Národní úřad
pro kybernetickou
a informační bezpečnost

ZPRÁVA O STAVU KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY

2025

ÚVODNÍ SLOVO ŘEDITELE NÁRODNÍHO ÚŘADU PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST

Vážené čtenářky, vážení čtenáři,

rok 2025 byl z pohledu kybernetické a informační bezpečnosti rokem významných posunů. Byť po třech letech došlo k meziročnímu poklesu celkového počtu kybernetických incidentů hlášených NÚKIB, bylo by chybou tento vývoj interpretovat jako oslabení hrozeb v kyberprostoru. Naopak vývoj uplynulého roku ukazuje, že kybernetické hrozby jsou stále sofistikovanější, cílenější a v řadě případů i závažnější.

Ing. Lukáš Kintr

ředitel Národního úřadu
pro kybernetickou
a informační bezpečnost

I přes výrazný úbytek DDoS útoků hacktivistických skupin zůstávají právě útoky na dostupnost nejčastějším typem evidovaných incidentů. Stejně tak phishing nadále představuje nejrozšířenější hrozbu, s níž se setkává naprostá většina z nás. Tyto skutečnosti potvrzují, že vedle technologických, systémových a legislativních opatření má klíčový význam i lidský faktor, prevence a systematické zvyšování povědomí o rizicích.

Uplynulý rok zároveň přinesl změnu z hlediska závažnosti nahlášených incidentů. Počet velmi významných kybernetických incidentů vzrostl, což ukazuje, že i při celkovém poklesu incidentů čelí Česká republika stále hrozbám s potenciálně zásadními dopady na chod státu, jeho institucí a jimi poskytovaných služeb občanům naší země.

Zásadní význam měl rok 2025 také v oblasti strategického a legislativního ukotvení kybernetické bezpečnosti. Vláda poprvé provedla národní atribuci škodlivé kybernetické kampaně, konkrétně té vedené státem sponzorovaným aktérem proti Ministerstvu zahraničních věcí. Tento krok jasně deklaruje připravenost státu otevřeně reagovat na závažné kybernetické hrozby. V této souvislosti bych rád uvedl také dvě varování, která NÚKIB v uplynulém roce vydal: proti produktům společnosti DeepSeek, ale hlavně široce aplikovatelné varování před hrozbou spočívající v předávání dat a ve výkonu vzdálené správy z Čínské lidové republiky. Obě tato varování reflektují rostoucí význam strategické závislosti na technologiích a potřebu posuzovat bezpečnost nejen optikou jednotlivých produktů, ale i širších geopolitických souvislostí.

Důležitým milníkem bylo rovněž nabytí účinnosti nového zákona o kybernetické bezpečnosti a spuštění Portálu NÚKIB, který vytváří jednotný nástroj pro plnění zákonných povinností regulovaných subjektů. V září minulého roku byla schválena také Národní strategie kybernetické bezpečnosti, založená na principu zdůrazňujícím společnou odpovědnost státu, veřejného, soukromého i akademického sektoru a jednotlivců. Právě schopnost spolupráce napříč společností bude do budoucna jedním z hlavních předpokladů odolnosti České republiky vůči kybernetickým hrozbám.

Věřím, že tato zpráva poskytne stejně jako každý rok srozumitelný přehled o stavu kybernetické bezpečnosti v České republice a že podobně jako v minulých letech podpoří další zájem o kybernetickou bezpečnost. Stejně tak věřím, že podpoří další odbornou i veřejnou debatu o tom, jak posilovat naši bezpečnost, důvěru a odpovědnost v dnešní digitální společnosti.

OBSAH

O DOKUMENTU

Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) na začátku roku 2026 rozeslal subjektům regulovaným podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů, i řadě dalších klíčových institucí a organizací, které zákonem o kybernetické bezpečnosti v době tvorby Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2025 (dále jen „Zpráva“) regulovány nebyly či stále nejsou (zákon č. 264/2025 Sb., o kybernetické bezpečnosti, začal platit v listopadu 2025 a lhůta na sebeurčování regulovaných subjektů skončila 31. 12. 2025), dotazník se 63 otázkami. 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 425 subjektů, z toho 338 regulovaných a 87 neregulovaných (podle zákona č. 181/2014 Sb.). Ze získaných dat NÚKIB čerpal informace pro potřeby Zprávy. Veškeré údaje z dotazníků jsou anonymizovány.

Proces hodnocení

Hodnocení stavu kybernetické bezpečnosti v České republice (dále jen „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 zkreslené. 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 2025 potýkala, stejně jako aktivity, které napomáhají jejich zmírnění.

Pravděpodobnostní výrazy použité ve Zprávě o stavu kybernetické bezpečnosti České republiky za rok 2025

Pravděpodobnostní výrazy a vyjádření jejich procentuálních hodnot:

Výraz	Pravděpodobnost
Téměř jistě	90–100 %
Velmi pravděpodobně	75–85 %
Pravděpodobně	55–70 %
Nelze vyloučit / reálná možnost	40–50 %
Nepravděpodobně	20–35 %
Velmi nepravděpodobně	0–15 %

SEZNAM POUŽITÝCH ZKRATEK

AI	Umělá inteligence
BIS	Bezpečnostní informační služba
CRA	Cyber Resilience Act
CSA	Cyber Security Act
ČLR	Čínská lidová republika
ČR	Česká republika
DDoS	Distributed Denial of Service
DORA	Digital Operational Resilience Act
ENISA	Evropská agentura pro bezpečnost sítí a informací
EU	Evropská Unie
GRU	Hlavní správa generálního štábu Ozbrojených sil Ruské federace, (Главное управление Генерального штаба Вооружённых Сил Российской Федерации)
ICT	informační a komunikační technologie
ISVS	informační systémy veřejné správy
IT	informační technologie
JCSA	Joint Cyber Security Advisory
KLDR	Korejská lidově demokratická republika
LLM	Velké jazykové modely
NATO	Severoatlantická aliance
NP	Národní politiky kryptografické ochrany utajovaných informací
NSKB	Národní strategie kybernetické bezpečnosti
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
p. b.	procentní body
PCSC	Prague Cyber Security Conference 2025
USA	Spojené státy americké
VZ	Vojenské zpravodajství
ZKB	zákon č. 264/2025 Sb., o kybernetické bezpečnosti
Zpráva	Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2025

