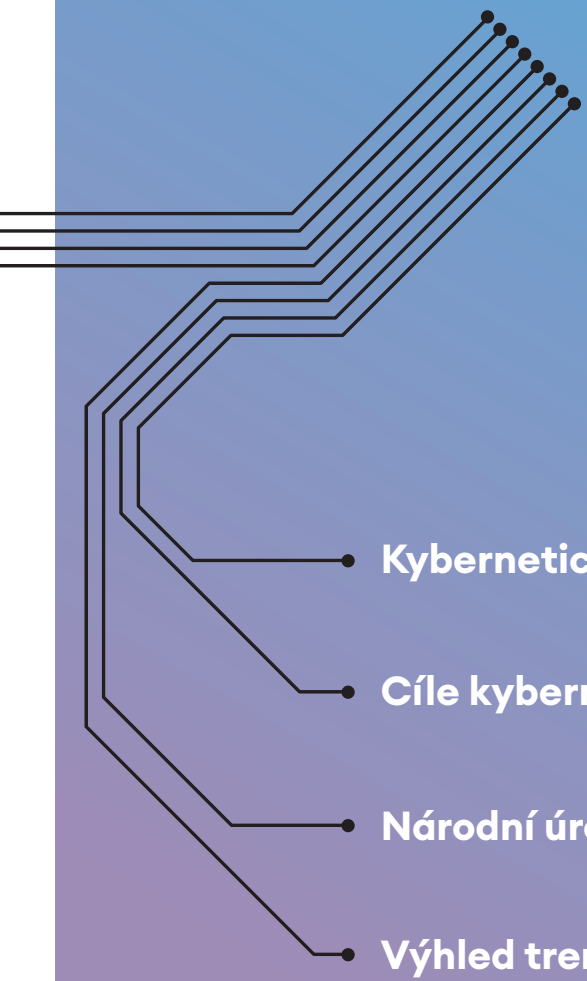
Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2024



- Kybernetické hrozby a aktéři
- Cíle kybernetických útoků
- Národní úroveň kybernetické bezpečnosti
- Výhled trendů na roky 2025 a 2026

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

Úvodní slovo ředitele

Ing. Lukáš Kintr
ředitel Národního úřadu pro kybernetickou a informační bezpečnost

Vážené dámy, vážení pánové,
je mi potěšením a ctí vám představit Zprávu o stavu kybernetické bezpečnosti České republiky za rok 2024, který byl plný výzev i pozitivních trendů. Děkuji za váš zájem o tuto klíčovou oblast, jejíž význam v životě naší společnosti stále roste.

V roce 2024 NÚKIB zaznamenal rekordní počet kybernetických bezpečnostních incidentů, a to 268. Na první pohled se toto číslo může zdát alarmující, ale nárůst je ve srovnání s předchozím rokem spíše drobný. Podstatný je pokles závažnosti dopadů těchto incidentů, která se již tři roky po sobě snižuje. V roce 2024 jsme zaznamenali pouze jeden velmi významný incident, což je velkým zlepšením oproti minulým obdobím. Počet významných incidentů klesl o více než polovinu a to je pozitivní trend.

Mezi nejčastější incidenty patřily DDoS kampaně cizojazyčných hacktivistických skupin. Tyto útoky způsobují krátkodobé výpadky a narušení dostupnosti napadených webových stránek, ale jejich dopad na kritickou infrastrukturu je minimální. Naopak jako velmi závažná hrozba se i nadále ukazují ransomwarové útoky, kterých bylo v porovnání s DDoS útoky sice méně, ale jejich reputační nebo finanční újma může být nevyčíslitelná. Co se týká incidentů, nelze nezmínit výpadek CrowdStrike. Ačkoli se nejednalo o cílený útok aktérů, technický výpadek zapříčiněný chybnou aktualizací otestoval připravenost a spolupráci nejen na národní, ale také na mezinárodní úrovni. Stejně jako v předchozích letech i v roce 2024 pokračovala činnost aktérů sponzorovaných státem. Nejvýrazněji se projevily zejména kyberútoky skupin, které působí pod ruskými zpravodajskými službami. Česká republika se v uplynulém roce zapojila do mezinárodní operace proti Ruskem sponzorované skupině APT28 a její škodlivé aktivity v kyberprostoru také spolu s dalšími státy a mezinárodními partnery odsoudila a přiřkla Ruské federaci.

Velkým úspěchem uplynulého roku je stabilizace v oblasti kyberkriminality, a to díky Policii ČR (dále jen „PČR“). Počet nově registrovaných trestných činů v kyberprostoru klesl, a to nejen pod úroveň roku 2023, ale také roku 2022. Zdá se, že osvětové kampaně, na kterých spolupracujeme s dalšími partnery, začínají pomalu přinášet ovoce. Neusínáme na vavřínech, protože s rychlým vývojem a masivním využíváním umělé inteligence se zvyšuje také sofistikovanost jednání kyberútočníků.

V průběhu uplynulého roku jsme ušli kus cesty i v oblasti legislativy. Jedním z milníků bylo schválení návrhu zákona o kybernetické bezpečnosti vládou – v tuto chvíli čekáme na publikaci zákona ve Sbírce zákonů, čímž bude uveden v platnost. Dalším důležitým krokem bylo dokončení návrhu Národní politiky koordinovaného zveřejňování zranitelností, která má podpořit identifikaci zranitelností v ICT produktech bez obavy z negativních právních dopadů pro jejich objevitele. Na mezinárodním poli jsme se pak aktivně zapojili do vyjednávání kolem nařízení o kybernetické odolnosti, jejímž cílem je zvýšit kybernetickou bezpečnost softwarových a hardwarových produktů.

V souvislosti s nárůstem počtu povinných subjektů NÚKIB intenzivně připravuje e-learningový kurz train-the-trainer. Jeho cílem je naučit zájemce připravit efektivní netechnické cvičení přímo v jejich domovské organizaci.

Těší mě, že náš každoroční průzkum mezi organizacemi ukazuje nejen pokračující trend v navyšování rozpočtů na kybernetickou bezpečnost, ale i pozvolný růst počtu organizací, které tyto rozpočty navyšují. Dlouhodobým problémem ale zůstává nedostatek kvalifikovaných odborníků a jejich nedostatečné ohodnocení. S druhým zmíněným nedostatkem se potýká především veřejný sektor – jednak je problematické obsadit specializované pozice, jednak zaměstnanci z důvodu nedostatečného finančního ohodnocení odcházejí. Důležitost kybernetické bezpečnosti neustále roste a s ní i potřeba kvalifikovaných specialistů. Tuto situaci je nutné aktivně řešit.

Rok 2024 nám přinesl nejen výzvy, ale i příležitosti k posílení našich kapacit a zajištění bezpečnosti v kybernetickém prostoru. Je na nás, abychom se těmto výzvám postavili čelem a společně budovali bezpečnější budoucnost pro všechny.

Obsah

O dokumentu

Dotazníkové šetření

NÚKIB na začátku roku 2024 rozeslal dotazník se 63 otázkami, a to jak subjektům regulovaným podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „zákon o kybernetické bezpečnosti“), tak i řadě dalších klíčových institucí a organizací, které zákonem o kybernetické bezpečnosti regulovány nejsou. Otázky se týkaly širokého záběru témat, například kybernetických útoků, nákladů na kybernetickou bezpečnost, personálních kapacit v oblasti kybernetické bezpečnosti, uživatelů, technologií i zavedených procesů. Dotazník vyplnilo celkem 415 subjektů, z toho 324 regulovaných a 91 neregulovaných. Ze získaných dat NÚKIB čerpal informace pro potřeby Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2024 (dále jen „Zpráva“). Veškeré údaje z dotazníků jsou anonymizovány.

Proces hodnocení

Hodnocení stavu kybernetické bezpečnosti v ČR je založeno na analytickém procesu, který zahrnuje kvantitativní i kvalitativní vyhodnocení dat z vyplněných dotazníků, poznatky NÚKIB, informace poskytnuté partnery a další dostupné informace z otevřených zdrojů. NÚKIB neměl možnost data poskytnutá respondenty kontrolovat ani hlouběji ověřovat uvedená tvrzení. Analytické závěry obsažené ve Zprávě jsou založeny na premise, že odpovědi v dotaznících nejsou zkresleny. K vyjádření analytického hodnocení používáme pravděpodobnostní výrazy (viz níže).

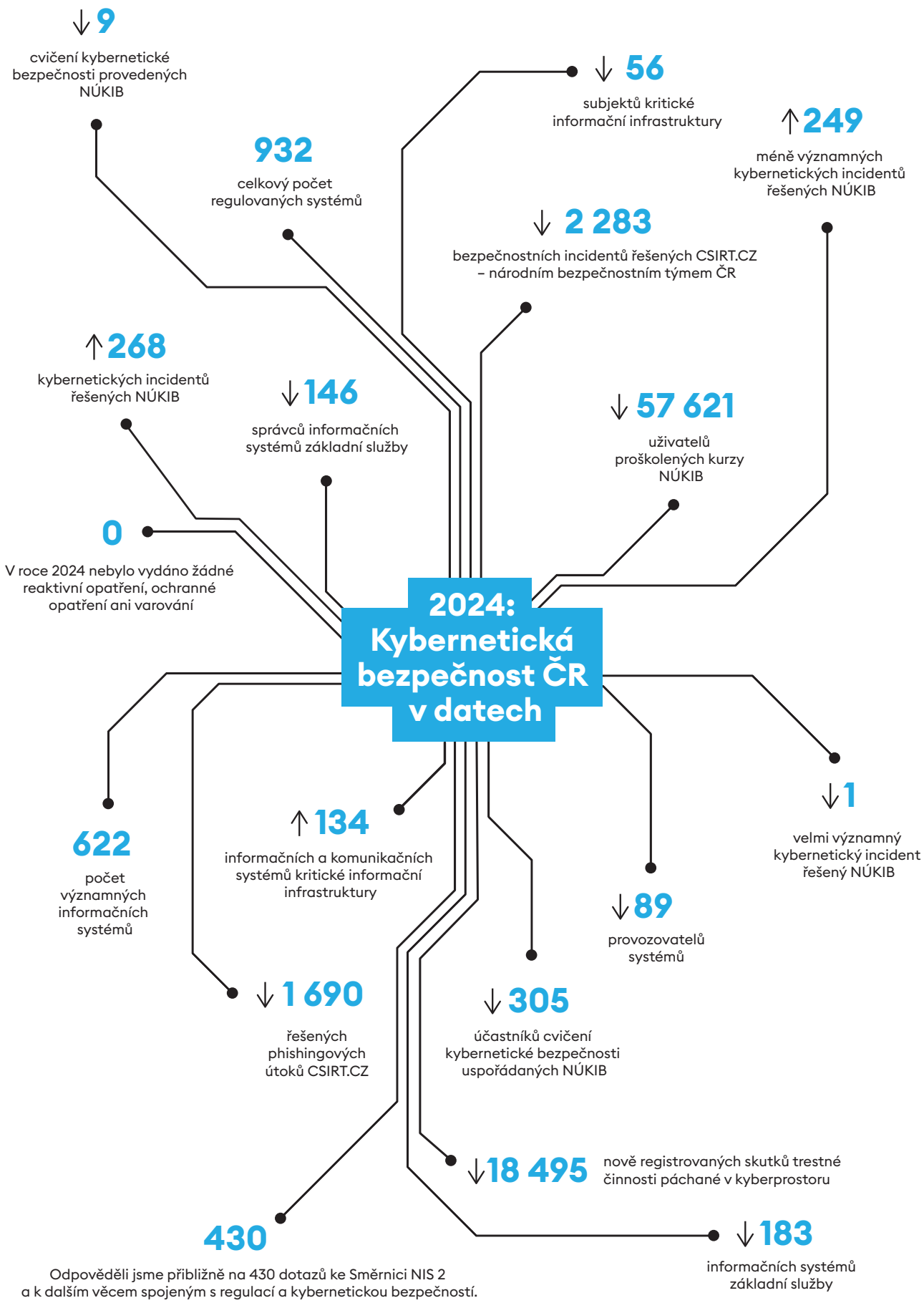
Zpráva neposkytuje vyčerpávající seznam všech aktivit v oblasti kybernetické bezpečnosti. Účelem dokumentu je popsat a vyhodnotit hrozby v kybernetickém prostoru, s nimiž se ČR v roce 2024 potýkala, stejně jako aktivity, které napomáhají jejich zmírnění.

Pravděpodobnostní výrazy použité ve Zprávě o stavu kybernetické bezpečnosti České republiky za rok 2024

Téměř jistě	90–100 %
Velmi pravděpodobně	75–85 %
Pravděpodobně	55–70 %
Nelze vyloučit / Reálná možnost	25–50 %
Nepravděpodobně	15–20 %
Velmi nepravděpodobně	0–10 %

Seznam použitých zkratek

AI	umělá inteligence (artificial intelligence)
ČLR	Čínská lidová republika
ČR	Česká republika
DoS/DDoS	Denial of Service / Distributed Denial of Service
ENISA	Agentura Evropské unie pro kybernetickou bezpečnost
EU	Evropská unie
GRU	Hlavní správa generálního štábu Ozbrojených sil Ruské federace (Главное управление Генерального штаба Вооружённых Сил России)
ISVS	informační systémy veřejné správy
NATO	Severoatlantická aliance
NIS2	Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022, o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS2)
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
PCSC	Prague Cyber Security Conference
PČR	Policie České republiky



Vizualizace 1: Kybernetická bezpečnost ČR v datech

Shrnutí Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2024

Nárůst počtu evidovaných kybernetických incidentů i pokles jejich závažnosti

V minulém roce Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) evidoval dosud nejvíce kybernetických bezpečnostních incidentů (dále jen „incident“), a to 268. Oproti roku 2023, kdy bylo evidováno 262 incidentů, se však jedná pouze o drobný nárůst. **Závažnost dopadů evidovaných incidentů klesá již třetím rokem v řadě.** V roce 2024 NÚKIB evidoval pouze jeden velmi významný incident. Významných incidentů bylo zaznamenáno 18, což oproti 43 z roku 2023 představuje pokles o více než polovinu.

Nejčastější typy útoků

Významnou část incidentů tvoří DDoS útoky, přičemž za většinou z nich stojí ruskojazyčné hacktivistické skupiny, zejména NoName057(16). Její škodlivé aktivity však nadále nepůsobily zasaženým cílům škody nad rámec krátkodobých výpadků napadených webů. **Nově zaznamenaným trendem je nárůst počtu hacktivistických skupin, které útočí na slabě zabezpečené systémy operačních technologií (OT) a SCADA systémy průmyslových podniků v západních zemích.**

V roce 2024 i nadále přetrvávala hrozba ransomwarových útoků, přičemž v posledním čtvrtletí došlo k jejich strmému nárůstu. **V říjnu 2024 NÚKIB zaregistroval 7 ransomwarových útoků, což představuje nejvyšší evidovaný počet za měsíc.**

Při pohledu na incidenty z perspektivy respondentů našeho dotazníkového šetření vyplývá, že nejčastějšími druhy útoků zůstávají phishing a podvodné e-maily. Přibližně polovina organizací se též setkala s útoky pomocí malwaru, skenováním vnějšího rozsahu sítě nebo spear-phishingem.

Zákon o kybernetické bezpečnosti

Rok 2024 také představuje zlom pro návrh nového zákona o kybernetické bezpečnosti. Návrh byl projednán Legislativní radou vlády a následně vládou schválen a postoupen Poslanecké sněmovně Parlamentu České republiky. V Poslanecké sněmovně byl zákon projednán ve Výboru pro bezpečnost, Výboru pro obranu a v Hospodářském výboru. K návrhu zákona byly ve výborech a při druhém čtení načteny pozměňovací návrhy. V současné chvíli zákon čeká na dokončení legislativního procesu v obou komorách Parlamentu ČR. NÚKIB k zákonu zpracoval řadu podpůrných materiálů, některé i v angličtině.

Nařízení o kybernetické odolnosti

NÚKIB se v minulém roce taktéž aktivně zapojoval do vyjednávání nařízení o kybernetické odolnosti, jež představuje průlomovou unijní legislativu. Její cíl je zvýšit bezpečnost pomocí zavedení požadavků na kybernetickou bezpečnost softwarových a hardwarových produktů.

Projekt BIVOJ

Loňský rok byl milníkem i pro Projekt BIVOJ, konkrétně byly definovány úkoly, které mají projekt posunout do dalších fází. **Zásadními kroky bylo zpracování studií proveditelnosti architektonického řešení a strategického směřování a ustanovení Řídicího výboru projektu.**

Národní politika koordinovaného zveřejňování zranitelností

V roce 2024 NÚKIB dále dokončil přípravu návrhu Národní politiky koordinovaného zveřejňování zranitelností, jejímž cílem je podporovat nalézání zranitelností v ICT produktech napříč subjekty v ČR bez hrozby negativních právních dopadů pro objevitele zranitelností. **V návrhu nového zákona o kybernetické bezpečnosti je určen koordinátorem pro účely koordinovaného zveřejňování zranitelností vládní CERT a jakákoli osoba mu tak bude moci i anonymně hlásit nalezené zranitelnosti.**

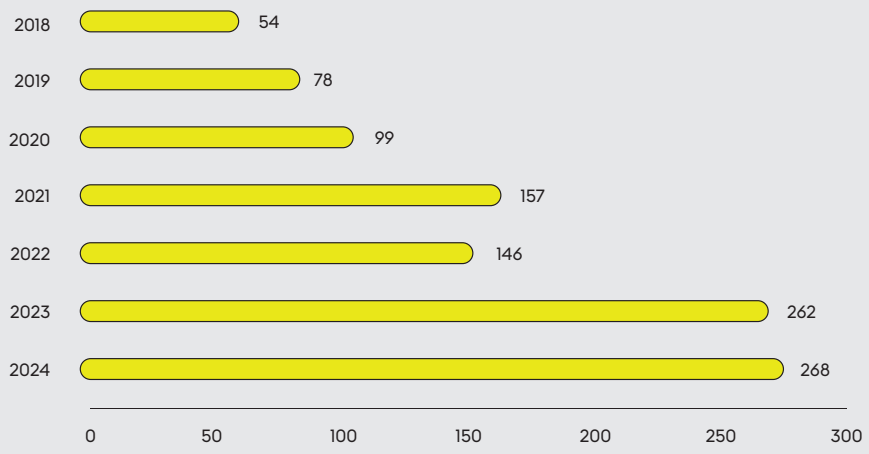
Osvětová činnost a cvičení

V neposlední řadě NÚKIB pokračoval v osvětové činnosti a organizaci cvičení kybernetické bezpečnosti. V oblasti cvičení se NÚKIB v loňském roce zaměřil na koncepční činnost v souvislosti s nárůstem počtu povinných subjektů. **Jedním z výsledků této činnosti bude e-learningový kurz train-the-trainer, jehož prostřednictvím se zájemci naučí, jak připravit efektivní netechnické cvičení v domovské organizaci.**

1 Kybernetická bezpečnost ČR v roce 2024 z pohledu NÚKIB[1]

[1] Prezentované informace vycházejí ze zdrojů NÚKIB a z vyhodnocení 415 dotazníků (viz část O dokumentu).

NÚKIB v roce 2024 evidoval celkem 268 kybernetických bezpečnostních incidentů, což je dosud nejvyšší evidovaná hodnota.

