bezpečnosti, vydané následne aj vo forme verejného dokumentu. V roku 2025 bol uskutočnený prieskum verejnej mienky medzi verejnosťou na vzorke tisíc respondentov.

Aj v roku 2025 Kompetenčné centrum ďalej rozširovalo okruh organizácií, s ktorými uzatvorilo spoluprácu formou podpisu memoranda, hlavne akademickí partneri a partneri Slovak Cyber Teamu.

Slovak Cyber Team

Kompetenčné centrum s podporou SK-CERT rozširuje tím mladých kybertalentov, ktorí Slovensko úspešne reprezentovali na viacerých on-site CTF turnajoch (Dublin Zerodays CTF 1. miesto, Bukurešť DCTF 4. miesto) a na množstve online CTF turnajov.

Slovak Cyber Team skončil v októbri 2025 na podujatí ECSC vo Varšave na fantastickom 4. mieste spomedzi 39 národných tímov. Aktivitu zastrešila ENISA a ECCC. Slovak Cyber Team reprezentovalo desať mladých talentov – deväť chlapcov a jedno dievča. Na súťaž sa tím pripravoval niekoľko mesiacov. V júli sa zúčastnili medzinárodného bootcampu vo Viedni a následne šiestich tréningových bootcampov v Brunovciach. Tím sa aktívne pripravoval na účasť na ECSC v roku 2026.

10. ČO OČAKÁVAŤ V ROKU 2026?

Hlásenia kybernetických bezpečnostných incidentov a štatistické údaje za rok 2025 potvrdzujú rast počtu aj závažnosti incidentov, ako aj zvyšovanie úrovne spôsobilostí útočníkov. Narastá počet aktívne zneužívaných zraniteľností, pričom skracovanie času medzi ich zverejnením a zneužitím zvyšuje tlak na rýchlosť reakcie. Tento trend bude pokračovať aj v roku 2026 a bude ďalej posilnený rozvojom AI. Tá zásadne ovplyvňuje charakter kybernetických hrozieb tým, že umožňuje automatizáciu útokov, zvyšuje ich rozsah a efektivitu, zlepšuje presvedčivosť phishingu a škodlivého obsahu.

Slovenská republika má definovaný strategický rámec kybernetickej bezpečnosti prostredníctvom Národnej stratégie kybernetickej bezpečnosti SR pre roky 2026 až 2030. Táto stratégia prinesie systematickejší prístup k riadeniu kybernetických rizík, posilnenie preventívnych mechanizmov, opatrenia zamerané na ďalší rozvoj a jasnejšie vymedzenie zodpovedností jednotlivých aktérov. Nadväzujúci akčný plán bude reflektovať na aktuálne hrozby, legislatívne požiadavky a potrebu efektívnej koordinácie medzi verejným a súkromným sektorom.

Súbežne dochádza k sprísňovaniu regulačného rámca na úrovni Európskej únie. Rok 2026 bude predstavovať významný míľnik vo vývoji kybernetickej bezpečnosti v Európskej únii, pričom jeho charakter bude formovaný najmä prehlbujúcou sa reguláciou, rastúcimi geopolitickými rizikami a snahou o posilnenie technologickej suverenity. V oblasti legislatívy bude pokračovať trend harmonizácie a zjednodušovania regulačného prostredia na úrovni EÚ, ako aj SR. Osobitný význam bude mať aj rozvoj certifikačných orgánov a schém, ktoré zohrávajú čoraz dôležitejšiu úlohu pri zabezpečovaní dôvery v digitálne produkty a služby.

Významnú úlohu bude zohrávať aj ekonomický rozmer kybernetickej bezpečnosti, a to najmä v podobe zvyšovania investícií do ochrany kritickej infraštruktúry, zabezpečenia dodávateľských reťazcov a rozvoja vlastných technologických kapacít. Neoddeliteľnou súčasťou tohto vývoja bude aj dôraz na rozvoj ľudského kapitálu, keďže nedostatok kvalifikovaných odborníkov v oblasti kybernetickej bezpečnosti predstavuje dlhodobú výzvu. Riešenie si vyžaduje systematické posilňovanie vzdelávania na úrovni stredných a vysokých škôl, rozširovanie špecializovaných študijných programov a intenzívnejšiu spoluprácu medzi akademickou obcou.

Celkový vývoj bude zároveň ovplyvnený geopolitickým posunom, ktorý sa prejavuje rastúcim významom kybernetického priestoru ako strategickej domény, v ktorej dochádza k čoraz intenzívnejšej interakcii medzi bezpečnostnými, ekonomickými a politickými záujmami štátov. Kybernetická bezpečnosť sa tak v roku 2026 bude čoraz viac prelínať s otázkami obrany, zahraničnej politiky a ochrany hospodárskych záujmov, čo si vyžaduje komplexný a koordinovaný prístup. Tento trend zvyšuje význam medzinárodnej spolupráce a zdieľania informácií v rámci Európskej únie a NATO.