2025: KYBERNETICKÁ BEZPEČNOST V ČÍSLECH

▲ 21 137
trestných činů v oblasti kybernetické kriminality a kriminality páchané na internetu

▲ 194
správců významných informačních systémů

▲ 2
velmi významné kybernetické incidenty řešené NÚKIB

▲ 373
účastníků cvičení kybernetické bezpečnosti uspořádaných NÚKIB

▲ 4509
celkový počet regulovaných systémů (k 31. 12. 2025)

▲ 183
informačních systémů základních služeb

▲ 69
správců kritické informační infrastruktury

(porovnání s rokem 2024)

▲ 11
cvičení kybernetické bezpečnosti provedených NÚKIB, z toho 5 s mezinárodní účastí

▲ 635
významných informačních systémů

▼ 56 033
uživatelů proškolených kurzy NÚKIB

▲ 134
systémů kritické informační infrastruktury (k 31. 10. 2025 dle předchozího zákona)

▲ 151
správců informačních systémů základních služeb

▼ 203
kybernetických incidentů řešených NÚKIB

▼ 12
významných kybernetických incidentů řešených NÚKIB

▼ 189
méně významných kybernetických incidentů řešených NÚKIB

V rámci interních, externích a wi-fi testů bylo identifikováno
227 zranitelností, z toho 18 kritických, 60 vysokých, 94 středních a 55 nízkých.

Za uplynulý rok proběhlo 36 penetračních testů, z toho 8 interních,
11 externích, 4 wi-fi, 6 fyzických, 6 phishingových kampaní a 1 zátěžový test.

Bylo podáno a vypořádáno přes 800 připomínek k novému zákonu
o kybernetické bezpečnosti.

V roce 2025 jsme na Portálu NÚKIB zaznamenali více než 252 tisíc návštěv.

Česká republika v roce 2025 obsadila 1. místo
mezi více než 140 zeměmi v žebříčku National Cyber Security Index,
který vydává estonská nadace e-Governance Academy.

Odpověděli jsme přibližně na 1 278 dotazů ke směrnici NIS 2
a dalším záležitostem spojeným s regulací a kybernetickou bezpečností.

V roce 2025 vyšla 2 varování, nebylo vydáno žádné reaktivní ani ochranné opatření.

SHRNUTÍ ZPRÁVY O STAVU KYBERNETICKÉ BEZPEČNOSTI ZA ROK 2025

V roce 2025 po třech letech klesl počet kybernetických incidentů, a to z 268 na 203. To je do velké míry dáno především snížením počtu incidentů spojených s DDoS útoky hacktivistických skupin. Oproti roku 2024 tento typ útoků klesl na méně než polovinu.

Podle klasifikace incidentů NÚKIB tvořily i v roce 2025 nejčastější typ (46 %) útoky zaměřené na dostupnost, mezi které patří i DDoS. Z pohledu respondentů dotazníkového šetření byl nejčastějším typem útoků phishing (50 %), který zaznamenalo 90 % respondentů. V minulém roce narostl počet velmi významných incidentů o jeden, tedy celkově na dva.

Z pohledu kybernetické bezpečnosti byl rok 2025 pro NÚKIB přelomový zejména v kontextu legislativního ukotvení, pro ČR pak v kontextu národní atribuce.

Vláda v květnu loňského roku provedla národní atribuci škodlivé kybernetické kampaně, kterou vedl čínský státem sponzorovaný aktér APT31 vůči Ministerstvu zahraničních věcí. NÚKIB se spolu s domácími partnery z bezpečnostní komunity účastnil vyšetřování útoku.

Dne 1. listopadu 2025 nabyl účinnosti zákon č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „ZKB“)**, čímž se uzavřela příprava tohoto klíčového předpisu, jež trvala 3 roky, 8 měsíců a 9 dní.** V této souvislosti byl též spuštěn nový Portál NÚKIB, který představuje jednotné místo pro plnění zákonných povinností regulovaných subjektů vůči NÚKIB.

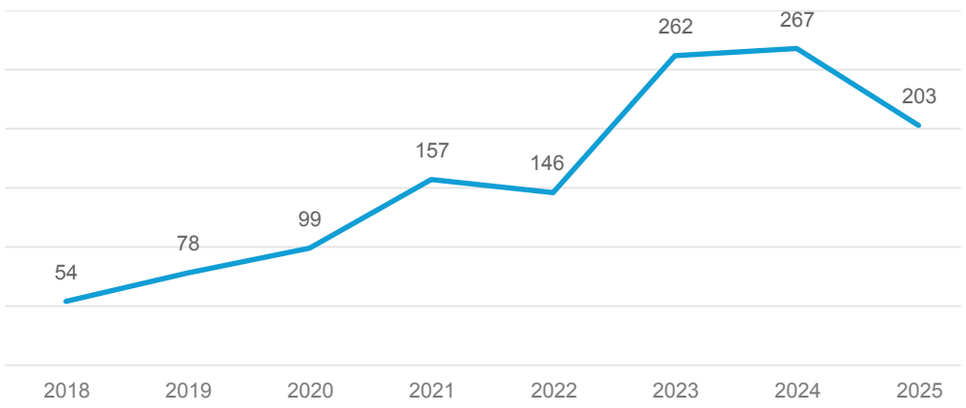
V průběhu roku byla vydána dvě varování, a to proti některým produktům společnosti DeepSeek a zejména pak před hrozbou spočívající v předávání dat a ve výkonu vzdálené správy z Čínské lidové republiky (dále jen „ČLR“). Na základě tohoto varování musí povinné osoby regulované podle zákona o kybernetické bezpečnosti zohlednit hrozbu v analýze rizik a na zjištěná rizika reagovat přijetím přiměřených bezpečnostních opatření.

Varování bylo do značné míry přelomové, jelikož není zaměřené jen na jednu technologii, ale upozorňuje na komplexní problém a je uplatnitelné na všechna odvětví, služby i zařízení.