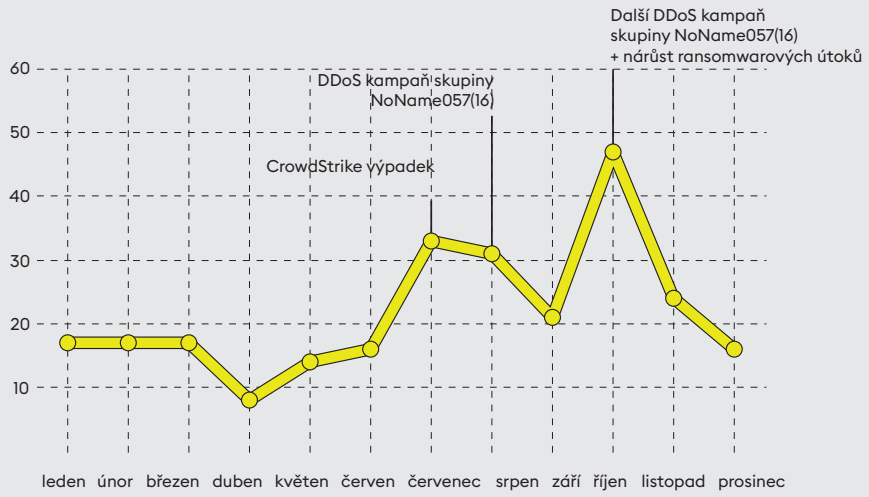


Graf 1: Vývoj počtu incidentů evidovaných NÚKIB v letech 2018–2024

Oproti roku 2023, kdy bylo evidováno 262 incidentů, se však jedná o pouze drobný nárůst.

Skladba incidentů je velmi podobná té z minulého roku, kdy největší podíl, 43 %, tvoří útoky na dostupnost.

I v roce 2024 stojí za většinou evidovaných DDoS útoků ruskojazyčná hacktivistická skupina NoName057(16).



Celkem 268 incidentů

Graf 2: Vývoj počtu incidentů evidovaných NÚKIB za rok 2024

V roce 2024 byla většina evidovaných DDoS útoků provedena převážně ruskojazyčnými hacktivistickými skupinami, jejichž činnost byla velmi často koordinována skupinou NoName057(16). Potvrzuje se tak nový trend spojování hacktivistických skupin do společných operací. Ovšem i nadále její škodlivé aktivity nepůsobily zasaženým subjektům větší škody než krátkodobé výpadky napadených webů. Skupina však prokazuje kontinuálně vysoké operační tempo, přičemž během října v tuzemsku stála za většinou z rekordních 30 DDoS útoků za daný měsíc.

Novým trendem v kontextu činnosti hacktivistů byl růst počtu aktérů, kteří útočí na slabě zabezpečené systémy operačních technologií (OT) a SCADA systémy průmyslových podniků v západních zemích. Jeden incident tohoto typu byl evidován i v ČR (více viz kapitola Výhled trendů v kybernetické bezpečnosti).

Po celý rok též přetrvávala hrozba ransomwarových útoků. NÚKIB jich evidoval nižší jednotky každý měsíc [reálný počet útoků mimo viditelnost NÚKIB je téměř jistě (90–100 %) vyšší].

Ačkoli ransomwarové útoky stály za necelými 11 % všech evidovaných incidentů, jejich dopady dokazují, že jde o velmi závažnou hrozbu. Kromě úniku citlivých informací mohou vést k zašifrování dat, ale i dočasnému pozastavení výroby nebo poskytování služeb. Vše zmíněné s sebou samozřejmě nese reputační nebo finanční újmu.

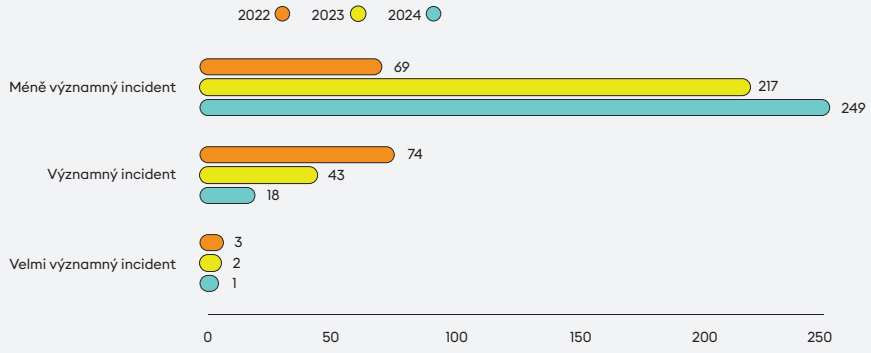
Během podzimu NÚKIB evidoval více než dvojnásobný nárůst těchto útoků oproti průměrným hodnotám – nejspíš se však nejednalo o koordinovanou kampaň, ale o zvýšenou aktivitu různých útočníků (více viz kapitola: Kybernetické hrozby a aktéři).

Specifickou událostí s celosvětovým dopadem byl výpadek EDR softwaru společnosti CrowdStrike, který v důsledku chybné aktualizace v červenci způsobil rozsáhlé výpadky systémů napříč sektory a následnou nedostupnost různých služeb.

V tuzemsku byly dopady události menší než v jiných západních státech, přesto však NÚKIB v této souvislosti evidoval celkem devět incidentů.

Z pohledu závažnosti evidovaných incidentů je již třetím rokem patrný trend snižování jejich dopadů. Velmi významný incident byl za rok 2024 evidován pouze jeden, významných incidentů bylo 18, tj. více než o polovinu méně než v roce 2023, a méně významných incidentů přibylo na celkový počet 249. **Tento trend byl i během uplynulého roku dán zejména opakovanými DDoS útoky v kontextu války na Ukrajině a v menší míře potom i výpadky dostupnosti služeb v důsledku zářijových povodní nebo výpadku CrowdStrike.** Celkově byla kategorie Dostupnost (DDoS, DoS, miskonfigurace nebo technické závady) zastoupena 62 %. Samotné útoky na dostupnost potom tvořily 43 % incidentů uplynulého roku.

Z pohledu závažnosti evidovaných incidentů je již třetím rokem patrný trend snižování jejich dopadů.



Graf 3: Meziroční srovnání závažnosti incidentů evidovaných NÚKIB v letech 2022–2024

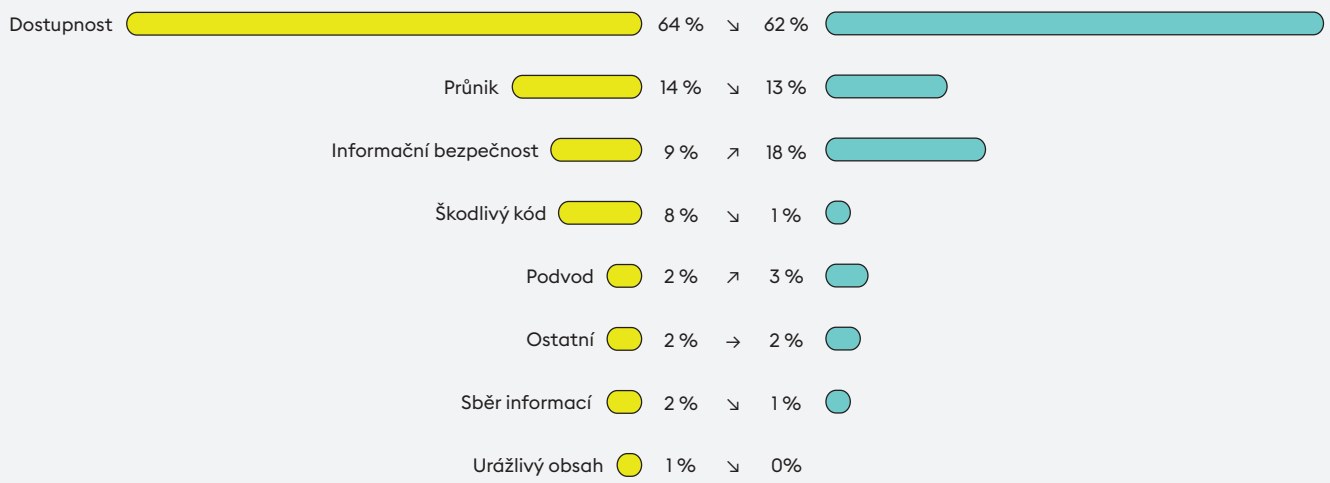
V blízké budoucnosti lze očekávat zejména pokračování současných trendů. Bude docházet k incidentům spojeným s geopolitickou situací, a to nikoliv pouze v kontextu války na Ukrajině.

Dále lze očekávat kontinuální výskyt ransomwarových útoků s možnými výkyvy v kontextu zvýšené aktivity jednotlivých aktérů, jako tomu bylo v roce 2024. Nelze vyloučit (40–50 %) ani cílenou kampaň jedné skupiny. **Přestože sofistikované kampaně státních aktérů spojovaných s Ruskou federací nebo Čínskou lidovou republikou (dále jen „ČLR“) tvoří velmi malé procento celkového počtu incidentů, jejich závažnost je obvykle vysoká.** Celková situace pak může být ovlivněna různými specifickými událostmi, jako jsou masivně zneužívané zranitelnosti, výpadky typu CrowdStrike nebo právě významnými kampaněmi státních a nestátních aktérů.

Posledním faktorem je také očekávaná účinnost nového zákona o kybernetické bezpečnosti. Ten s sebou přinese nárůst regulovaných subjektů, což bude velmi pravděpodobně (75–85 %) znamenat nárůst nejen počtu evidovaných incidentů, ale může proměnit i skladbu jejich závažnosti.

Klasifikace kybernetických incidentů nahlášených NÚKIB [2]

Procentuální zastoupení v incidentech



Dostupnost – např. narušení dostupnosti způsobené DoS/DDoS útokem nebo sabotáží
Průnik – např. kompromitace aplikace nebo uživatelského účtu
Informační bezpečnost – např. neautorizovaný přístup k datům, neautorizovaná změna informace
Škodlivý kód – např. virus, červ, trojský kůň, dialer, spyware
Podvod – např. phishing, krádež identity nebo neoprávněné využití ICT
Pokus o průnik – např. pokus o zneužití zranitelnosti, pokus o přihlášení apod.
Sběr informací – např. skenování, sniffing, sociální inženýrství

Vizualizace 2: Klasifikace kybernetických incidentů nahlášených NÚKIB

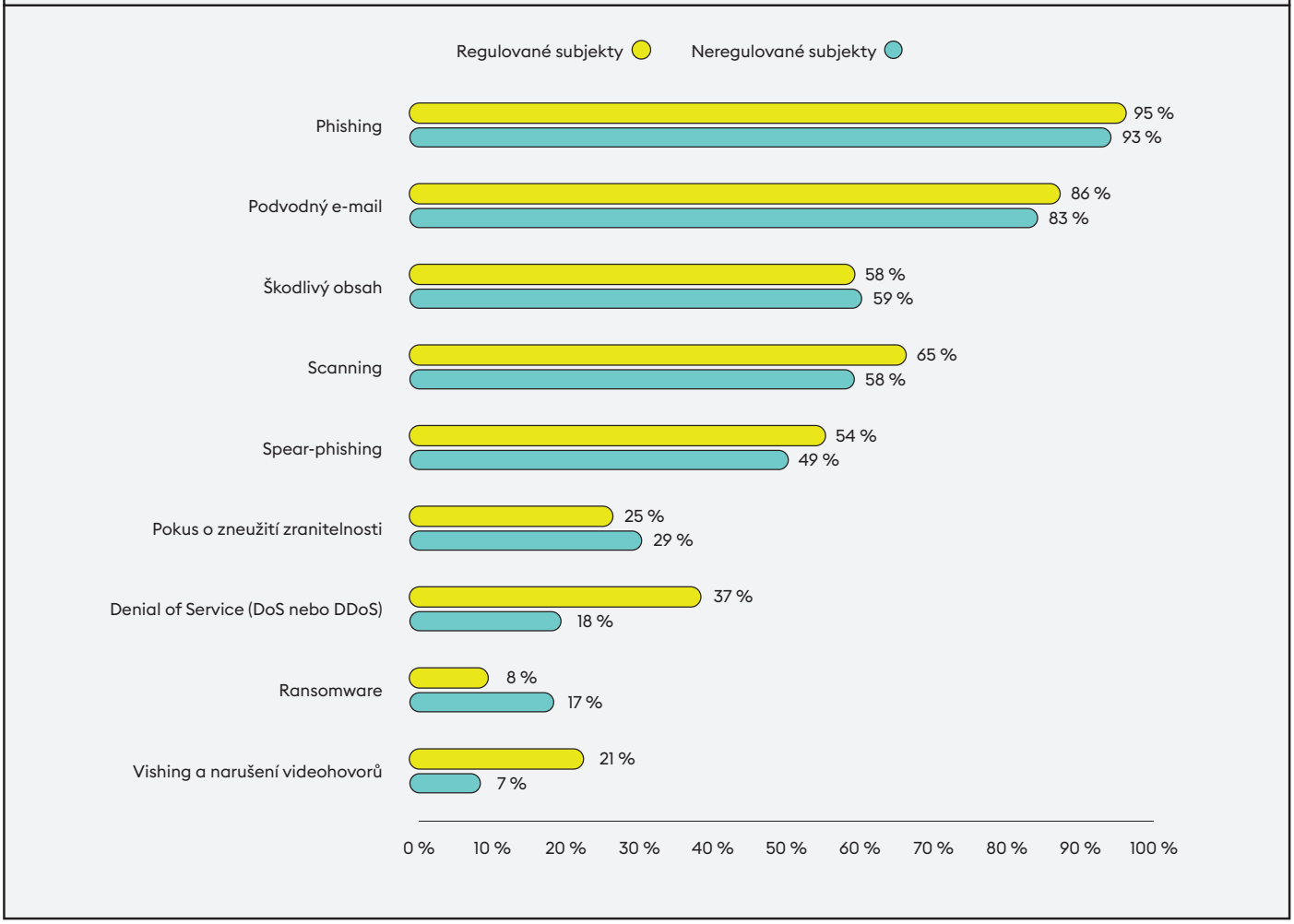
Z hlediska klasifikace incidentů nejvíce převažovaly incidenty cílící na dostupnost, což odpovídá vysokému počtu zaznamenaných DDoS útoků. Tato kategorie nicméně obsahuje také řadu incidentů, za kterými nestojí útoky, ale například technické chyby vedoucí k výpadku systémů. Druhou nejpočetnější pak byla kategorie Informační bezpečnost. Do ní spadaly zpravidla ransomwarové útoky. Tato kategorie tak oproti roku 2023 předstihla kategorii Průnik, do které se řadí zejména phishingové útoky vedoucí ke kompromitaci e-mailových nebo jiných účtů a která byla v roce 2024 třetí nejčastější.

[2] Klasifikace kybernetických incidentů je založena na taxonomii ENISA: Reference Incident Classification Taxonomy — ENISA (europa.eu).

Incidenty pohledem subjektů

Phishingové nebo jinak podvodné e-maily a výpadky dostupnosti jsou hlavní hrozbou pro většinu organizací.

DDoS útoky zaznamenalo o téměř 20 % víc regulovaných subjektů. Naopak ransomwarové útoky uvedlo o necelých 10 % víc organizací, které nejsou zákonem regulovány.



Graf 4 : Kategorie nejčastějších typů kybernetických útoků na regulované a neregulované subjekty

Při pohledu na incidenty z perspektivy respondentů našeho dotazníkového šetření vyplývá, že nejčastějším druhem útoků zůstává phishing, se kterým se setkalo více než 90 % dotázaných organizací.

Přibližně polovina organizací se též setkala s útoky pomocí malwaru, skenováním vnějšího rozsahu sítě nebo spear-phishingem.

Více než 80 % organizací též zaznamenalo podvodné e-maily, primárně v kontextu snahy útočníků získat finanční prostředky prostřednictvím taktiky sociálního inženýrství.

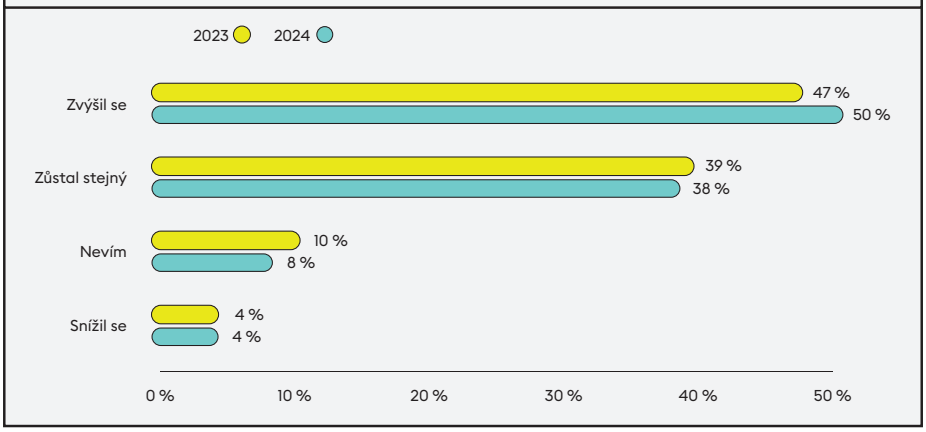
Při porovnání odpovědí regulovaných a neregulovaných organizací podle zákona o kybernetické bezpečnosti jsou patrné dva výraznější rozdíly v zaznamenaných útocích. **DDoS útoky zaznamenalo o téměř 20 % regulovaných subjektů víc. Naopak ransomwarové útoky uvedlo o necelých 10 % víc organizací, které nejsou zákonem regulovány.** To lze vysvětlit motivacemi původců obou útoků. Hactivistické skupiny cílí primárně na instituce veřejného sektoru, kdežto kyberkriminální skupiny spíše na soukromé společnosti s cílem získat finanční prostředky.

V kontextu nejzávažnějších detekovaných incidentů respondenti nejčastěji uváděli DDoS útoky, různé podoby podvodných e-mailů nebo phishingu, ale také výpadky dostupnosti služeb v důsledku technických závad. Přestože většina DDoS útoků, které NÚKIB za rok 2024 evidoval, nevedla k významným dopadům, data ukazují, že alespoň pro část subjektů mohou i takové útoky působit obtíže a narušení obvyklého provozu. Odpovědi též ukazují, že pro řadu organizací mohou významné incidenty vzniknout pouhou miskonfigurací nebo závadou, přičemž malá část respondentů též specificky zmiňovala výpadek společnosti CrowdStrike.

Třetina respondentů odpověděla, že v případě, že měl incident na organizaci dopad, se jednalo zejména o omezení služeb, což dále ilustruje význam dostupnosti služeb.

Finance: Rozpočty na kybernetickou bezpečnost postupně narůstají, ale méně se potkávají s reálnými potřebami

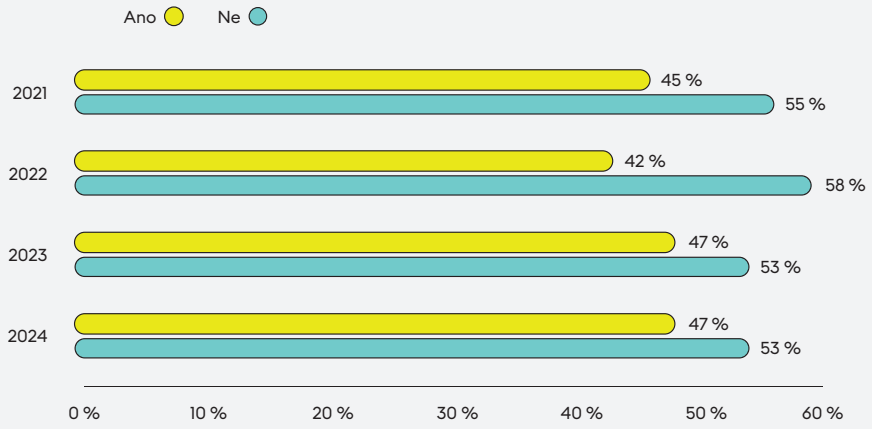
Dlouhodobým pozitivním trendem v posledních třech letech je navyšování rozpočtů alokovaných na kybernetickou bezpečnost jednotlivých dotazovaných organizací.