V září byla vládou schválena Národní strategie kybernetické bezpečnosti, která vychází z principu „whole-of-society“, jehož cílem je propojit všechny relevantní aktéry a vytvořit odolné prostředí schopné reagovat na rozsáhlé krize, dynamické hrozby i technologické změny.

KYBERNETICKÁ BEZPEČNOST ČR V ROCE 2025 Z POHLEDU NÚKIB

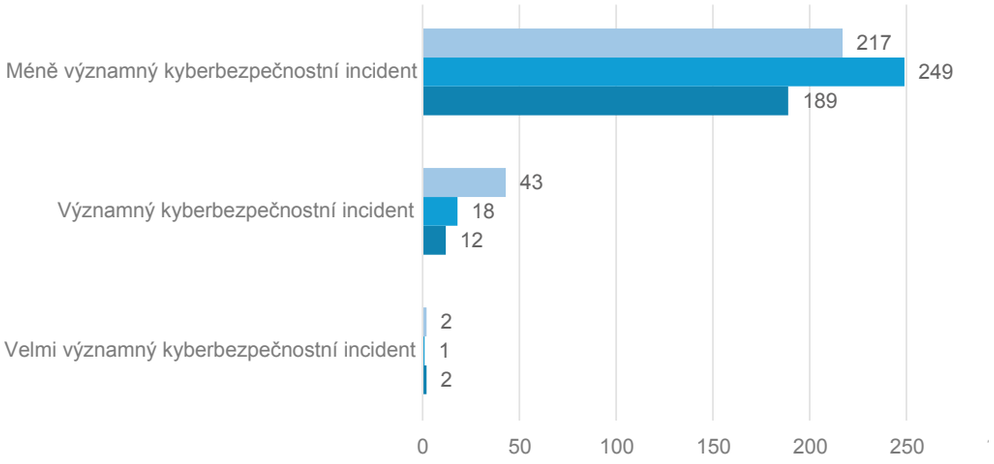
NÚKIB za rok 2025 evidoval celkem 203 kybernetických bezpečnostních incidentů, což je nejnižší hodnota za poslední tři roky. Tento pokles byl do velké míry způsoben zejména výrazně nižším počtem incidentů spojených s DDoS útoky hacktivistů. Oproti roku 2024 tento typ útoků klesl o méně než polovinu (z 167 v roce 2024 na 94 v roce 2025).



Graf 1: Vývoj počtu incidentů evidovaných NÚKIB v letech 2018–2025

Co se závažnosti incidentů týče, v minulém roce narostl počet velmi významných incidentů o jeden, tedy na dva incidenty. Významných incidentů NÚKIB evidoval celkem 12. Ostatní incidenty (189) pak spadaly do kategorie méně významných.

Graf 2: Meziroční srovnání závažnosti incidentů evidovaných NÚKIB v letech 2023–2025

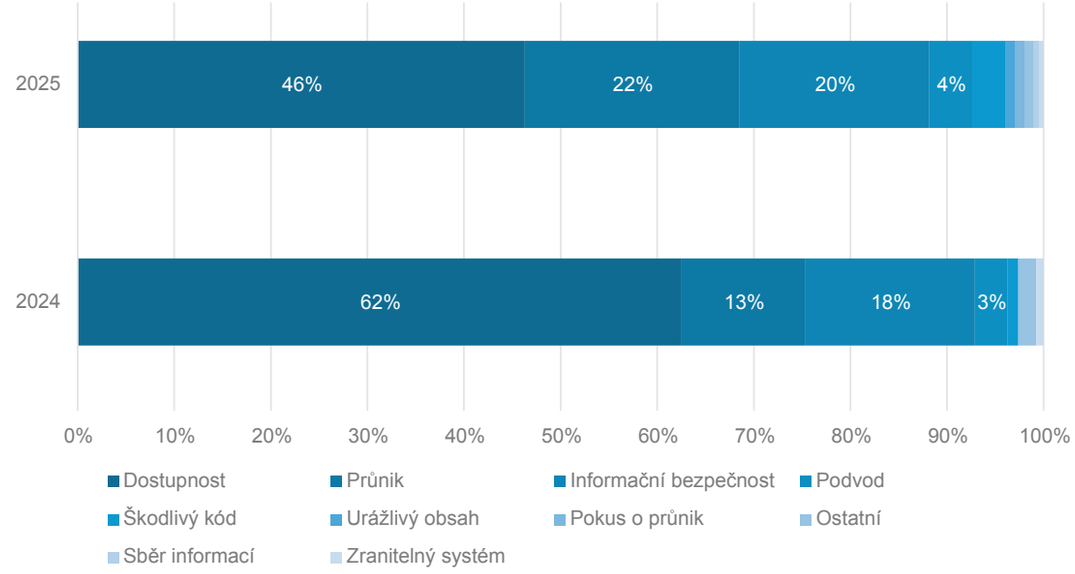


KLASIFIKACE KYBERNETICKÝCH INCIDENTŮ NAHLÁŠENÝCH NÚKIB

Z hlediska klasifikace incidentů již několikátý rok v řadě převažovaly incidenty cílící na dostupnost, ačkoliv jejich podíl se oproti předešlému roku značně snížil.

Narostl naopak počet průniků, které tak tvořily druhou nejpočetnější kategorii. Nárůst průniků NÚKIB nespojuje s žádnou konkrétní rozsáhlejší kampaní a jde spíše o souhru okolností. Další v pořadí byla kategorie Informační bezpečnosti, kam spadaly především ransomwarové útoky.

Graf 3: Procentuální zastoupení kategorií v rámci klasifikace incidentů v letech 2024–2025



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.

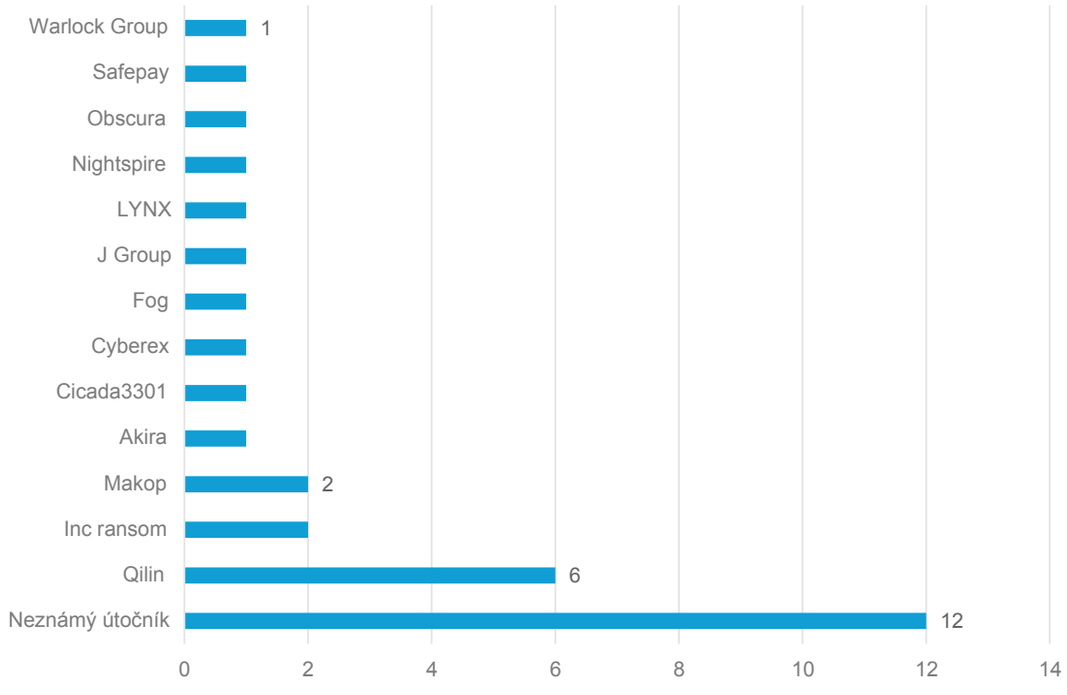
Sběr informací – např. skenování, sniffing, sociální inženýrství

RANSOMWAROVÉ ÚTOKY

Ransomwarové útoky patří dlouhodobě mezi jednu z nejzávažnějších kybernetických hrozeb. Ransomwarovým gangům jde primárně o finanční zisk a tomu odpovídá i skutečnost, že nejsou vybíraví a útočí na společnosti i organizace různých velikostí napříč sektory. Během roku 2025 evidoval NÚKIB incidenty spojené s ransomwarem například ve veřejném, vzdělávacím, zdravotnickém, bezpečnostním, průmyslovém či technologickém sektoru. Stejně tak různorodá byla skladba aktérů, kteří za těmito útoky stály. **S výjimkou gangu Qilin, který patří mezi nejaktivnější ransomwarové aktéry globálně, stály ostatní skupiny za jedním až dvěma útoky.**

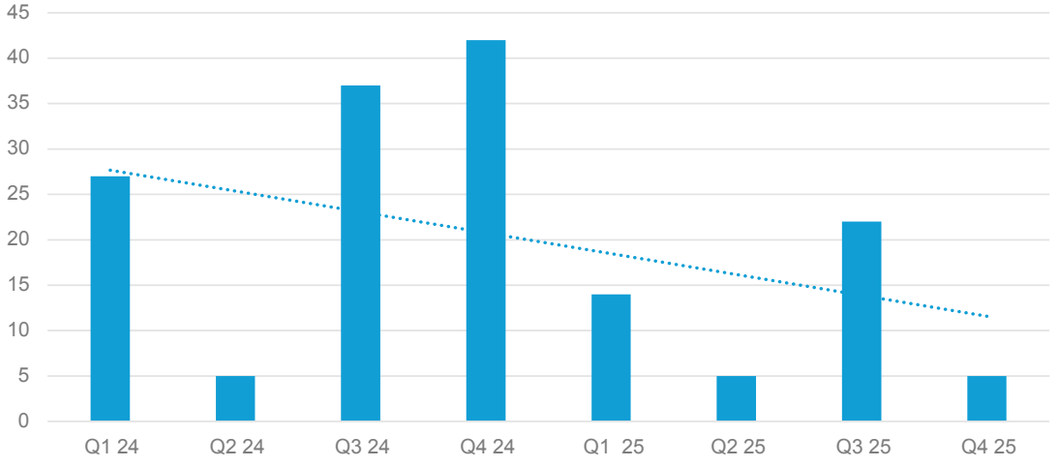
Kromě výše uvedeného evidoval NÚKIB trend postupné změny celého ekosystému ransomwarových skupin. **Stejně jako v globálním měřítku, tak i v českém kyberprostoru působil větší počet menších ransomwarových skupin.** Celá problematika byla během roku 2025 navíc velmi dynamická. Aktéři rychleji vznikali, rebrandovali se, slučovali se a podobně. V tomto důsledku se stává mnohem složitější udržovat si přehledu o modu operandi každého z nich.

Graf 4: Aktéři stojící za ransomwarovými útoky evidovanými NÚKIB v roce 2025



Ačkoliv DDoS útoky zpravidla nevedou k tak závažným dopadům jako ransomware, jedná se o dlouhodobě nejpočetnější typ útoku v rámci evidence NÚKIB. To platilo i v roce 2025, ačkoliv v tomto období jejich počet výrazně poklesl. Na poli hacktivismu došlo během roku ke značnému vývoji. Jednou z klíčových událostí byla společná mezinárodní operace s názvem Eastwood koordinovaná Europolem a Eurojustem, která se zaměřila na proruskou hacktivistickou skupinu NoName0578(16). ČR patřila mezi státy, které se do operace, jejímž cílem bylo narušit infrastrukturu a aktivity této skupiny, zapojily. Operace vyústila v červenci 2025 v narušení klíčové infrastruktury skupiny a vydání několika zatykačů na zodpovědné osoby.