Graf 5: Jak se změnil rozpočet organizací alokovaný na kybernetickou bezpečnost v letech 2023 a 2024 (% respondentů)

Nejenom že přibližně polovina dotazovaných subjektů dlouhodobě hlásí, že se jejich rozpočet navyšuje, ale i jejich podíl pozvolna stoupá. To může značit jak mírně se zlepšující finanční situaci, tak i větší reflexi kybernetických hrozeb a důraz subjektů na kybernetickou bezpečnost.

Vývoj v roce 2024 ovšem vykazuje stagnaci ve vnímání rozpočtů na kybernetickou bezpečnost, což naznačuje, že dřívější pozitivní trend mohl narazit na svůj strop.



Graf 6: Považujete vyčleněné finance na zajištění kybernetické bezpečnosti své organizace za dostatečné? (% respondentů)

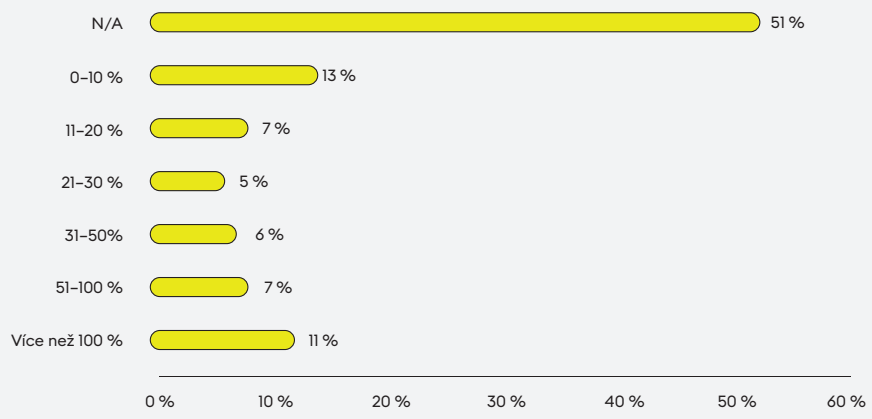
Po zlepšení v roce 2023, kdy podíl organizací vnímajících financování jako dostatečné vzrostl na 47 %, zůstává tato hodnota i v letošním roce beze změny.

Ačkoliv rozpočty na kybernetickou bezpečnost organizací rostou, nedaří se jim uspokojit poptávku. Klíčovým faktorem může být nejistota ohledně reálných potřeb. Přibližně polovina respondentů, kteří uvedli, že rozpočet není dostatečný, totiž nedokáže určit, o kolik by ho bylo potřeba navýšit, aby odpovídal jejich požadavkům (viz graf 7).

To může poukazovat na nedostatek jasných měřítek pro vyhodnocení odpovídajícího rozpočtu a potenciální rozdíl mezi očekáváními a skutečnými možnostmi.

Je proto možné, že organizace čelí nejen finančním omezením, ale i výzvě, jak efektivněji definovat a řídit své potřeby v oblasti kybernetické bezpečnosti.

Pokud hodnotíte rozpočet jako nedostatečný, o kolik procent by se měl navýšit?



Graf 7

Odborníci: Nedostatek kvalifikovaných odborníků a nízké platové ohodnocení jako hlavní faktory nízkých stavů

Dlouhodobým negativním trendem v kybernetické bezpečnosti, který pokračoval i v roce 2024, je nedostatečné finanční ohodnocení zaměstnanců.

Jako hlavní předpokládaný důvod odchodu pracovníků to uvedlo 19 % respondentů z dotazovaných organizací, je to tedy nejčastěji jmenovaným negativním faktorem.

V otázce nedostatečné obsazenosti pracovních míst jmenovali respondenti stejně jako v minulých letech jako klíčový faktor odrazující uchazeče v prvé řadě nedostačující finanční ohodnocení (viz graf 8), přičemž meziročně došlo k výraznému nárůstu z loňských 54 % až na 77 %.

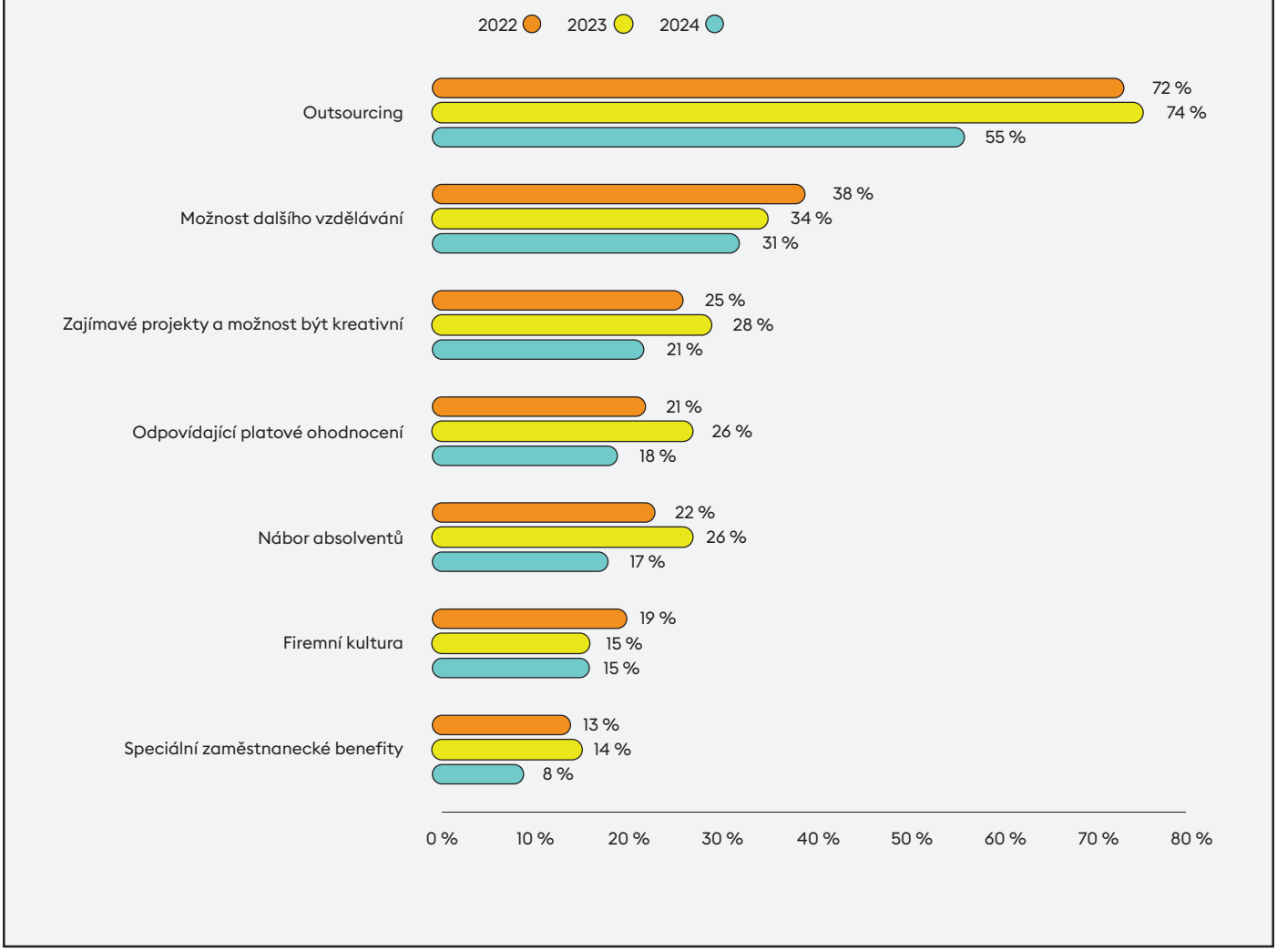
Mezi další faktory zařadili i chybějící perspektivu osobního nebo kariérního rozvoje a nedostatečné benefity.

Jaké jsou podle vás nejzásadnější faktory, které uchazeče při náborech na pozice v oblasti kybernetické bezpečnosti vaší organizace odrazují?

Graf 8

Až 55 % organizací pak problém nedostatku kvalifikované pracovní síly řeší prostřednictvím outsourcingu, což nadále představuje hlavní, avšak oproti dřívějším rokům méně využívanou strategii, za kterou následují příležitosti k dalšímu vzdělávání.

Jak se organizace v letech 2020–2024 snažily vypořádat s nedostatkem odborníků (% respondentů)



Graf 9

Mezi nejčastější pozice, které organizace nejvíce potřebují obsadit, patří bezpečnostní dohled SIEM, architekt nebo auditor kybernetické bezpečnosti a správa síťové infrastruktury.

Uživatelé: Větší počet organizací alokuje finanční prostředky na školení uživatelů a školení také probíhají častěji

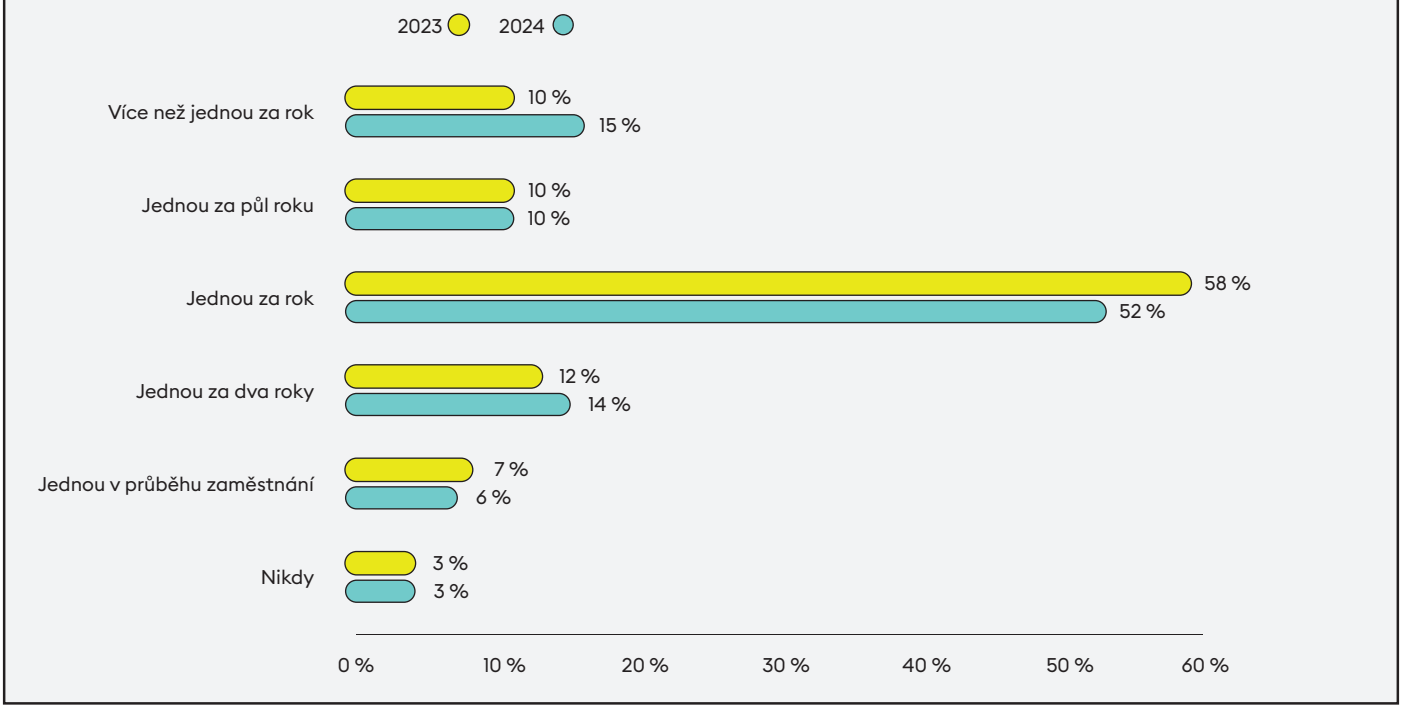
V kybernetické bezpečnosti školí své zaměstnance 94 % oslovených organizací, přičemž školení probíhají nejčastěji jednou ročně.

Podobně jako v předchozím roce je nejčastějším způsobem školení informování zaměstnanců např. formou e-mailů nebo interních portálů. **Ve většině případů respondenti, kteří doposud své zaměstnance netestovali, s tím plánují začít.**

Pozitivním posunem je, že větší množství oslovených společností začalo alokovat finanční prostředky specificky na školení svých zaměstnanců v kybernetické bezpečnosti. **V meziročním srovnání se jedná o 8% nárůst ze 43 na 51 %.**

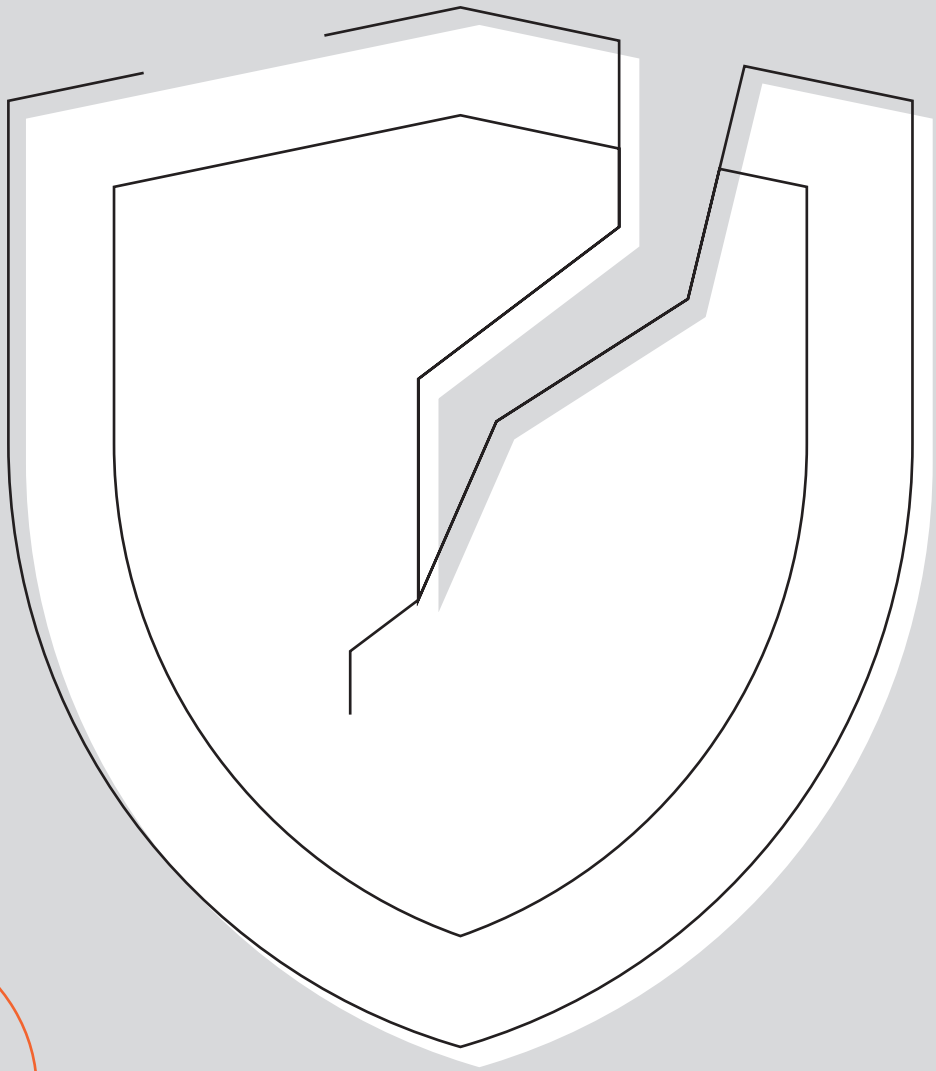
Je pravděpodobné, že se tento posun promítl i do četnosti školení zaměstnanců, kde lze oproti minulému roku pozorovat navýšení frekvence školení (viz graf 10).

Srovnání četnosti školení zaměstnanců za rok 2023 a 2024 (% respondentů)



Graf 10

Kybernetické hrozby a aktéři

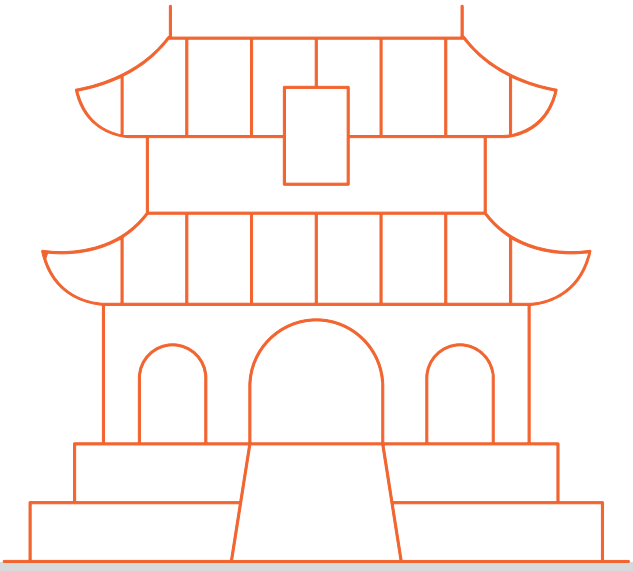


2

Aktivity ruských a čínských aktérů nadále pokračují: Česká republika aktivně reaguje na hrozby s nimi spojené

Kybernetické útoky státem sponzorovaných aktérů zaměřených na ČR pokračovaly také v roce 2024. Nejvýrazněji se projevily zejména kyberútoky skupin působících pod ruskými zpravodajskými službami.

V ČR byly například detekovány kampaně spojované se skupinami APT29 (též Midnight Blizzard nebo BlueBravo, spojovaná se Službou vnější rozvědky, SVR) a COLDRIVER (též Star Blizzard nebo Callisto Group, spojovaná s Federální službou bezpečnosti, FSB).



Aktivní zásah ČR proti ruské skupině APT28

Rok 2024 byl významný zejména z pohledu reakce ČR na škodlivé ruské aktivity v kybernetickém prostoru. **Během ledna provedlo Vojenské zpravodajství aktivní zásah v kybernetickém prostoru proti skupině APT28** (též známé jako Fancy Bear nebo Forest Blizzard, spojované s ruskou vojenskou rozvědkou, GRU). Učinilo tak při mezinárodní operaci DYING EMBER vedené Spojenými státy americkými. Operace spočívala v provedení opatření proti infrastruktuře kompromitovaných routerů zneužívaných daným aktérem proti cílům v ČR i v zahraničí.

Mezinárodní odsouzení ruské kyberšpionáže

Na začátku května 2024 pak došlo k přisouzení škodlivých aktivit v kyberprostoru (tzv. atribuci) Ruské federaci. **ČR společně se Spolkovou republikou Německo, Evropskou unií** (dále jen „EU“), **Severoatlantickou aliancí** (dále jen „NATO“) **a mezinárodními partnery odsoudila kyberšpionážní útoky výše zmíněného aktéra.** V rámci atribuce byla zmíněna kampaň z roku 2023 zneužívající do té doby neznámou zranitelnost aplikace Microsoft Outlook. Skupina APT28 se na cíle v ČR zaměřuje dlouhodobě.

Aktivita čínských aktérů v kyberprostoru

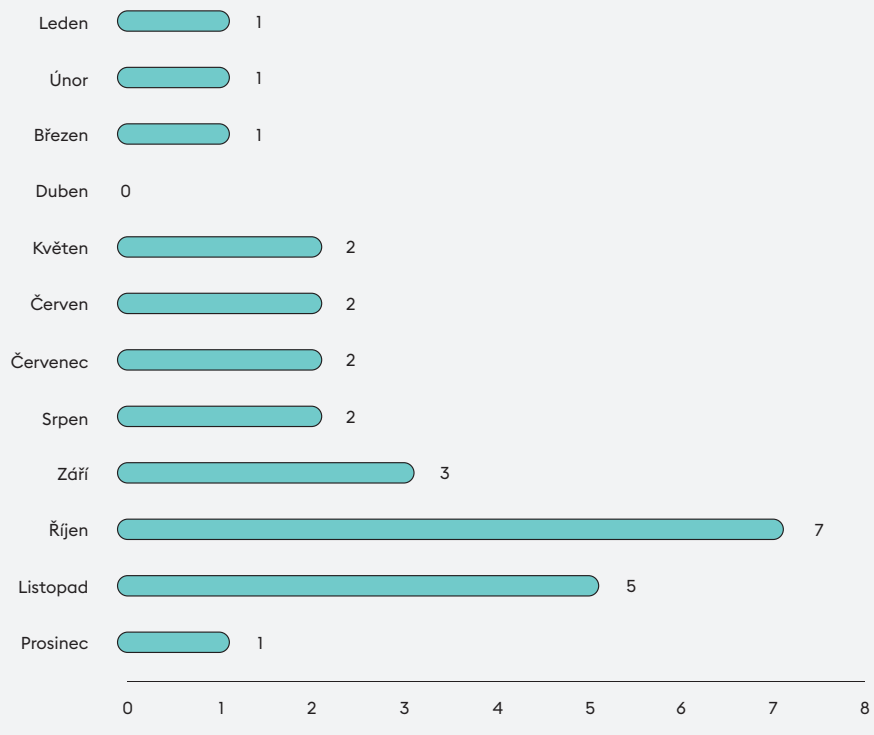
Aktéři spojovaní s ČLR zůstávají rovněž nadále aktivní vůči cílům v rámci EU a NATO. Jejich kampaně cílené na kritickou infrastrukturu, telekomunikační nebo jiné sektory výrazně rezonovaly ve veřejném prostoru, zejména s ohledem na potenciální dopady těchto kompromitací. **Aktivity čínských aktérů byly v roce 2024 detekovány také v rámci ČR, a to přinejmenším ve dvou odlišných případech.**

Ransomware
zůstává přetrvávající hrozbou

Ačkoli po většinu roku bylo množství evidovaných ransomwarových útoků konstantní, v posledním čtvrtletí množství incidentů spojených s ransomwarem strmě vzrostlo.

V říjnu NÚKIB dokonce zaregistroval rekordní počet útoků tohoto typu mířených na státní i soukromé subjekty. Zatímco běžně se počet tohoto typu incidentů pohybuje v nižších jednotkách, během října jich NÚKIB zaregistroval 7, v listopadu potom 5. Podle poznatků NÚKIB nešlo o koordinovanou kampaň, ale pouze o jednotlivé útoky ze strany řady různých ransomwarových gangů.

V uplynulém roce NÚKIB evidoval celkem 27 incidentů spojených s ransomwarem.



Graf 11: Incidenty spojené s ransomwarem evidované NÚKIB v roce 2024

V rámci evidovaných ransomwarových útoků byla zaznamenána celá řada typů využitých ransomwarů.

Graf 12: Evidované útoky ransomwarových skupin

Nižší jednotky byly evidovány u ransomwarů Ransomhub, Inc. Ransomware a Akira, které globálně patřily mezi jedny z nejaktivnějších skupin.

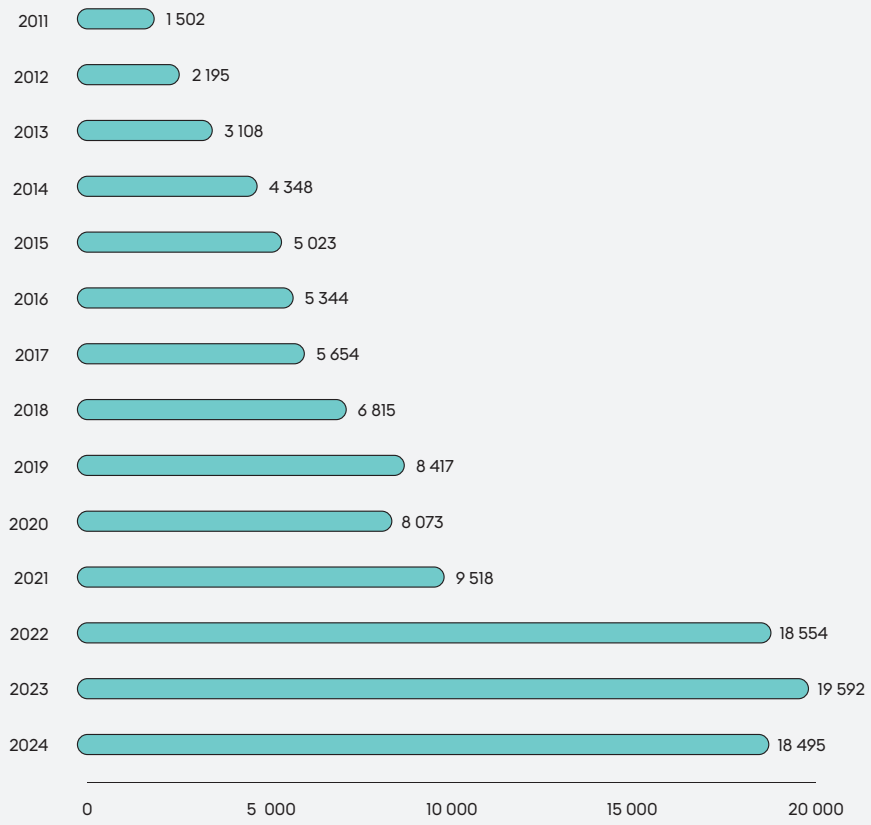
Naopak podíl nejčastěji evidovaných ransomwarů roku 2023 jako PLAY nebo LockBit významně poklesl. U druhého zmíněného byla tato změna velmi pravděpodobně (75–85 %) ovlivněna mezinárodním zásahem bezpečnostních složek vůči jeho infrastruktuře v únoru 2024 (více viz Kybernetické incidenty pohledem NÚKIB za únor 2024).

Ačkoli ransomwarové útoky stály pouze za zhruba 10 % všech evidovaných incidentů, jejich dopady dokazují, že jde o velmi závažnou hrozbu. U řady obětí bylo zaznamenáno zašifrování, smazání nebo exfiltrace různých typů dat napříč různými systémy. Zatímco v některých případech se díky dobře nastaveným bezpečnostním opatřením a včasné reakci podařilo dopady minimalizovat, v jiných případech byl vliv na chod subjektů významný a obnova komplikovaná.

NÚKIB v kontextu této hrozby již v minulosti vydal ve spolupráci s AFCEA a NAKIT podpůrnou analýzu Ransomware: Doporučení pro mitigaci, prevenci a reakci, která shrnuje základní doporučená opatření. Zejména s ohledem na aktuálnost této hrozby zůstávají tato doporučení nadále relevantní.

Úroveň kyberkriminality v rámci evidence PČR meziročně poklesla

Vývoj registrovaných skutků trestné činnosti v kyberprostoru mezi lety 2011–2024 podle údajů PČR



V roce 2022 došlo k výraznému zlomu, kdy meziroční nárůst těchto skutků je téměř dvojnásobný.

Graf 13

V roce 2024 došlo k další úspěšné stabilizaci počtu (18 495) nově registrovaných skutků trestné činnosti páchané v kyberprostoru (kybernetické kriminality a ostatní kriminality páchané v kyberprostoru).

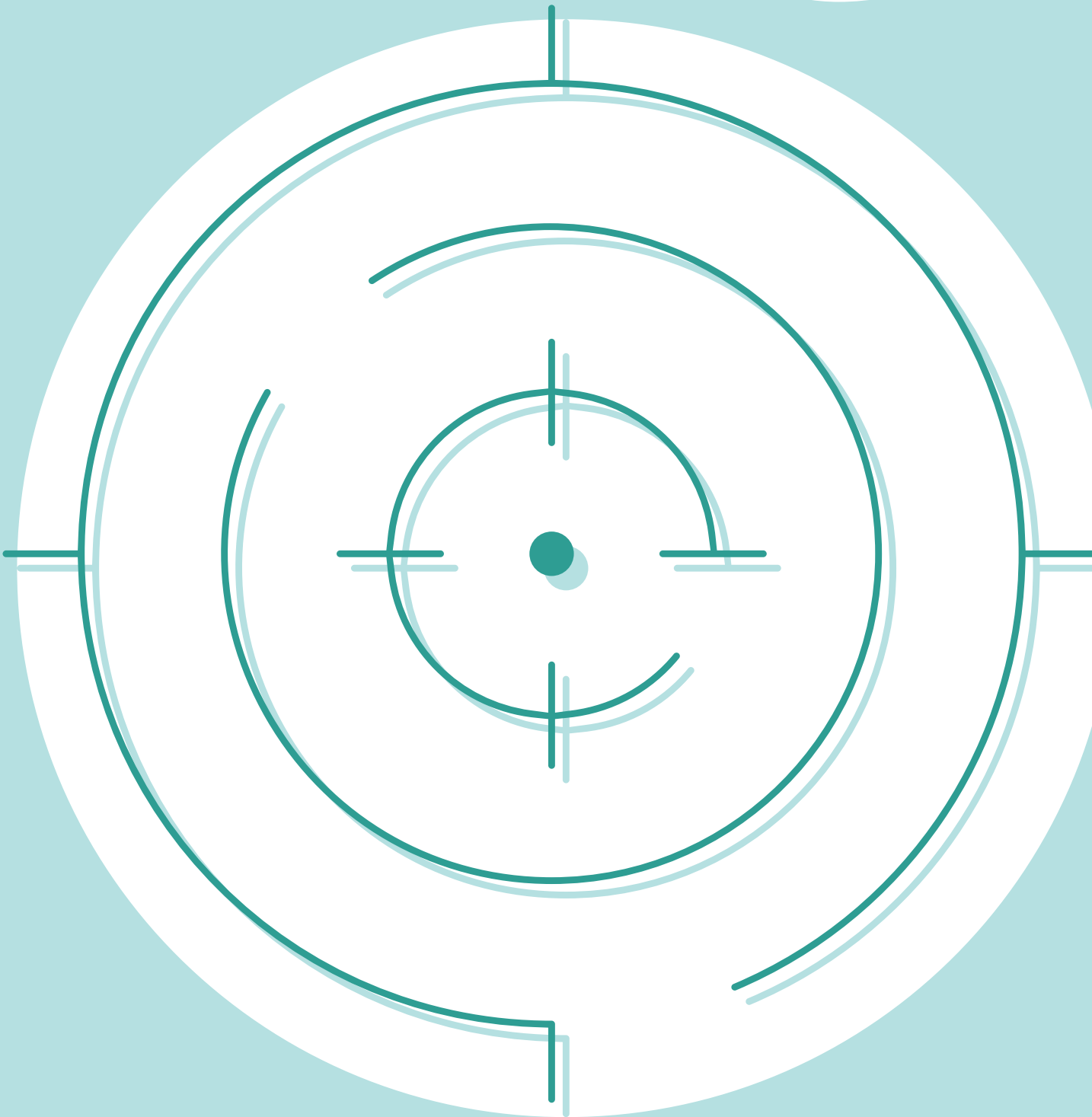
Po čtyřech letech nárůstu byl zaznamenán meziroční pokles o téměř 6 %, přičemž celkový počet těchto trestných činů byl nižší nejen oproti roku 2023, ale i oproti roku 2022. Lze tedy konstatovat, že se PČR daří úspěšně realizovat příslušná koncepční opatření, kterými se zvyšují schopnosti tohoto bezpečnostního sboru ve vztahu ke kyberprostoru. Je tak možné dosahovat vyšší efektivity a úspěšnosti jednotlivých policejních orgánů při odhalování této kriminality.

Nejvyšší podíl představují stejně jako v minulých letech různé druhy online podvodných jednání. Opětovně byl zaznamenán pokles případů „hackingu“, tedy kybernetické kriminality v té nejčistší podobě. Tato skutečnost je již tradičně zapříčiněna také vysokou latencí této „technické“ kriminality, se kterou se občané a firmy setkávají kupříkladu v reportech svých antivirových programů nebo při dočasné nedostupnosti svých webových stránek, ale již nevidí důvod takovou věc řešit s PČR. U skutků, které byly oznámeny a evidovány, je naproti tomu zaznamenávána zvyšující se sofistikovanost, tedy i nebezpečnost jejich způsobu páchání.

Výrazně pozitivní efekt mají rovněž mnohé preventivní aktivity, které PČR každoročně organizuje a na kterých spolupracuje i s mnohými dalšími partnery.

Cíle kybernetických útoků

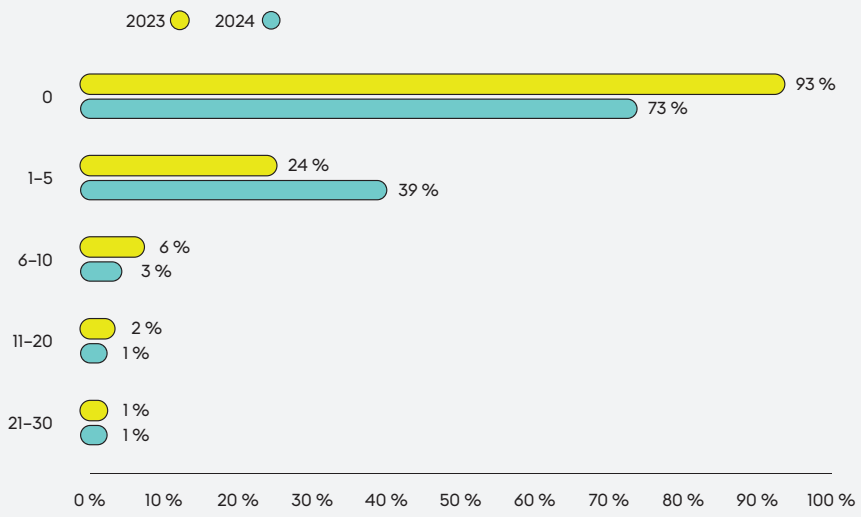
3



Veřejný sektor: Útočníci dále cílí na omezení dostupnosti dat a služeb

Veřejný sektor se nadále řadí k těm více exponovaným. Oproti roku 2023 nevzrostl počet pokusů o útok, ale mírně se zvýšilo množství pokusů, které vyústily v incident (viz graf 14).

Počet pokusů o útok, které vyústily v kybernetický incident (% respondentů)



Největší počet kybernetických útoků opět směřoval na dostupnost služeb.

Hlavním důvodem tohoto trendu nadále zůstávají DDoS kampaně zaměřené na vládní a veřejné instituce.

Graf 14

Stejně jako v roce 2023 ani minulý rok nebyly kampaně tolik navázané na konkrétní kroky české vlády a institucí, jako tomu bylo v roce 2022 (například na konkrétní hlasování o podpoře Ukrajiny), nicméně většinu těchto útoků lze i nadále přisuzovat ruskojazyčným geopoliticky motivovaným aktérům. Stejně jako ve dvou minulých letech se však nejednalo o technicky propracované operace, jejichž dopad by byl zásadní – útoky měly spíše omezenou efektivitu i reálný vliv.

Veřejný sektor se dlouhodobě potýká s nedostatkem financí na kybernetickou bezpečnost. V roce 2024 však došlo k posunu, a to k patrné pozitivní změně ve financování kybernetické bezpečnosti v tomto sektoru.

Podíl organizací, které zaznamenaly nárůst rozpočtu, se zvýšil z 30 na 50 % ve srovnání s loňským rokem, což může znamenat znatelný posun směrem k větším investicím. Oproti průměru ostatních sektorů, kde růst rozpočtu uvedlo 39 % organizací, veřejný sektor v roce 2024 investoval do kybernetické bezpečnosti výrazněji než většina ostatních sektorů (viz graf 15).

Snížení rozpočtu je v tomto sektoru rovněž méně časté než v předchozím roce. Přestože dlouhodobá stagnace rozpočtů v roce 2024 ustoupila, zůstává otázkou, zda se bude jednat o dlouhodobý trend, nebo jen o krátkodobý výkyv, po kterém se situace vrátí do stavu z let před rokem 2024.

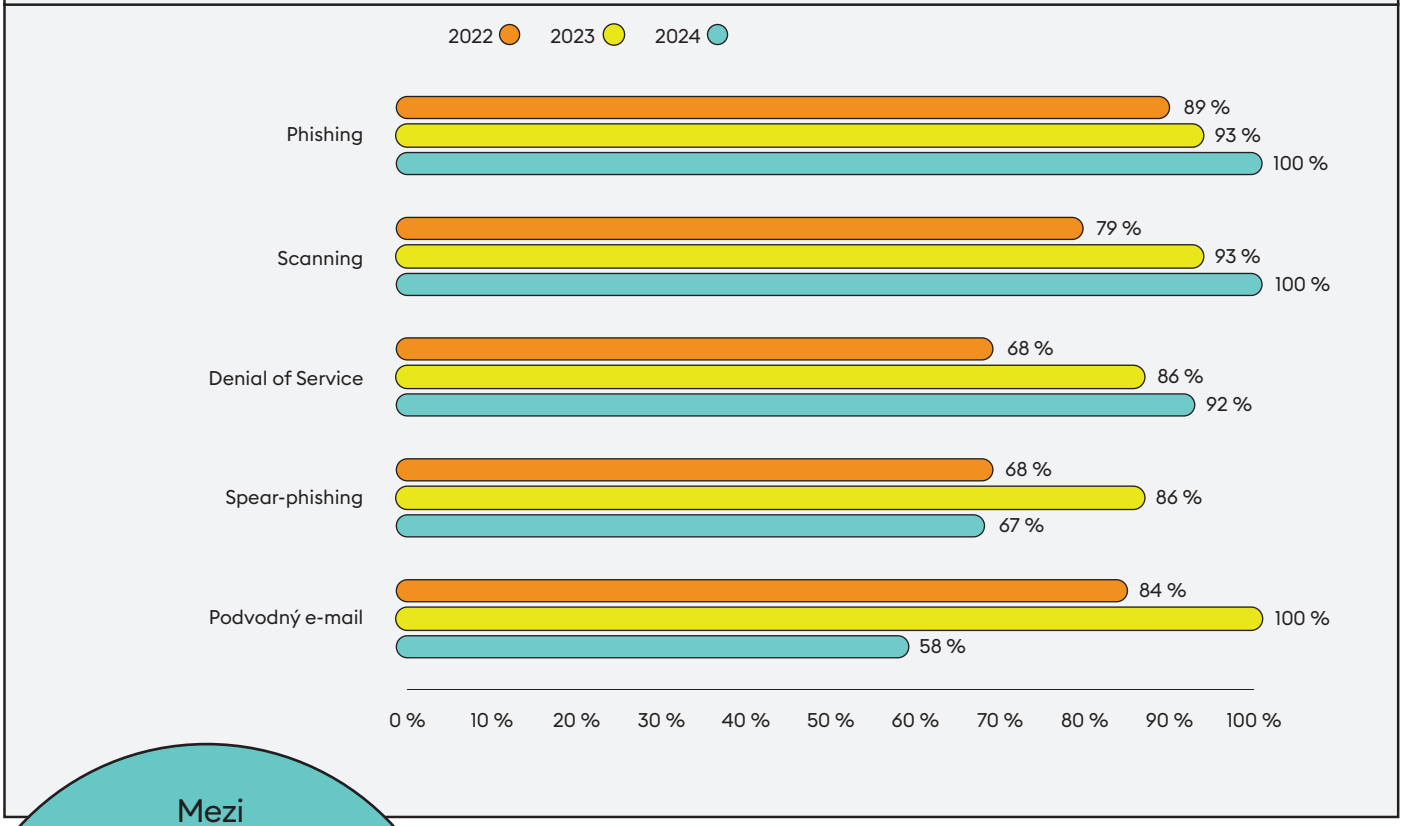
Vývoj rozpočtů ve veřejném sektoru ve srovnání s průměrem ostatních sektorů v letech 2023 a 2024

Graf 15

Finanční sektor: Pokračování phishingových útoků, někdy i s využitím umělé inteligence

S výjimkou jedné instituce se dále všichni respondenti setkali i s tzv. DoS či DDoS útoky. Až polovina respondentů dále zaznamenala pokusy o útoky prostřednictvím různých podvodných e-mailů (od snah o vylákání finančních obnosů pod různými záminkami přes tzv. CEO podvody nebo vydírání) nebo pokusy o kyberútoky pomocí škodlivého obsahu, jako jsou například počítačové viry, trojské koně apod.