NÚKIB nicméně zaznamenal postupný útlum aktivit proruských hacktivistů již před operací Eastwood. Pro srovnání – v první polovině roku 2025 NÚKIB evidoval necelé dvě desítky incidentů spojených s DDoS útoky, zatímco během druhé poloviny roku 2024 šlo o téměř čtyřnásobek. **Ačkoliv ve třetím čtvrtletí došlo k mírnému nárůstu útoků mj. v důsledku odvetných útoků hacktivistů v reakci na operaci Eastwood, celkový počet incidentů spojených s DDoS útoky se meziročně snížil více než dvojnásobně.**



Graf 5: Čtvrtletní vývoj incidentů spojených s DDoS útoky v letech 2024–2025

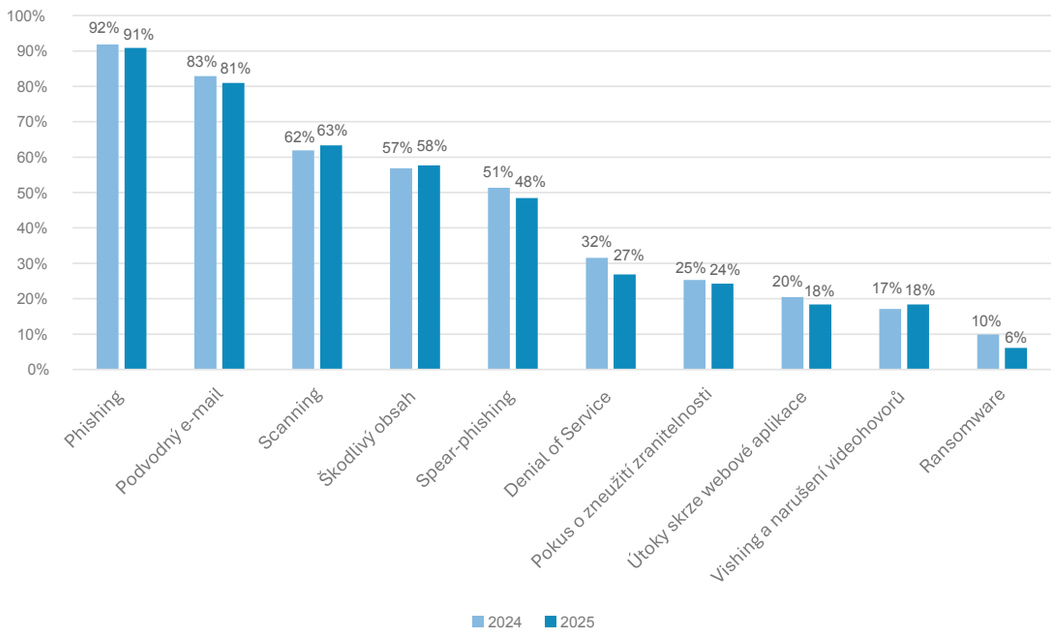
Naopak trend cílení hacktivistů na systémy operačních technologií, který NÚKIB zmiňoval již v minulé Zprávě o stavu kybernetické bezpečnosti, zaznamenal mírný nárůst. Tyto útoky se od DDoS útoků liší tím, že necílí pouze na dosažení dočasné nedostupnosti, ale zpravidla na manipulaci se systémem. Navzdory mírnému nárůstu se však stále jednalo o nižší jednotky případů, a to o útoky primárně proti nedostatečně zabezpečeným systémům se zařízeními vystavenými do internetu. Žádný z útoků nevedl k významnějším škodám, celkově se tak stále jedná o minoritní trend.

INCIDENTY POHLEDEM SUBJEKTŮ

V roce 2025, tak jako v minulých letech, tvořily nejčastější typy útoků phishing, podvodný e-mail a scanning, přičemž jejich závažnost byla respondenty hodnocena jako méně závažná až marginální. Obecně nejzávažnější typy útoků pak představovaly škodlivý obsah, útoky na dostupnost (např. DDoS) a ransomware.

Respondenti nejčastěji upozorňovali na vyšší sofistikovanost phishingových útoků a jejich variant, včetně možného zapojení nástrojů umělé inteligence (dále jen „AI“) při jejich tvorbě. Současně však platí, že více než čtvrtina oslovených organizací své zaměstnance vůbec netestovala (např. pomocí falešných phishingových e-mailů). **Přitom právě pravidelné testování a osvěta patří k nejúčinnějším nástrojům pro posilování odolnosti zaměstnanců vůči kybernetickým hrozbám.**

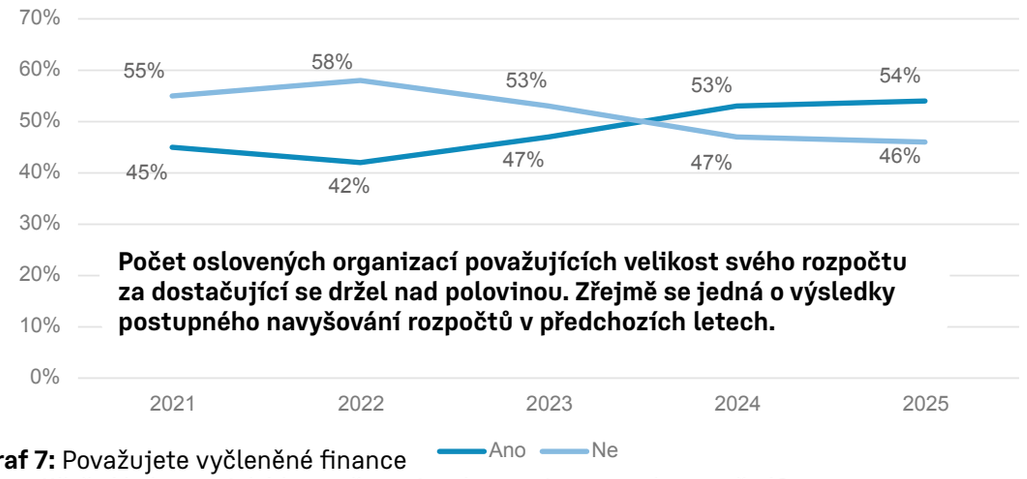
Phishing, podvodný e-mail a scanning zůstávají nejčastějšími typy útoků.