Jaké typy útoků na vaši organizaci nebo pokusů o ně jste v minulém roce zaznamenali? (% respondentů)



Mezi nejčastější typy útoků cílících na instituce ve finančním sektoru či jejich zákazníky patřil phishing a scanning. Setkaly se s ním všechny instituce, které se letošního dotazníkového šetření zúčastnily.

Graf 16

Až třetina dotazovaných uvedla, že v roce 2024 detekovala více než 100 pokusů o kybernetický útok, přičemž u poloviny dotazovaných pak tyto útoky vyústily v 6 a více kybernetických incidentů.

Velmi pozitivním vývojem pro kybernetickou bezpečnost ve finančním sektoru je, že respondenti obecně hodnotí úroveň bezpečnosti ve svých institucích jako postupně se zlepšující. Přes 83 % respondentů uvádí, že se úroveň kybernetické bezpečnosti v jejich organizaci za uplynulý rok rozhodně zlepšila, zbytek uvádí, že se spíše zlepšila.

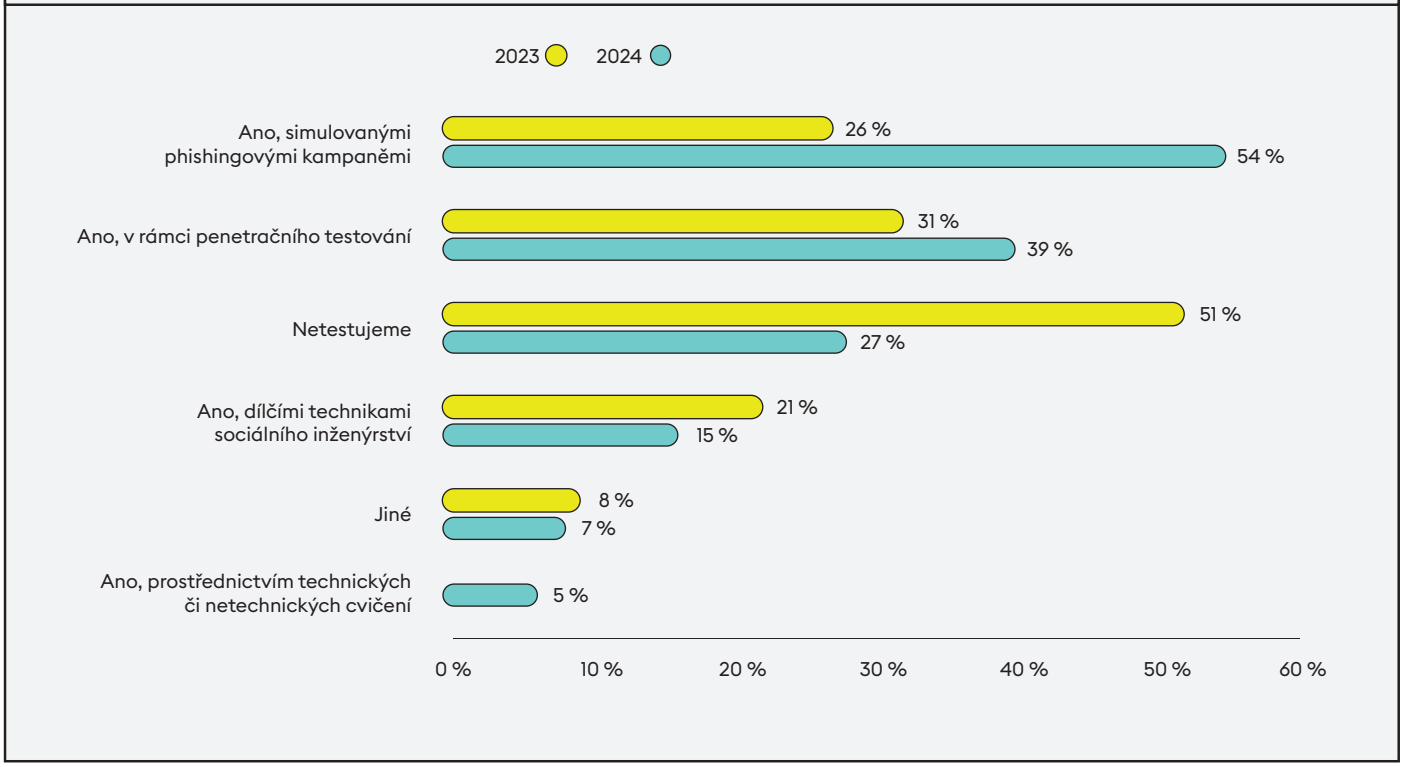
Do strategií útoků na finanční instituce nebo jejich zákazníky se v roce 2024 vyšší mírou promítaly i některé trendy spojené s novými technologiemi. **Respondenti uvedli, že se v některých případech setkali s personalizovanými a kreativnějšími phishingovými e-maily, které poukazovaly na možné využití AI k přípravě útoků.** Dále byly detekovány i útoky se zapojením sofistikovanějších technik vyhýbání se detekci nebo mitigačním nástrojům.

Průmysl a energetika:
Navýšení testování, ale i pokusů o kybernetický útok

V minulém roce energetika zaznamenala výraznější nárůst pokusů o útok z 67 na 74,5 %, přičemž ostatní sektory vyjma veřejného v minulém roce zaznamenaly buď stagnaci, nebo zlepšení.

Pokusům o kybernetický útok čelilo v energetickém a průmyslovém sektoru v roce 2024 v průměru 66 % dotazovaných organizací, což je mírný nárůst o 3 % oproti roku 2023. V kybernetický incident pak vyústilo 21 % pokusů, což je o 5 % více než v roce předchozím. Nelze vyloučit (25–50 %), že se jedná o výchylku ovlivněnou globálním výpadkem systémů společnosti Crowdstrike, jenž postihl taktéž i některé subjekty v domácím energetickém sektoru.

Zatímco v roce 2023 v tomto sektoru více než polovina respondentů zaměstnance netestovala, v roce 2024 je netestovala již jen zhruba čtvrtina dotazovaných společností.



Graf 17: Testujete odolnost zaměstnanců proti kybernetickým hrozbám?

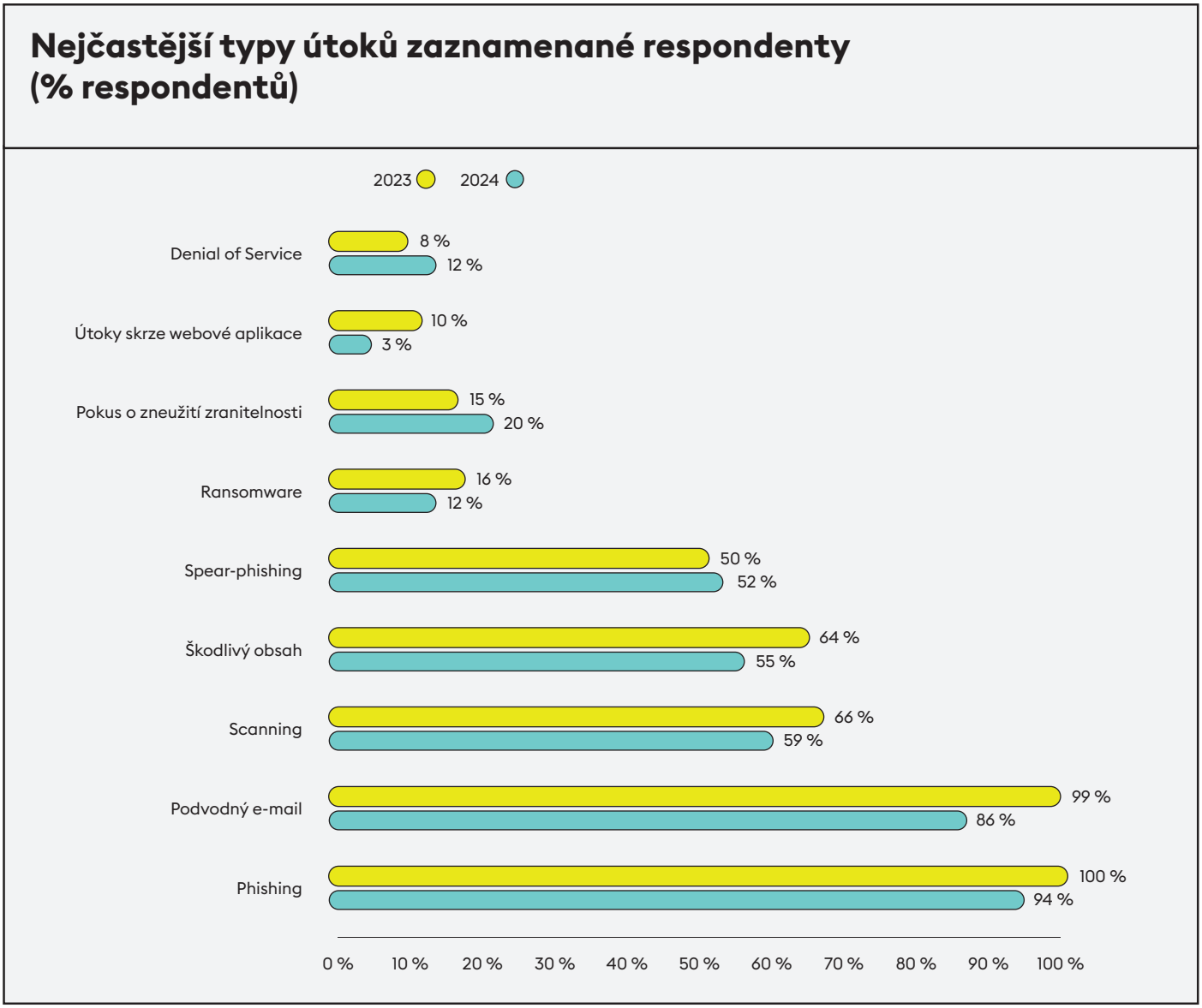
Novým trendem z pohledu bezpečnosti průmyslového sektoru je též nárůst útoků ruskojazyčných skupin na slabě zabezpečené OT systémy s cílem poškodit na ně připojené stroje. Útočníci tak činí prostřednictvím manipulace ovládacích panelů na dálku řízených strojů, kde záměrně mění různé provozní parametry (průtoky ventilů, hladiny nádrží apod.). Přestože NÚKIB eviduje v ČR pouze jeden obdobný incident bez významných dopadů (více viz kapitola: Výhled trendů v kybernetické bezpečnosti), v budoucnu mohou podobné útoky způsobit škody na majetku.

Průmyslový sektor zaznamenal skokovou změnu týkající se testování zaměstnanců. Zatímco v roce 2023 v tomto sektoru více než polovina respondentů zaměstnance netestovala, v roce 2024 je netestovala již jen zhruba čtvrtina dotazovaných společností (viz graf 17). V minulém roce byly nejčastějším typem testování v obou sektorech simulované phishingové útoky.

Zdravotnictví: Útoky spojené se sociálním inženýrstvím zůstávají nejčastější hrozbou, školení zaměstnanců přitom provádí méně zaměstnavatelů než v jiných sektorech

Phishing zůstává i nadále nejrozšířenější formou kybernetického útoku, se kterým se organizace ve zdravotnickém sektoru běžně setkávají. **V roce 2024 jej zaznamenalo přibližně 94 % respondentů. Podobně vysoký podíl organizací hlásil také výskyt podvodných e-mailů nebo dalších forem sociálního inženýrství.** Mezi časté typy hrozeb pak patří scanning vnější sítě, který zaznamenalo 59 % organizací, a škodlivý obsah, který se objevil v 55 % případů. Tato data jsou velmi podobná hodnotám z roku 2023 (viz graf 18).

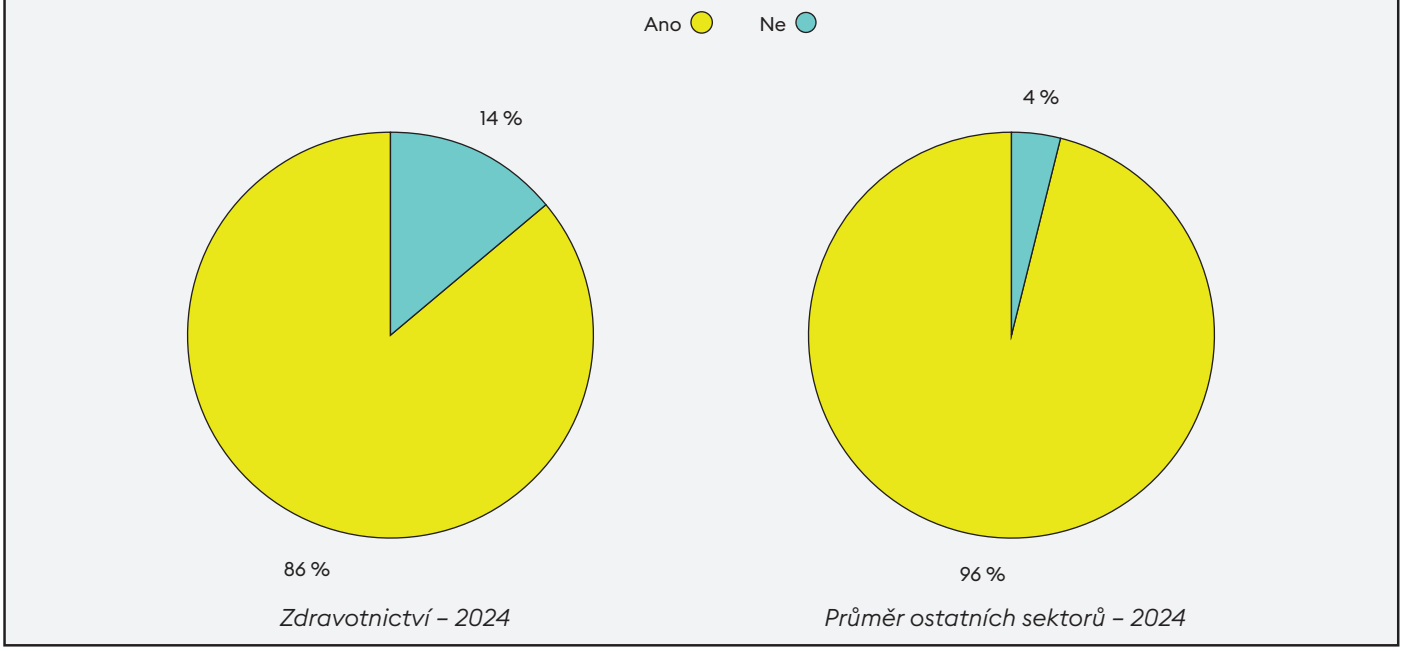
Nejčastější typy útoků zaznamenané respondenty (% respondentů)



Graf 18

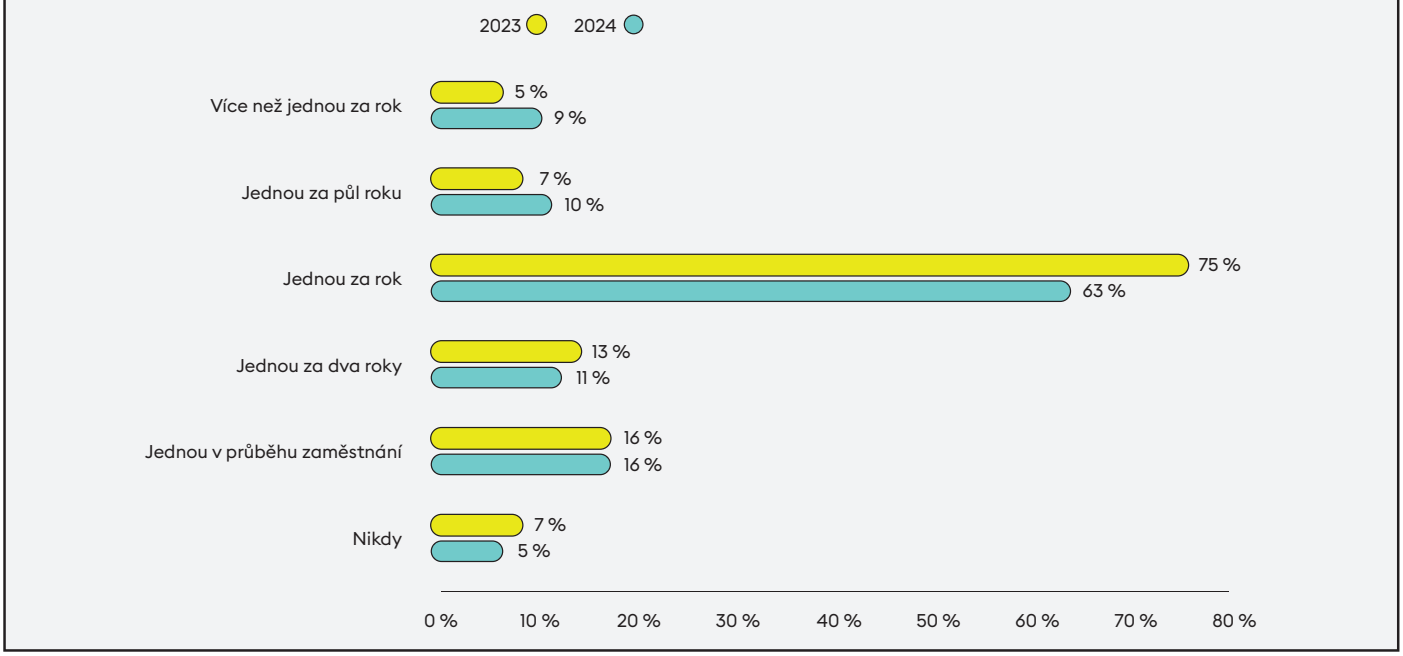
Ačkoliv množství případů phishingu a dalších metod sociálního inženýrství mírně pokleslo ve srovnání s rokem 2023, pořád se jedná o nejčastější typy útoků. **Jedním z nejúčinnějších způsobů ochrany před phishingem, podvodnými e-maily a dalšími formami sociálního inženýrství je pravidelné testování zaměstnanců.** Množství subjektů ve zdravotnictví, které školí své zaměstnance, se ve srovnání s rokem 2023 prakticky nezměnilo a nadále tak oproti ostatním sektorům zaostává o 10 % (viz graf 19). Pozitivním faktem je i skutečnost, že ve srovnání s minulým rokem nyní více subjektů testuje své zaměstnance vícekrát než jednou ročně (viz graf 20).

Školíte zaměstnance o kyberbezpečnostních hrozbách? (% respondentů)



Graf 19

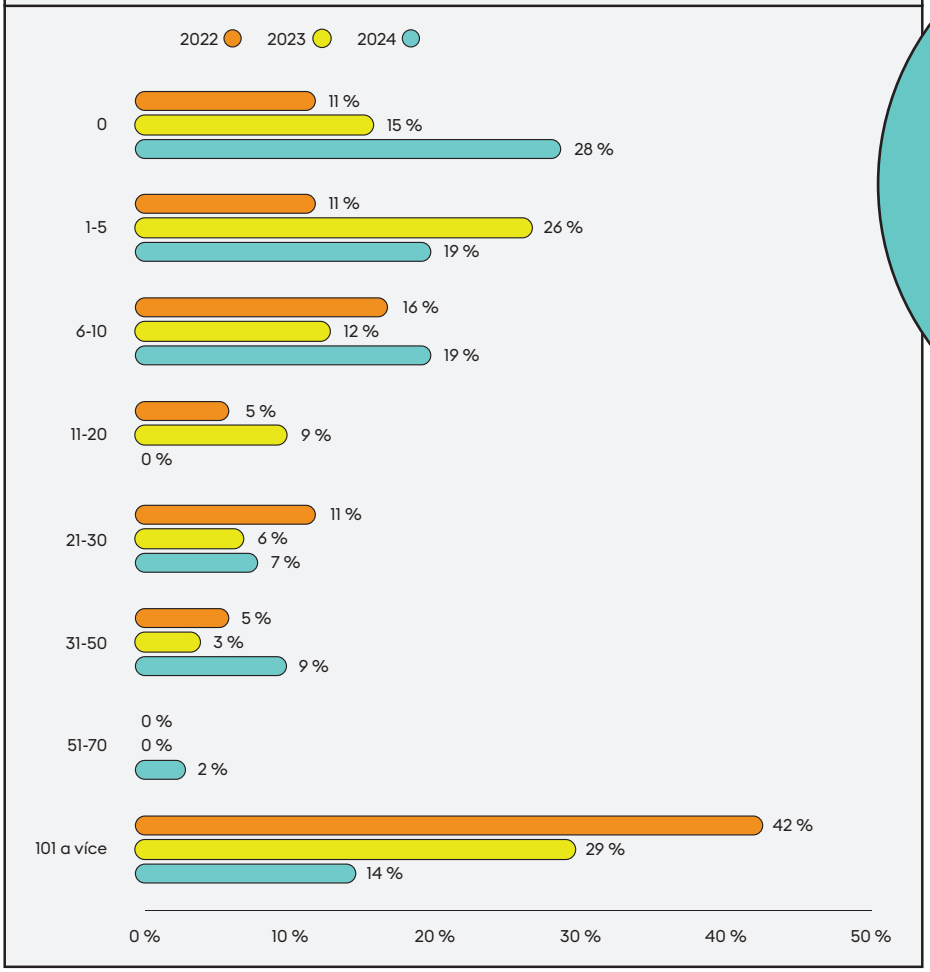
Jak často školíte zaměstnance o kyberbezpečnostních hrozbách?



Graf 20

Vzdělávací sektor: Pokles v počtu detekovaných útoků, trend phishingu a podvodných e-mailů pokračuje

Srovnání počtu zaznamenaných pokusů o kybernetický útok respondenty vzdělávacího sektoru (% respondentů)



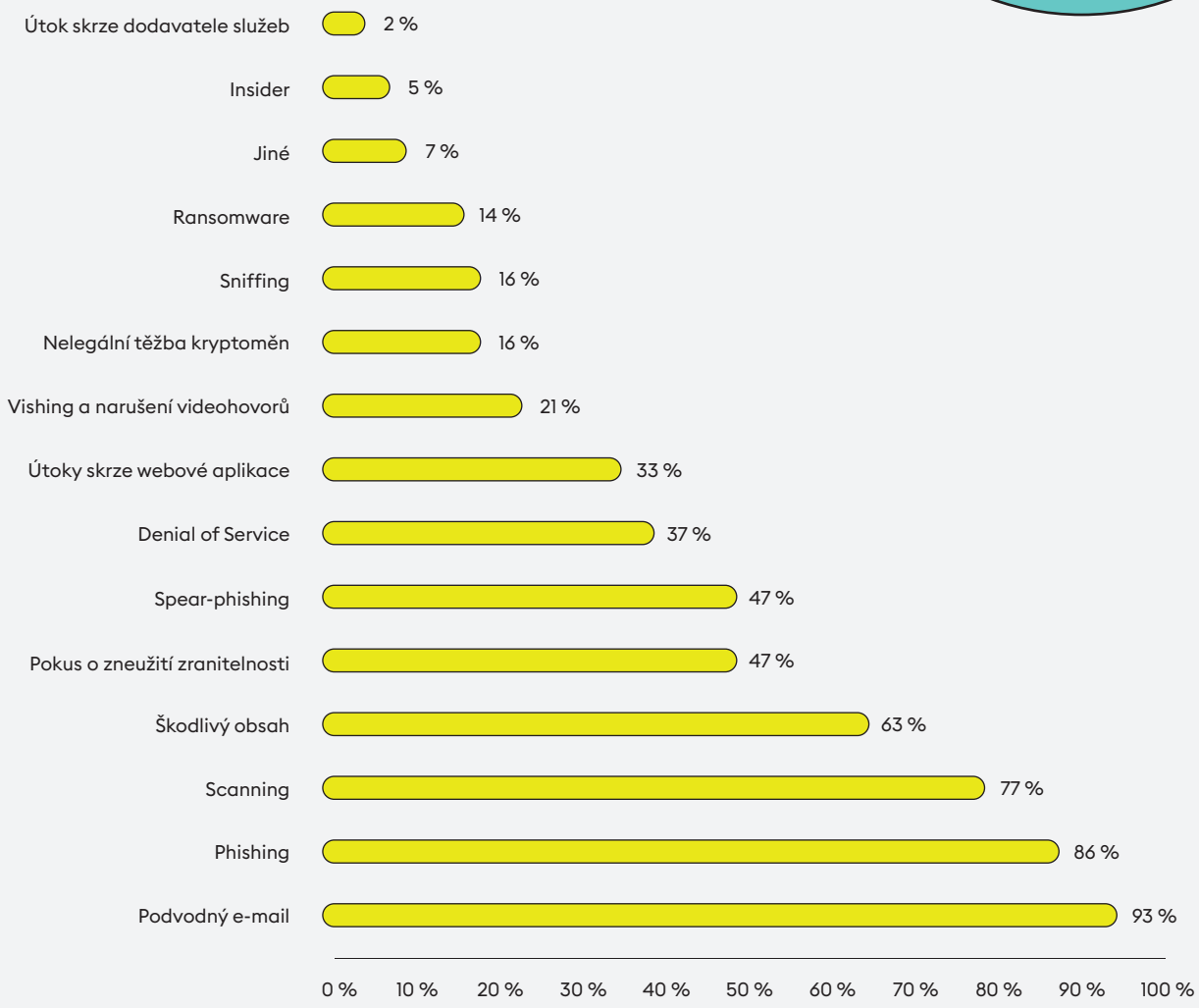
V uplynulém roce zaznamenaly vzdělávací instituce významně menší množství pokusů o kybernetické útoky v porovnání s předchozími dvěma lety.

Graf 21

Pouze 14 % respondentů uvedlo, že evidovali 101 a více pokusů o útok oproti 42 % v roce 2022. Naopak více než čtvrtina dotazovaných nezaznamenala žádný kybernetický útok. Tento pokles může indikovat skutečný pokles provedených pokusů, ale může být i znamením sofistikovanějších útoků a zvýšené schopnosti útočníků vyhnout se detekci a v závislosti na tom i sníženou schopnost institucí útoky odhalit.

Stejně jako v minulých letech i v roce 2024 patřily mezi hlavní typy útoků cílících na vzdělávací sektor různé typy podvodných e-mailů a phishing.

Jaké typy útoků na vaši organizaci nebo pokusů o ně jste v minulém roce zaznamenali?



Graf 22

Různé typy podvodných e-mailů a phishing zaznamenalo přes 90 % dotazovaných institucí. S tím koresponduje i pokračující úsilí institucí vzdělávat uživatele v kybernetické bezpečnosti, což provádí 83 % respondentů. Nadále však oproti celkovému průměru všech sektorů (93 %) zaostávají. Školení a osvěta probíhají nejčastěji formou informování prostřednictvím vhodných platforem a formou on-line školení.

Časová osa vybraných upozornění NÚKIB v roce 2024

Leden

Upozornění na hrozbu útoku Terrapin mířícího na SSH protokol

První upozornění roku 2024 vydal NÚKIB již v lednu. Na konci prosince 2023 došlo ke zveřejnění nového druhu útoku mířícího na SSH protokol – útok Terrapin, který využívá zranitelnosti CVE-2023-48795. Jedná se o prefix truncation attack, kdy útočník manipuluje daty při ustanovování komunikace, tzv. handshake. Tím zapříčiní použití méně bezpečných algoritmů a deaktivaci některých bezpečnostních protiopatření.

Únor

Upozornění na dvě kritické zranitelnosti v OS FortiOS

V únoru NÚKIB upozornil na dvě zranitelnosti v OS FortiOS, které mohly být vzdáleně zneužitelné, z nichž jedna byla aktivně zneužívána. NÚKIB zároveň doporučil neprodleně provést aktualizaci všech zranitelných produktů od této společnosti.

Upozornění na kompromitaci routerů Ubiquity Edge OSaktérem sponzorovaným ruským státem

Předmětem druhého únorového upozornění byla kompromitace routerů Ubiquity Edge OS. Podle informací amerického ministerstva spravedlnosti a jeho tiskové zprávy měl ruským státem sponzorovaný aktér APT28, podléhající ruskému vojenskému zpravodajství (GRU), vytvořit síť kompromitovaných routerů Ubiquity Edge OS (tzv. botnet síť). Kompromitace se týkala stovek těchto zařízení pro malé a domácí kanceláře (SOHO routers), přičemž největší riziko kompromitace platilo pro zařízení s výchozími administrátorskými hesly.

Červen

Upozornění na zvýšené riziko DDoS útoků během voleb do Evropského parlamentu

V souvislosti s volbami do Evropského parlamentu NÚKIB vydal upozornění před rizikem nesofistikovaných útoků cílících na dostupnost (tzv. DDoS) v období od 7. do 9. června 2024. Jako pravděpodobné cíle označil zejména kandidující politické strany, případně organizace jinak zapojené do volebního procesu (např. veřejnou správu nebo média).

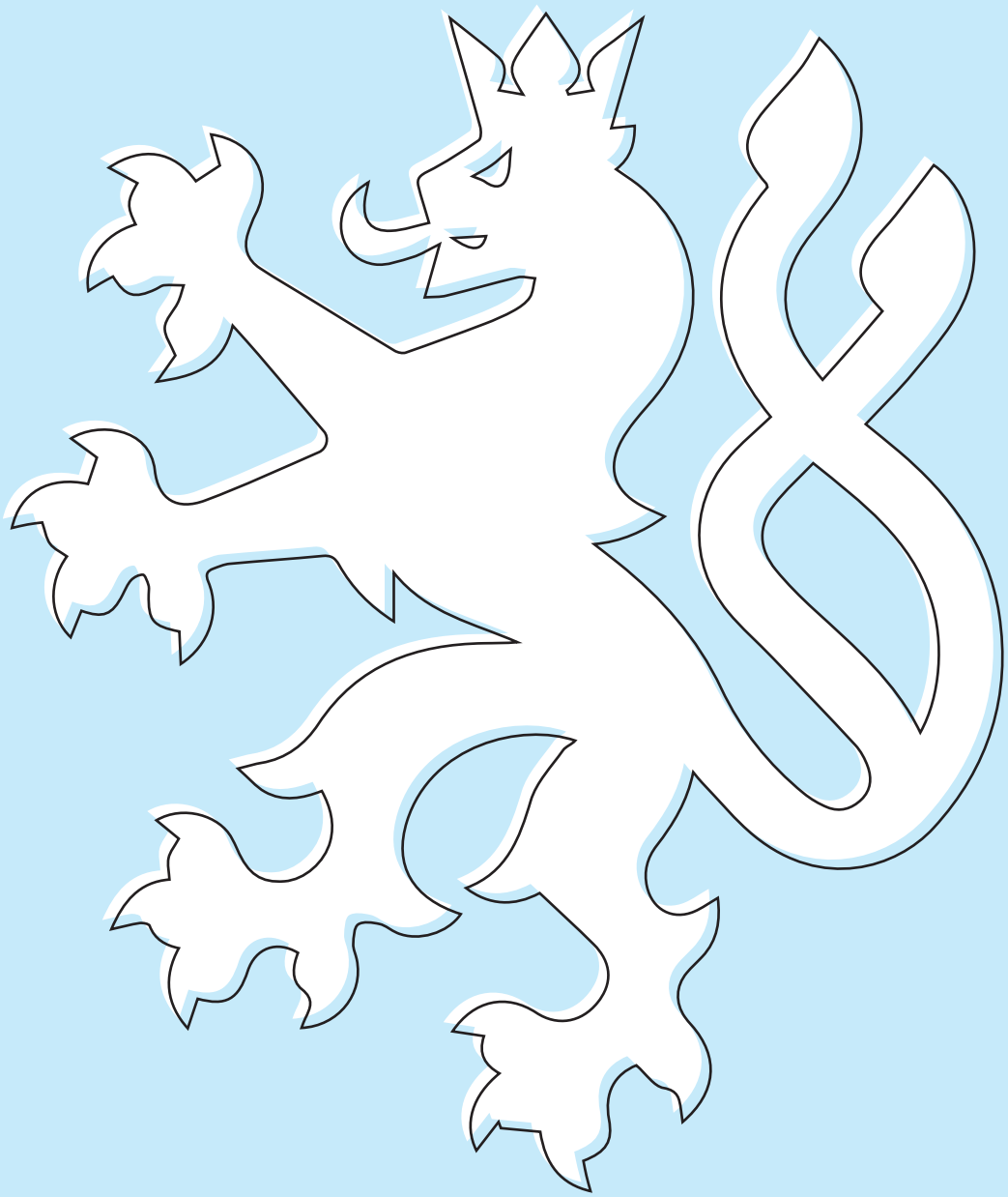
Říjen

Upozornění na zneužívání identit Amazon, Microsoft a státních institucí

Koncem října NÚKIB upozornil na aktivní phishingovou kampaň neznámého útočníka. Útoky byly potvrzeny v několika partnerských zemích, včetně vyšších desítek případů v ČR. Útočník se přitom vydával za společnosti Amazon, Microsoft nebo vládní kyberbezpečnostní instituce v napadených zemích. NÚKIB taktéž doporučil i řadu mitigačních opatření.

Národní úroveň kybernetické bezpečnosti

4



Projekt BIVOJ

V roce 2024 NÚKIB ve spolupráci s partnery pokračoval v práci na projektu BIVOJ (Bezpečný, Inovativní, pro Veřejnou správu, Odolný, Jednotný). Cílem je vytvoření jednotné, funkční a bezpečné sdílené platformy poskytující bezpečnostní a komunikační služby, do které budou postupně připojeny instituce veřejného sektoru.

Jedním z milníků projektu v uplynulém roce bylo schválení usnesení Bezpečnostní rady státu č. 2 ze dne 21. 2. 2024, které mj. uložilo NÚKIB a zapojeným subjektům práci na devíti úkolech, jež měly projekt BIVOJ posunout do dalších fází rozpracovanosti. Zásadními kroky podle tohoto usnesení bylo zpracování studií proveditelnosti architektonického řešení a strategického směřování a ustanovení Řídicího výboru Projektu BIVOJ. Ten je složen ze zástupců relevantních institucí s rozhodovací pravomocí. Během roku 2024 se Řídící výbor sešel za koordinace NÚKIB celkem pětkrát a jedním z výsledků jednání bylo mj. rozdělení konkrétních gescí k realizaci jednotlivých úkolů.

Koordinované zveřejňování zranitelností

V roce 2024 NÚKIB dokončil přípravu návrhu Národní politiky koordinovaného zveřejňování zranitelností (dále jen „CVD“), která má za cíl podporovat nalézání zranitelností v produktech ICT napříč subjekty v ČR bez hrozby negativních právních dopadů pro objevitele zranitelností.

V rámci návrhu nového zákona o kybernetické bezpečnosti je vládní CERT určen koordinátorem pro účely CVD, a jakákoli osoba mu tak bude moci i anonymně hlásit nalezené zranitelnosti. Vládní CERT pak bude identifikovat a kontaktovat dotčené subjekty, pomáhat fyzickým nebo právnickým osobám oznamujícím zranitelnost a dojednávat lhůty pro zveřejnění a řešení zranitelností, které mají dopad na více subjektů.

NÚKIB dále v průběhu roku 2024 připravil implementaci CVD na vybrané webové aplikace úřadu, které užívá a u kterých je minimální bezpečnostní riziko způsobení škody nebo jiné újmy ze strany objevitelů zranitelností.

Koncepce ochrany neutajovaných informací citlivé povahy

Zpracování Koncepce ochrany neutajovaných informací citlivé povahy (dále jen „Koncepce ochrany neUI“) je splnění úkolu vyplývajícího z Akčního plánu k Národní strategii kybernetické bezpečnosti ČR na období let 2021–2025. Koncepce ochrany neUI analyzuje aktuální stav v oblasti ochrany neutajovaných informací citlivé povahy a na strategické úrovni navrhuje vizi a cíle k jejímu dosažení.

Po zpracování analýzy stávajícího stavu a četných konzultacích s interními a externími partnery byla vypracována finální verze materiálu, kterou v září 2024 schválil Výbor pro kybernetickou bezpečnost a následně v listopadu Bezpečnostní rada státu. Od roku 2025 by měla být zahájena implementace Koncepce ochrany neUI příslušnými orgány státní správy pod vedením Ministerstva vnitra ČR. Lhůta pro předložení vybrané varianty koncepce, včetně navazujících legislativních změn, byla stanovena do roku 2027.

Národní politika kryptografické ochrany utajovaných informací

Na základě povinnosti dle § 137a písm. g) zákona č. 412/2005 sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, vypracoval NÚKIB návrh „Národní politiky kryptografické ochrany utajovaných informací v České republice pro období let 2024 až 2030 s výhledem do roku 2040“ (dále jen „NP KOUI“).

NP KOUI je vrcholovým strategickým dokumentem, který udává hlavní směry rozvoje kryptografické ochrany utajovaných informací. NP KOUI byl v září 2024 schválen Výborem pro kybernetickou bezpečnost a následně v listopadu téhož roku Bezpečnostní radou státu.

Jednotlivé strategické cíle uvedené v NP KOUI budou rozpracovány v dokumentu „Implementační plán politiky kryptografické ochrany utajovaných informací v České republice“, v němž budou obsaženy konkrétní adresné a termínované úkoly. Tento plán by měl být zpracován do konce roku 2025, přičemž jeho garantem je NÚKIB, který na NP KOUI spolupracoval a nadále bude spolupracovat s relevantními partnery.

Projekt Kyberliga

Cílem projektu Kyberliga je zapojit dobrovolníky z řad primárně kybernetických expertů a institucionalizovat jejich využití při zajišťování kybernetické bezpečnosti. V návaznosti na interní rozhodnutí NÚKIB z roku 2023 o dalším směřování projektu rozpracoval NÚKIB v roce 2024 původní záměr do podoby konkrétních procesů a administrativního a právního ukotvení, včetně vytvoření dedikované online komunikační platformy. V první polovině roku 2025 by mělo proběhnout pilotní testování projektu a nastaveného schématu. V dalších obdobích by následně měl být tento projekt rozvíjen a měly by se navyšovat jeho kapacity, a to včetně množství členů a škály aktivit realizovaných v jeho rámci.