Graf 6: Jaké typy útoků nebo pokusů o ně jste v minulém roce zaznamenali?

Rok 2025 představoval v otázkách finančních prostředků vynaložených na kybernetickou bezpečnost období pokračování mírně pozitivních trendů bez výrazných propadů. Ačkoliv přibližně polovina dotazovaných subjektů (51 %) stále hlásila nárůst rozpočtu na kybernetickou bezpečnost, ve srovnání s minulými lety byla patrná stagnace, neboť podíl těchto subjektů se dále nezvýšil. **Již druhým rokem však bylo možné sledovat stoupající množství institucí, které považovaly svůj rozpočet na kybernetickou bezpečnost za dostatečný** (viz graf 7). Ačkoliv tato hodnota v roce 2025 opět stoupla, jedná se bohužel pouze o navýšení o jeden procentní bod (dále jen „p. b.“) a neopakuje se tak výrazný nárůst z období mezi roky 2023 a 2024. Zřejmě se tedy nejednalo o začátek trendu uspokojivého naplňování potřeb IT oddělení oslovených organizací, ale pouze o dílčí zlepšení.

Finance vynaložené na kybernetickou bezpečnost: Jako nedostatečný hodnotila svůj rozpočet méně než polovina subjektů, výrazně se však lišily v potřebném navýšení

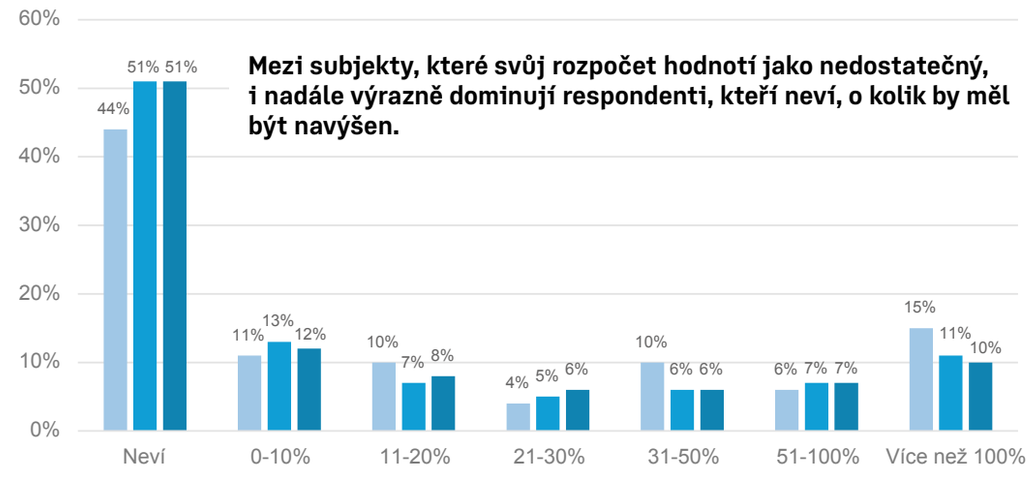


Počet oslovených organizací považujících velikost svého rozpočtu za dostačující se držel nad polovinou. Zřejmě se jedná o výsledky postupného navyšování rozpočtů v předchozích letech.

Graf 7: Považujete vyčleněné finance na zajištění kybernetické bezpečnosti své organizace za dostatečné?

Druhým významným aspektem bylo určení potřebného navýšení rozpočtu v případě, že současná výše nestačí. Dlouhodobě převažují respondenti, kteří nedokážou odhadnout, o kolik by měl být jejich rozpočet navýšen (viz graf 8). Rozdíl mezi touto skupinou a druhou nejčastější odpovědí (0–10 %) činil 39 p. b. Je možné, že právě obtížnost stanovit vlastní reálné potřeby a komunikovat je v rámci organizace, mohla taktéž hrát roli v pomalu stoupajícím navyšování rozpočtů.

Bez ohledu na představy o výši ideálního rozpočtu se však organizace s nedostatečným rozpočtem shodovaly na konkrétních prioritách. Největší investice byly potřeba do nových technologických řešení a zabezpečení infrastruktury.



Mezi subjekty, které svůj rozpočet hodnotí jako nedostatečný, i nadále výrazně dominují respondenti, kteří neví, o kolik by měl být navýšen.

Graf 8: Pokud rozpočet na zajištění kybernetické bezpečnosti hodnotíte jako nedostatečný, o kolik procent by se podle vás měl navýšit?

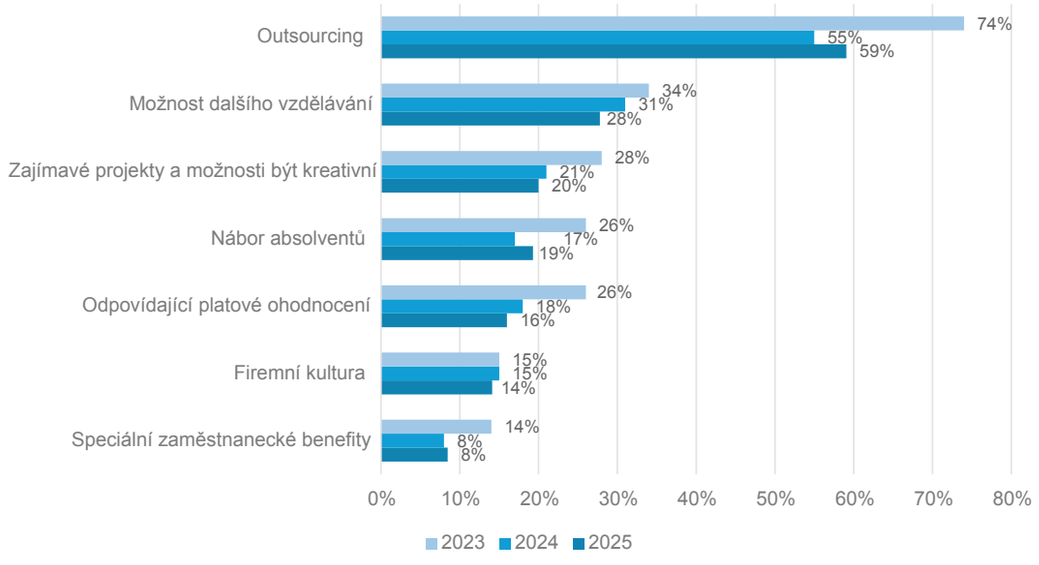
LIDÉ: PŘETRVÁVAL NEDOSTATEK KVALIFIKOVANÝCH ODBORNÍKŮ NA TRHU PRÁCE, UŽIVATELÉ BYLI PRAVIDELNĚ ŠKOLENI, ALE NEDOSTATEČNĚ TESTOVÁNI