Legislativní ukotvení

NÚKIB poskytl povinným osobám i odborné veřejnosti desítky konzultací nejen ke směrnici NIS2, ale i k dalším předpisům s přesahem do kybernetické bezpečnosti, jako jsou např. eIDAS, DORA, Networkcode, CRA či CER.

Nový zákon o kybernetické bezpečnosti

V roce 2024 byl návrh nového zákona o kybernetické bezpečnosti projednán Legislativní radou vlády a následně schválen vládou a postoupen do Poslanecké sněmovny Parlamentu ČR. Poslanecká sněmovna uložila Výboru pro bezpečnost, Výboru pro obranu a Hospodářskému výboru návrh zákona projednat. K návrhu zákona byly na výborech a při druhém čtení načteny pozměňovací návrhy a v současné chvíli čeká na dokončení legislativního procesu v obou komorách Parlamentu ČR. V srpnu minulého roku taktéž došlo k přesunutí informačního portálu o směrnici NIS2 na nově spuštěný Portál NÚKIB. Původní informační portál ke směrnici NIS2 zaznamenal více než 400 tisíc návštěv. NÚKIB taktéž zpracoval podpůrné materiály pro nový zákon o kybernetické bezpečnosti v angličtině.

Posuzování ISVS z pohledu bezpečnosti

NÚKIB z pohledu plnění základních bezpečnostních opatření posoudil více než 137 žádostí o stanovisko pro odbor hlavního architekta eGovernmentu stran informačních systémů veřejné správy (dále jen „ISVS“). Jde o naplňování požadavku akčního plánu na zavedení zásady „security by design“ do architektury informačních systémů v rámci veřejné správy.

Jedná se o nástroj, s jehož pomocí lze myšlenku na zajišťování kybernetické bezpečnosti dodat již do fáze tvorby nových systémů. Zároveň tím NÚKIB získává přehled o tom, jak k bezpečnosti přistupují jednotliví správci ISVS.

Regulace cloud computingu

V rámci regulace cloud computingu bylo posouzeno více než 35 poskytovatelů cloudu a více než 39 nabídek cloudových služeb. Ve skutečnosti jde o více než 300 služeb, u kterých je posuzováno naplnění bezpečnostních požadavků definovaných legislativou. Byly zveřejněny první služby, které uplatňují výjimky z požadavků na místo uložení dat, konkrétně se jednalo o služby společnosti Microsoft. V průběhu roku došlo k aktualizaci výjimek u Microsoft a doplnění dvou nových poskytovatelů ALVAO a GORDIC. Celkem je na výjimku (z požadavků na místo uložení dat) zapsáno v katalogu poskytování služeb cloud computingu 47 služeb.

Evropské certifikace kybernetické bezpečnosti

NÚKIB taktéž dokončil interní procesy stran akreditace a autorizace evropské certifikace podle Cyber Security Act. V roce 2024 taktéž proběhla akreditace a autorizace Evropského systému certifikace kybernetické bezpečnosti založeném na společných kritériích (EUCC), jehož certifikáty NÚKIB může vydávat od 25. února 2025. V listopadu 2024 v Brně proběhla Konference evropských certifikací, již NÚKIB pořádal a které se zúčastnilo 122 účastníků.

Dozorová činnost NÚKIB v roce 2024

Celkem bylo v roce 2024 provedeno 22 auditů a kontrol podle zákona o kybernetické bezpečnosti, respektive jeho prováděcí vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů.

Nad rámec běžných kontrolních činností se NÚKIB stejně jako v předchozích letech věnoval také metodické podpoře především u povinných subjektů formou odpovídání dotazů, vydávání podpůrných materiálů a provádění auditů u vybraných subjektů.

Na základě usnesení vlády ze dne 20. prosince 2023 č. 991 a v souladu s Memorandem o vzájemné spolupráci při zajišťováni kybernetické bezpečnosti v době konání Mistrovství světa IIHF v ledním hokeji 2024 ze dne 16. února 2024 byl v roce 2024 dále proveden audit kybernetické bezpečnosti u vybraných společností, které se organizačně podílely na uskutečnění této akce ještě před jejím zahájením.

S ohledem na nově chystanou legislativu a potenciální nárůst povinných subjektů dále NÚKIB provedl audit u tří obcí podle návrhu vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností, aby následně mohly být i dalším obcím snáze demonstrovány nároky na tento režim povinností a jeho aktuální plnění vybranými obcemi.

Spolupráce NÚKIB s dalšími dozorovými orgány v oblasti kontroly v roce 2024

V roce 2024 byla nadále prohlubována spolupráce s dalšími dozorovými orgány. NÚKIB přizval na svoji kontrolu odborníky z Českého telekomunikačního úřadu a současně došlo k uzavření memoranda o spolupráci s tímto úřadem. Dále proběhlo jednání se zástupci z České národní banky, kde se řešil další postup ohledně spolupráce s ohledem na dopady nové regulace jak na bankovní sektor, tak na kybernetickou bezpečnost.

Nejvýznamnější identifikované nedostatky:

CYBER_CON

V září 2024 uspořádal NÚKIB jubilejní 10. ročník konference CYBER_CON, a to kromě tradičního workshopového dne na půdě Fakulty sociálních studií Masarykovy univerzity v Brně také poprvé v prostorech brněnského výstaviště v sále Rotunda. Konference tak kromě nového, atraktivního prostředí získala zejména větší kapacitu pro účastníky hlavního programu a více prostoru pro doprovodný program, konzultace a networking účastníků. Hlavním cílem konference v roce 2024 bylo přiblížit účastníkům spolupráci subjektů veřejného a soukromého sektoru při zajišťování kybernetické bezpečnosti a prezentovat aktuální dění a trendy v oblasti kybernetické a informační bezpečnosti. Během třídenního programu si více než 500 účastníků mohlo poslechnout přednášky a diskuse reflektující technické, politické i právní aspekty kybernetické bezpečnosti.

Cvičení kybernetické bezpečnosti

9

cvičení kybernetické bezpečnosti provedených NÚKIB

305

účastníků cvičení kybernetické bezpečnosti uspořádaných NÚKIB

V roce 2024 se NÚKIB v oblasti cvičení zaměřil na koncepční činnost v souvislosti s nárůstem počtu povinných subjektů. Jedním z výsledků této činnosti bude e-learningový kurz train-the-trainer, prostřednictvím kterého se zájemci naučí, jak připravit efektivní netechnické cvičení v domovské organizaci. Součástí kurzu budou metodické materiály, typové scénáře a dále možnost absolvovat workshop vedený pracovníky NÚKIB, na kterém si zájemci budou moci prakticky procvičit znalosti získané v kurzu.

Také v roce 2024 proběhla cvičení s mezinárodním přesahem, mezi něž již tradičně patří cvičení Locked Shields pořádané NATO Cooperative Cyber Defence Centre of Excellence v estonském Tallinnu, jež se konalo v dubnu, a dále Cyber Coalition, které proběhlo v prosinci a představuje mezinárodní cvičení kybernetické bezpečnosti pravidelně pořádané Severoatlantickou aliancí. NÚKIB se dále aktivně zapojil do cvičení Cyber Europe, které pořádá ENISA. Letošní ročník byl primárně zaměřený na energetický sektor.

Prevence, osvěta a vzdělávání

I v roce 2024 byly prevence, osvěta a vzdělávání jednou z priorit pro zajištění kybernetické bezpečnosti a zvýšení odolnosti společnosti. Jejich rozvoj a důraz na ně napříč celou společností odpovídaly cílům Národní strategie kybernetické bezpečnosti 2021–2025 a reflektovaly výskyt kyberbezpečnostních rizik kopírující růst digitalizace ČR.

Zvyšovaly se digitální dovednosti občanů ČR, a tím rostla i jejich připravenost k bezpečnému využívání digitálních technologií. V základním a středním školství i nadále probíhají změny výuky související s implementací revidovaných rámcových vzdělávacích programů.

Ve vysokém školství a v dalším vzdělávání je situace obdobná jako v roce 2023. Kapacita dostupných studijních programů vysokých škol a dalšího vzdělávání nemá potenciál uspokojit poptávku trhu práce po odbornících kybernetické bezpečnosti, což zůstane výzvou i v roce 2025.

Mezinárodní spolupráce

Cyber Resilience Act, CRA

Na konci roku 2024 bylo v úředním věstníku EU zveřejněno nařízení o kybernetické odolnosti (Cyber Resilience Act, CRA), do jehož vyjednávání se NÚKIB aktivně zapojoval.

CRA představuje průlomovou unijní legislativu na poli kybernetické bezpečnosti, jejímž cílem je zvýšit bezpečnost zavedením požadavků na kybernetickou bezpečnost softwarových a hardwarových produktů, které bude nutné naplňovat po celou dobu jejich životního cyklu. Cílem nařízení dále je snížit počet zranitelností v produktech a zlepšit informovanost jejich uživatelů.

Dále se NÚKIB aktivně spolupodílel s Ministerstvem zahraničních věcí ČR na přípravě Prohlášení k aplikaci mezinárodního práva v kyberprostoru, které bylo vydáno na konci loňského roku.

ENISA Support Action

NÚKIB se i v roce 2024 zapojil do aktivit ENISA prostřednictvím správní rady, sítě styčných důstojníků a vyslaného národního experta, stejně jako pokračoval v administraci projektu ENISA Support Action.

Supply Chain Toolbox

V rámci Skupiny pro spolupráci zřízené směrnicí NIS2 pak pokračovala práce na souboru opatření pro bezpečnost dodavatelského řetězce informačních a komunikačních technologií (tzv. Supply Chain Toolbox), stejně jako úzká koordinace států i Evropské komise ve vztahu k výkladu směrnice NIS2.

Činnost kyber atašé

NÚKIB taktéž posiloval stávající partnerství především v zemích s přítomností vyslaných kyber atašé. V prvním roce fungování nově zřízené pozice kyber atašé pro Indo-Pacifik došlo k posílení bilaterálních vztahů s Austrálií. Významným prvkem spolupráce byla mj. podpora ze strany Austrálie při atribuci aktivit skupiny APT28. Prohloubení vzájemné spolupráce se dále týkalo Kanady, Státu Izrael nebo Estonska.

Spolupráce v rámci NATO

ČR se spolu s dalšími spojenci aktivně zasadila o vznik NATO Integrated Cyber Defence Centre, které má za cíl přispět zejména k navýšení situačního povědomí NATO i spojenců a odolnosti sítí NATO. Zároveň byla ČR kladně hodnocena ve vztahu k plnění závazků k NATO směřujících k navyšování schopností kapacit v oblasti kybernetické bezpečnosti a obrany.

Nové strategické vazby

Minulý rok byl také ve znamení vytváření nových strategických vazeb, mj. došlo k podpisu Memoranda o porozumění s litevským Národním centrem kybernetické bezpečnosti, na jehož základě bude realizována spolupráce v oblasti sdílení analytických informací.

Významnou událostí byla účast technického týmu NÚKIB na mezinárodním kybernetickém cvičení APEX (Allied Power Exercise), která umožnila aktivně prezentovat český pokrok v oblasti kybernetické bezpečnosti.

Counter Ransomware Initiative

NÚKIB rovněž v roce 2024 pokračoval v zapojení do Counter Ransomware Initiative, v jejímž rámci bylo mj. přijato společné prohlášení vyzývající k odpovědnému chování států v kyberprostoru a využívání všech dostupných nástrojů a prostředků v boji proti ransomware. ČR na summitu prezentovala dosavadní spolupráci v rámci mezirezortní pracovní skupiny pro boj s ransomware, kterou NÚKIB spolu s Národní centrálou proti terorismu, extremismu a kybernetické kriminalitě PČR založil v lednu 2024. Díky varování amerických partnerů a včasnému sdílení informací mezi CERT byl NÚKIB schopen ochránit před ransomwarovým útokem jeden ze subjektů v ČR.

Prague Cyber Security Conference

V roce 2024 se mezinárodní událost Prague Cyber Security Conference (dále jen „PCSC“) poprvé otevřela soukromému sektoru. Stěžejními tématy byly dopady AI na kybernetickou bezpečnost, ochrana podmořských kabelů před kybernetickými hrozbami, kybernetické válčení nebo boj s organizovanými kyberkriminálními skupinami. Další PCSC se konala v březnu 2025 a opět se těšila velké mezinárodní účastí.

Činnost Vládního CERT

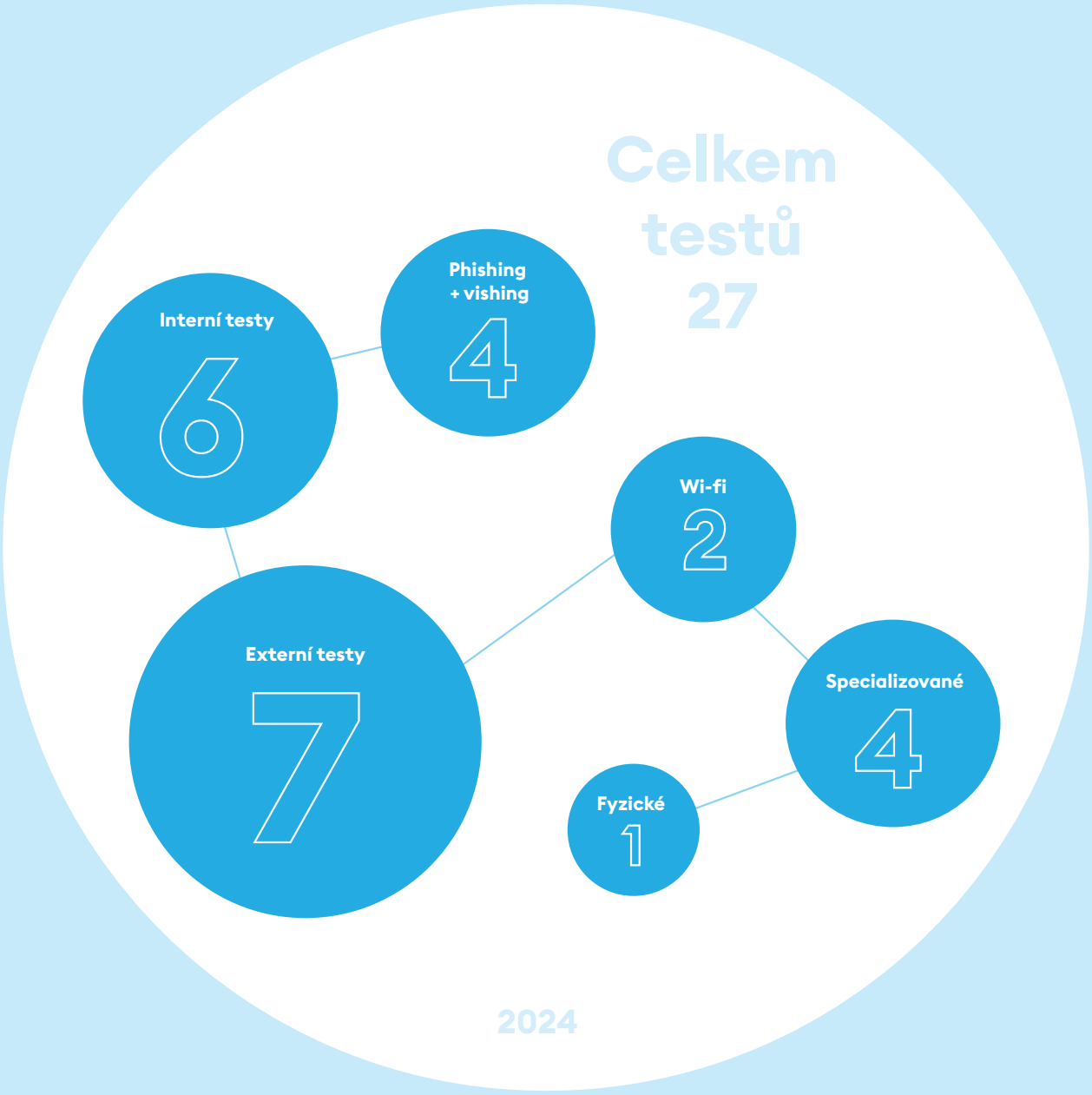
Testování wi-fi sítí

CERT v rámci svých služeb penetračního testování začal nově poskytovat provádění testování wi-fi sítí a začal se více zaměřovat na specializované systémy, ať v zdravotnickém, nebo energetickém sektoru.

Přetvoření infrastruktury pro phishingové kampaně a rozšiřování schopností

Dále v průběhu roku došlo k přetvoření infrastruktury pro phishingové kampaně, a také byly rozšiřovány testovací schopnosti o nový hardware a software. To se týká i služby skenování zranitelností, kde bylo cílem získat nástroj pro automatizované skenování velkého počtu konstituentů, do kterého je aktuálně zapojeno 73 institucí.

Statistiky penetračního oddělení za rok 2024



V roce 2024 byla dále prohlubována spolupráce jak na národní úrovni s relevantními partnery při řešení incidentů, tak na mezinárodní úrovni, ať už bilaterálně, nebo v rámci mezinárodních platforem, jako je CSIRT Network či TF-CSIRT, kterých jsme se aktivně účastnili.

Výhled trendů v kybernetické bezpečnosti v ČR na roky 2024 a 2025

Předpokládaný vývoj na poli AI

V roce 2024 byla generativní AI a s ní spojené produkty jako chatboti na bázi velkých jazykových modelů nadále hybným tématem kybernetické bezpečnosti. Oproti rozmachu v roce 2023 šlo ovšem sledovat významné zpomalení vývoje těchto produktů a jistou stagnaci. Místo snahy o obcházení bezpečnostních zábran velkých AI služeb bylo možné sledovat vznik menších a méně sofistikovaných AI nástrojů, které byly ovšem přímo vycvičeny a provozovány s cílem asistovat při nekalých aktivitách. V roce 2024 byl rovněž vyvíjen čínský jazykový model DeepSeek R1, který vyšel na začátku roku 2025, a přinesl významnou konkurenci západním službám, ale spojenou s riziky, která se pojí s čínskými produkty (sběr dat o uživateli a jejich netransparentní zpracování, vazby společnosti na státní aparát a cenzura informací, které chatbot poskytuje). **V roce 2025 můžeme na poli AI očekávat především další vyhrocení technologického soupeření mezi západem a ČLR, které DeepSeek svým vydáním na počátku roku 2025 eskaloval.** To se odrazí do druhého významného trendu pro rok 2025, kterým bude navyšování investic do budování AI infrastruktury (a navázaných odvětví, například energetiky). S tím se zřejmě budou pojit i snahy o větší monetizaci AI, protože v roce 2024 se i největší lídři na trhu nacházeli ve ztrátě, již ovšem kompenzovali masivními investicemi.