Oslovené organizace měly i v roce 2025 problémy s hledáním kvalifikovaných odborníků v oblasti kybernetické bezpečnosti. Zcela dominantním faktorem, který podle oslovených organizací uchazeče odrazoval, bylo nedostatečné finanční ohodnocení (75 %). Nejhorší byla v tomto ohledu situace ve veřejném sektoru a ve vzdělávání, kde finanční ohodnocení jako hlavní překážku uvedlo 92 %, respektive 84 % organizací.

Mezi další faktory patřila chybějící perspektiva osobního anebo profesního rozvoje (21 %) a nedostatečné zaměstnanecké benefity (19 %). Respondenti také uvedli, že významnou překážku představuje nedostatečné množství uchazečů na trhu práce.

Nedostatek kvalifikovaného personálu v oblasti kybernetické bezpečnosti organizace nadále nejčastěji řešily prostřednictvím outsourcingu. Získat nové odborníky se snažily i příležitostmi k dalšímu vzdělávání a zajímavými projekty, byť méně než v předchozích letech (viz graf 9).

Nejčastějším řešením nedostatku odborníků zůstává outsourcing.

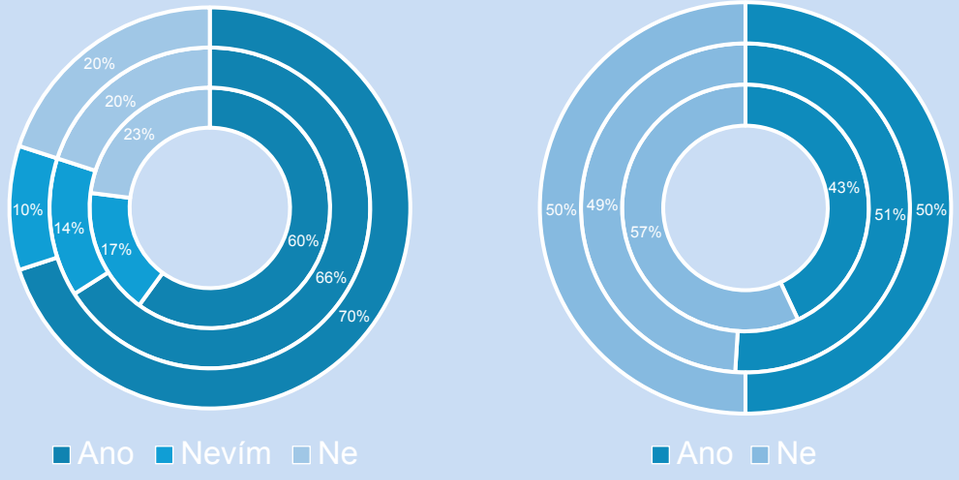


Graf 9: Pokud se vaše organizace potýká s nedostatkem odborníků na kybernetickou bezpečnost, jak se s tímto nedostatkem snaží vypořádat?

Mezi pět nejobtížněji obsazovaných pozic respondenti řadili architekty kybernetické bezpečnosti, pozice bezpečnostního dohledu SIEM, správce síťové infrastruktury, správce serverové infrastruktury a auditory kybernetické bezpečnosti.

Pozitivním trendem byl kontinuálně narůstající podíl organizací, které hodnotí prostředky vydávané na školení svých odborníků jako dostatečné (70 %). Nepokračoval však nárůst podílu organizací, které dedikují finanční prostředky specificky na školení uživatelů. Celých 50 % organizací tak muselo vzdělávání zaměstnanců provádět bez dodatečných zdrojů (viz graf 10).

Finanční prostředky směřují na školení odborníků.
Vzdělávání uživatelů se v polovině případů musí obejít bez financí.