Hrozba kvantových počítačů, postkvantová kryptografie a HNDL útoky

S množstvím investic a narůstajícími pokroky ve vývoji se zvyšuje riziko kvantových počítačů. Tato zařízení mají potenciál během příštích dekád v některých aspektech výrazně předčit schopnosti současných počítačů a způsobit revoluci v mnoha oblastech lidské činnosti. Zároveň však představují hrozbu pro bezpečnost aktuálně používaných asymetrických šifrovacích standardů. Primárním nástrojem mitigace této hrozby je tzv. postkvantová kryptografie a nové šifrovací algoritmy, které by měly kvantovým počítačům odolat. Vzešly ze soutěže amerického Národního institutu standardů a technologie (NIST). **Jejich včasná implementace bude klíčovým tématem roku 2025. Potřebu implementace těchto šifrovacích standardů zvyšují tzv. HNDL útoky (anglicky harvest now, decrypt later, tedy „získej nyní, dešifruj později“).** Vyspělí aktéři, kteří mohou kalkulovat s tím, že budou v budoucnu disponovat kvantovými počítači, mohou již dnes nepozorovaně sbírat data zašifrovaná současnými nedostatečnými algoritmy a později je prolomit s pomocí kvantových počítačů. Tyto útoky **je těžké odhalit a prakticky nemožné zastavit jinak než co nejvčasnější implementací postkvantové kryptografie, která data ochrání před prolomením i v případě odcizení.**

Hacktivisté: dlouhotrvající i proměnlivá hrozba

Během roku 2024 pokračoval již nastolený trend škodlivých aktivit různých hacktivistických skupin. **Z pohledu ČR hraje primární roli zejména ruskojazyčný aktér NoName057(16), který stál za většinou v tuzemsku detekovaných DDoS útoků.** Přestože obecně mají tyto útoky pouze marginální dopady, jejich vysoká četnost a vytrvalost bude velmi pravděpodobně (70–85 %) pokračovat i v roce 2025 a 2026. Existuje také reálná šance (40–50 %), že ani případný konec války proti Ukrajině, kterou v zásadě deklarují jako hlavní důvod svých aktivit vůči Západu, jejich činnost neovlivní a činnost obdobných skupin se stane novým normálem.

Novým a rostoucím trendem jsou pak útoky ruskojazyčných hacktivistů vůči slabě zabezpečeným systémům operačních technologií (OT), zejména v podnicích vodohospodářského sektoru. Útočníci při nich přistupují k ovládacím konzolím různých strojů, které jsou často přístupné z internetu a zabezpečené výchozími hesly. Následně s nimi neodborně manipulují ve snaze docílit fyzických efektů (vypuštění či naopak přetečení různých nádrží apod.). Celou aktivitu si obvykle nahrávají a následně sdílejí na sociální síti Telegram. Přestože ve většině známých případů útoky nevedly ke škodám, jejich počet, zejména v západních zemích, se pohybuje alespoň v nižších desítkách, přičemž NÚKIB jeden útok v uplynulém roce evidoval i v ČR.

Existuje reálná šance (40–50 %), že i v ČR počet těchto útoků v budoucnu poroste a v některých případech může dojít i ke škodám na majetku. Přestože řada OT rozhraní je díky špatné konfiguraci přístupná z internetu a slabě zabezpečená, obvykle disponuje i další vrstvou bezpečnostní prvků, což snižuje riziko nehody při neodborné a škodlivé manipulaci.

Příloha 1:

Vyhodnocení plnění cílů Národního plánu výzkumu a vývoje v kybernetické a informační bezpečnosti za rok 2024

Budování národního koordinačního centra

I v roce 2024 NÚKIB pokračoval v budování Národního koordinačního centra podle nařízení Evropského parlamentu a Rady č. 2021/887. Zkvalitnění služeb v oblastech budování informačního zázemí, poradenství v čerpání evropských rámcových programů a šíření výsledků výzkumu a vývoje v rámci ČR bylo podpořeno z grantu EU, který NÚKIB získal z programu Digitální Evropa. Díky této podpoře NÚKIB vypsal výzvu k podávání návrhů projektů v oblastech rozvoje odborných kapacit a zvyšování kvalifikace, podpory mezisektorové spolupráce a zvyšování povědomí o kybernetické bezpečnosti. Celkově bylo podpořeno sedm projektů ve výši 3,7 milionu Kč.

Aktivity na úrovní EU

Na úrovni EU se NÚKIB podílel na přípravě řady strategických dokumentů klíčových pro fungování Evropského centra kompetencí pro kybernetickou bezpečnost nebo věcného zaměření programů Digitální Evropa a Horizont Evropa.

Podpora výzkumných a vývojových projektů

Z pozice aplikačního garanta NÚKIB podpořil několik výzkumných a vývojových projektů financovaných z programů veřejných soutěží (například Technologická agentura ČR) s cílem zvýšit uplatnitelnost výsledků výzkumu a vývoje v praxi. NÚKIB se rovněž zapojil do mezinárodního projektu předloženého v rámci programu Horizont Evropa a pokračoval ve spolupráci na mezinárodní projektu CHESS, jehož cílem je posílit regionální inovační excelenci v oblasti kybernetické bezpečnosti.

Budování informačního zázemí a komunity

NÚKIB pokračoval v budování informačního zázemí a komunity v oblasti výzkumu a vývoje. Na webových stránkách NÚKIB jsou pravidelně publikovány newslettery „Aktuality ve výzkumu a vývoji v kybernetické bezpečnosti“. Vazby mezi akademickým, veřejným a soukromým sektorem se posilovaly prostřednictvím pravidelných setkání skupiny kyberbezpečnostního výzkumu a inovací CYRIS (dříve Platformy pro výzkum a vývoj v kybernetické a informační bezpečnosti).

Příloha 2:

Naplňování Akčního plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025

Rok 2024 byl čtvrtým rokem vyhodnocování Akčního plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025 (dále jen „Akční plán"). NÚKIB nejenže koordinuje vyhodnocení celého Akčního plánu, ale podílí se z pozice gestora či spolupracujícího subjektu na plnění 101 z celkových 105 úkolů. V roce 2024 se jedná o předposlední vyhodnocení stávajícího Akčního plánu a od roku 2026 by měl být v návaznosti na probíhající aktualizaci Národní strategie kybernetické bezpečnosti již v platnosti nový Akční plán.

V roce 2024 přibyly také nově vyhodnocované úkoly. Jedná se například o úkol č. 4 „Sbližovat přístup ke kybernetické bezpečnosti a ochraně utajovaných informací v informačních a komunikačních systémech v souladu s Koncepcí rozvoje Národního úřadu pro kybernetickou a informační bezpečnost. Navrhnout případné změny přístupu na základě analýzy současného stavu a potřeb". Úkol byl plněn například skrze zpracování *Národní politiky kryptografické ochrany utajovaných informací pro období 2024 až 2030, s výhledem do roku 2040.* Tato národní politika, schválená v listopadu 2024 Bezpečnostní radou státu, je vrcholovým strategickým dokumentem státu, který udává hlavní směry rozvoje kryptografické ochrany utajovaných informací v následující dekádě.

Příkladem úkolu pouze částečně splněného je úkol číslo 13 „Vytvořit metodiku pro strategickou komunikaci relevantních subjektů na národní úrovni pro případ reakce na kybernetické incidenty, útoky a jiné hrozby". Plnění tohoto úkolu bude přeneseno do roku 2025 a na přípravě metodiky pro strategickou komunikaci se bude nadále pracovat.

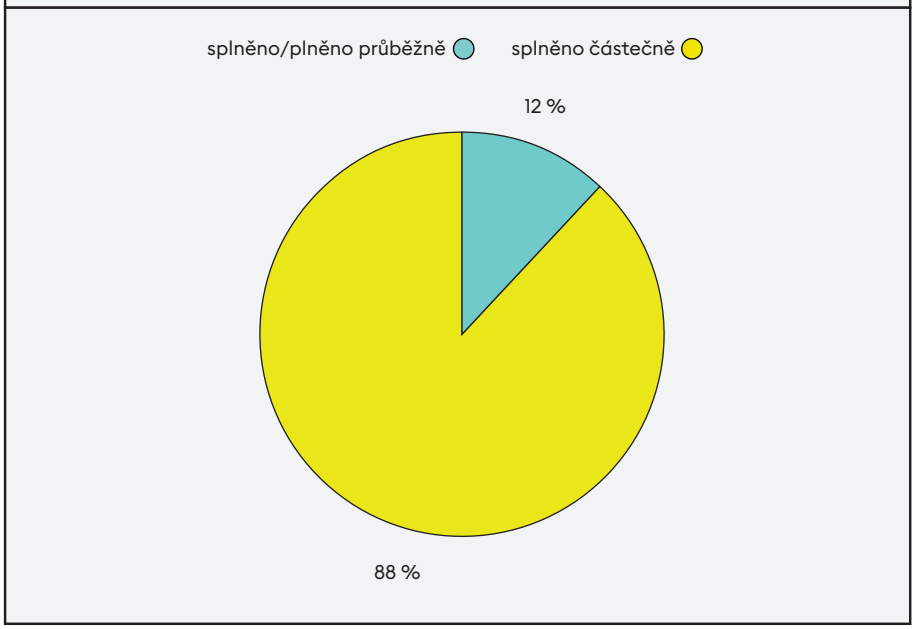
V roce 2024 bylo také dosaženo splnění některých úkolů dlouhodobě neuzavřených, například úkolu č. 68 „Vytvořit ucelenou národní pozici ČR k interpretaci stávajícího mezinárodního práva v oblasti kybernetické bezpečnosti a obrany". Ministerstvo zahraničních věcí v roce 2024 publikovalo ve spolupráci s ostatními gestory národní pozici k aplikaci mezinárodního práva veřejného na kyberprostor. Přijetí tohoto dokumentu má usnadnit reakce ČR na výzvy vyplývající z neustálého rozvoje technologií a s tím souvisejících rizik.

V případě částečně splněných úkolů se převážně jedná o komplexní a dlouhodobé úkoly, jejichž plnění bylo opakovaně přeneseno do následujícího roku. Nedostatečné plnění určitých úkolů je způsobeno zejména časovými a kapacitními možnostmi gestorů nebo nutnou reprioritizací. Tyto poznatky z nastavení úkolů budou zohledněny při tvorbě dalšího Akčního plánu.

Za rok 2024 bylo předmětem vyhodnocení 87 úkolů.

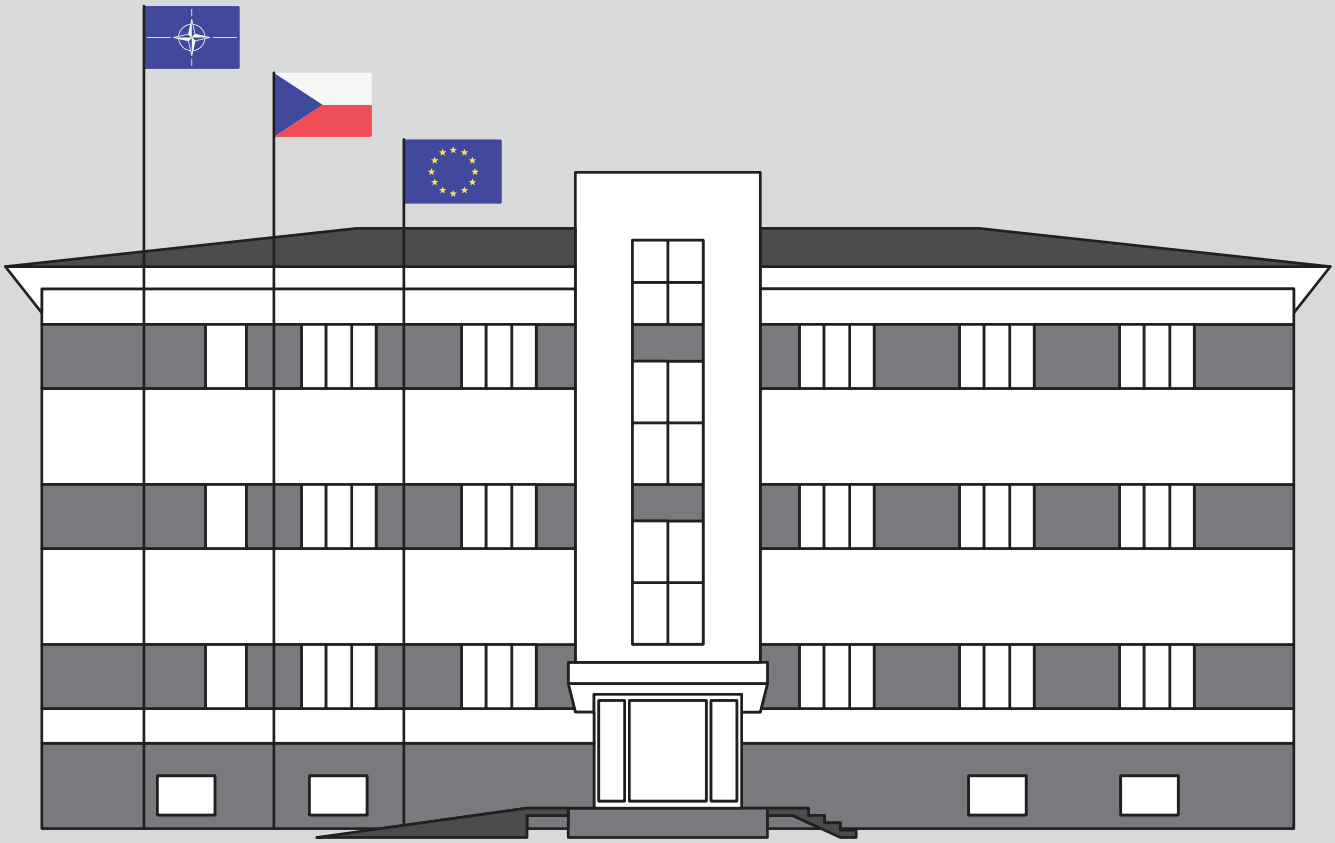
Z tohoto počtu bylo v roce 2024 splněno (či plněno průběžně) 77 úkolů, což představuje celkem 88% úspěšnost.

Z celkového počtu 87 bylo 10 úkolů splněno pouze částečně. Oproti roku 2023 se jedná o mírné zlepšení úspěšnosti.



Graf 23: Vyhodnocení Akčního plánu za rok 2024

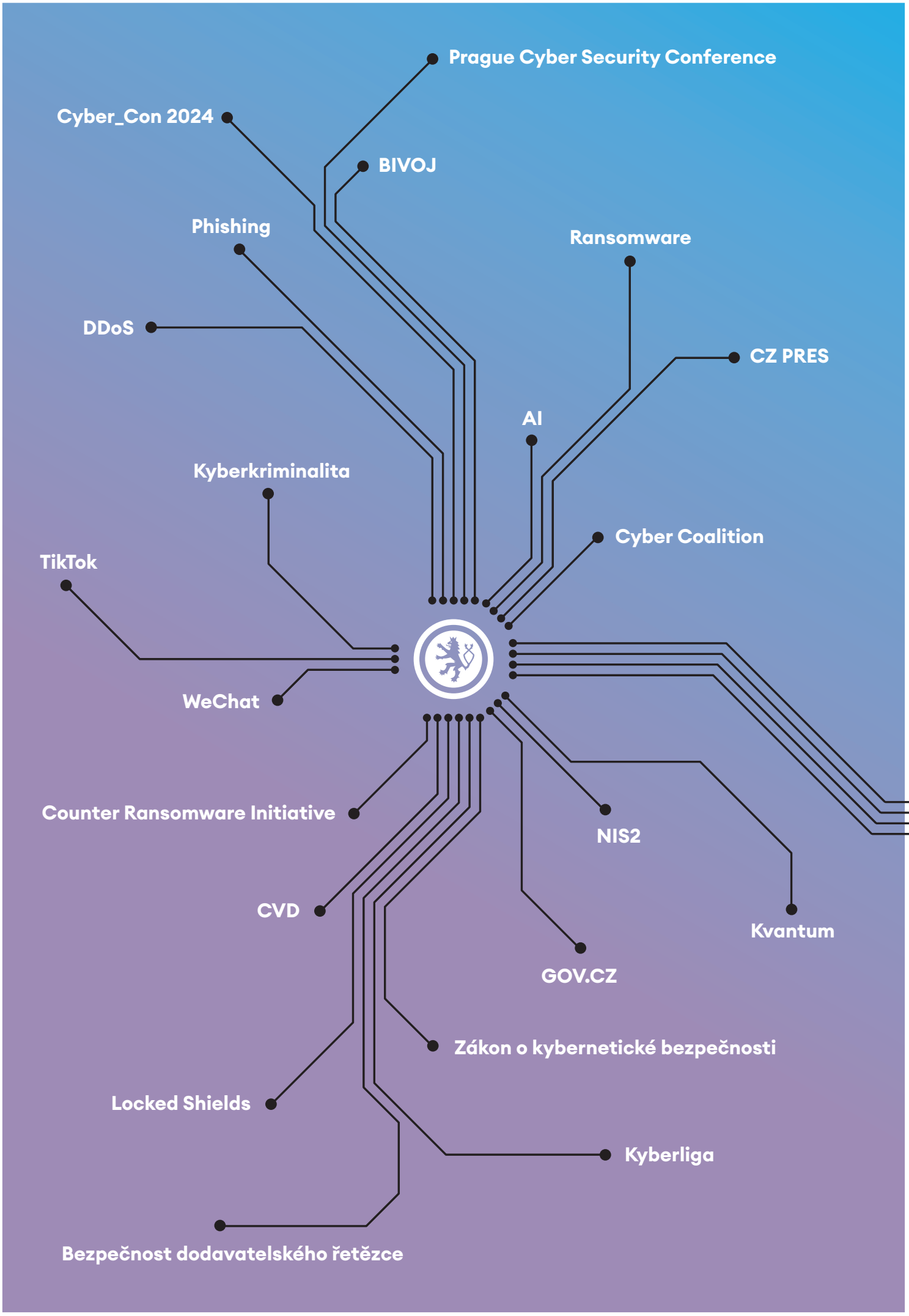
O NÚKIB



NÚKIB je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Dále má na starosti problematiku veřejně regulované služby v rámci družicového systému Galileo. NÚKIB vznikl 1. srpna 2017 na základě zákona č. 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

Pro více informací o NÚKIB navštivte naše webové stránky www.nukib.gov.cz nebo sledujte aktuality z oblasti kybernetické bezpečnosti v ČR na našich sociálních sítích X, LinkedIn, Facebook nebo Instagram. Záznamy z některých akcí, které NÚKIB pořádá nebo se jich účastní jeho zástupci, pak najdete na YouTube kanálu NÚKIB.


Zajišťování bezpečnosti utajovaných informací v informačních a komunikačních systémech včetně kryptografické ochrany
Vyhodnocování rizik v oblasti kybernetické bezpečnosti a přijímání příslušných nápravných a preventivních opatření
Poskytování včasných, jasných a relevantních informací subjektům kritické informační infrastruktury, provozovatelům základní služby i orgánům veřejné správy
Analýzy trendů v oblasti kybernetické bezpečnosti
Vedení operativní reakce na kybernetické incidenty s využitím expertizy a přístupu k informacím pro efektivní zvládnutí incidentů
Pořádání tréninků a kybernetických cvičení na národní i mezinárodní úrovni
Spolupráce s veřejným, soukromým a akademickým sektorem na národní i mezinárodní úrovni
NÚKIB zajišťuje kybernetickou bezpečnost ČR a jejích obyvatel prostřednictvím:
Poskytování metodické podpory, vzdělávání a osvěty v tématech spojených s oblastí kybernetické bezpečnosti
Implementace a provoz veřejně regulované služby Evropského programu družicové navigace Galileo (PRS)
Zastupování České republiky v orgánech mezinárodních organizací působících v oblasti kybernetické bezpečnosti
Poskytování technické pomoci a dalších služeb (prověření zabezpečení pomocí technik penetračního testování nebo poskytování skenů zranitelností)
Provádění kontroly dodržování požadavků zákona o kybernetické bezpečnosti u regulovaných osob
Přípravy národních bezpečnostních standardů, zákonů a podzákonných norem v oblasti kybernetické bezpečnosti
Provádění výzkumu a vývoje v oblasti kybernetické bezpečnosti


Prague Cyber Security Conference
Cyber_Con 2024
BIVOJ
Phishing
Ransomware
DDoS
CZ PRES
AI
Kyberkriminalita
Cyber Coalition
TikTok
WeChat
Counter Ransomware Initiative
NIS2
CVD
Kvantum
GOV.CZ
Zákon o kybernetické bezpečnosti
Locked Shields
Kyberliga
Bezpečnost dodavatelského řetězce