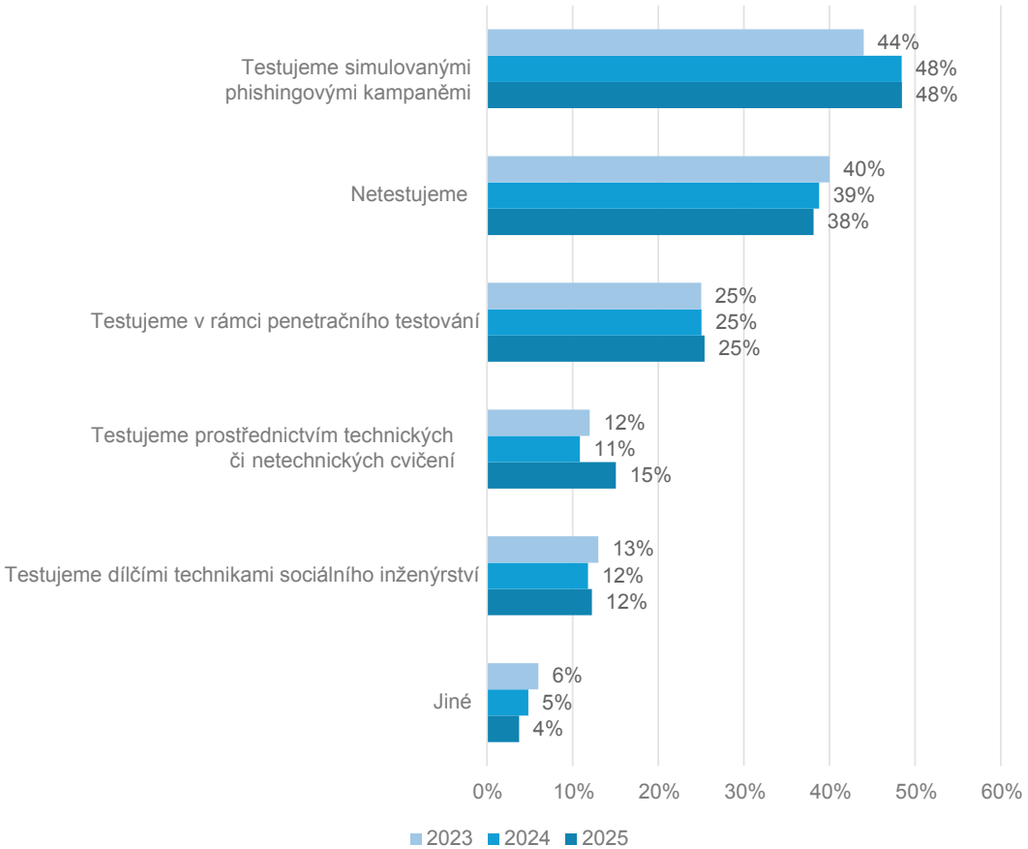


Graf 10: Odborníci: Disponuje podle vás vaše organizace dostatečnými finančními prostředky na pravidelná školení odborníků v oblasti kybernetické bezpečnosti?
Uživatelé: Alokuje vaše organizace každý rok finanční prostředky specificky na školení všech uživatelů v oblasti kybernetické bezpečnosti?

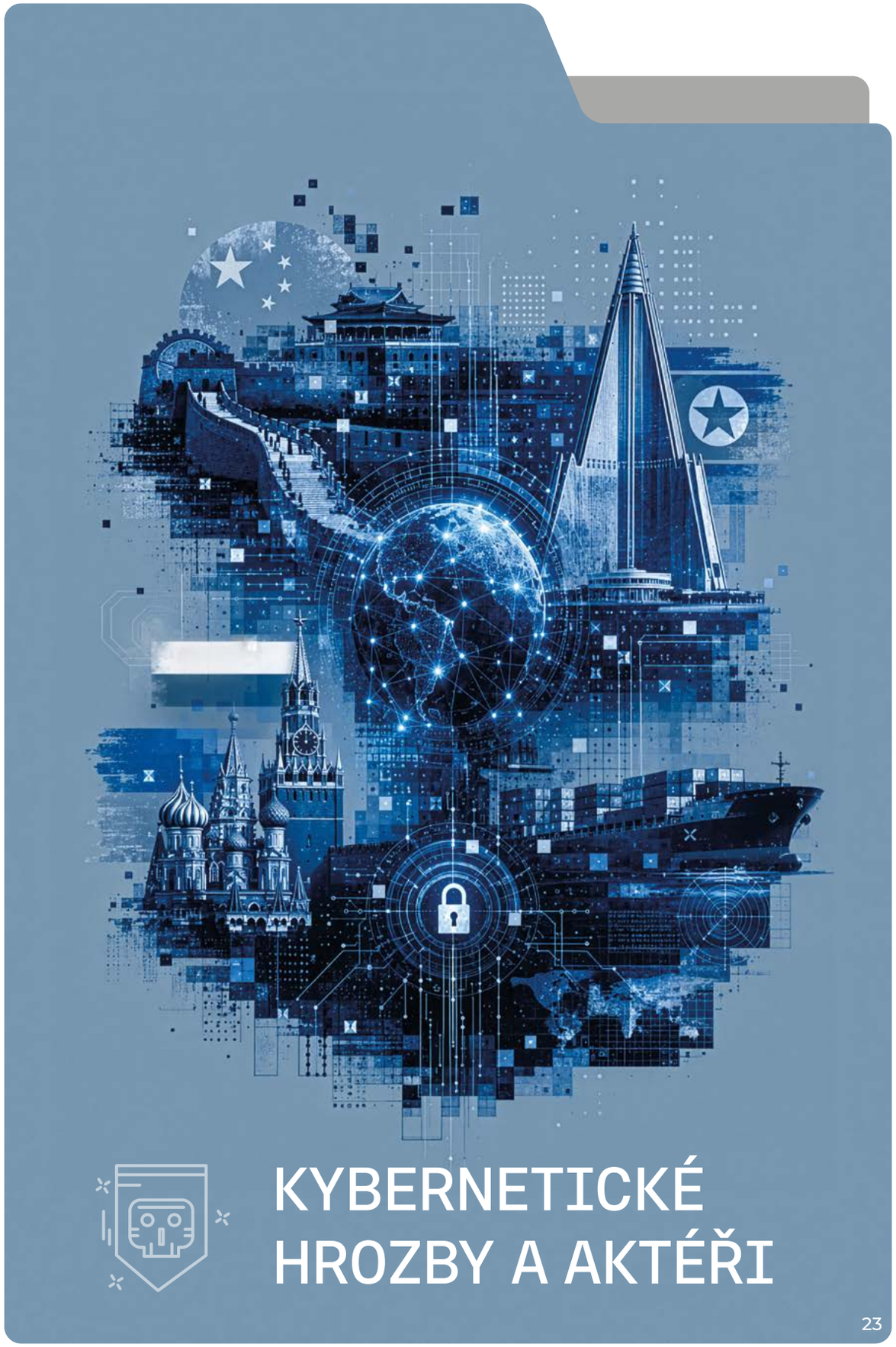
Podíl organizací školících své zaměstnance v kybernetické bezpečnosti narostl již na 96 %; školení probíhají nejčastěji jednou ročně (56 %).
Častěji školí své zaměstnance 27 % organizací, méně často 17 %.

Nejběžnějším způsobem školení bylo i nadále informování zaměstnanců např. formou e-mailů nebo interních portálů. Testování kybernetické odolnosti zaměstnanců probíhalo nejčastěji formou simulovaných phishingových kampaní, dále v rámci penetračního testování, pomocí technických či netechnických cvičení anebo dílčími technikami sociálního inženýrství (např. náhodně rozmístěné USB disky). **Celých 38 % organizací však své zaměstnance v roce 2025 netestovalo vůbec, přičemž tento podíl se dlouhodobě nedaří významně snižovat** (viz graf 11).

Nejčastější způsob testování zaměstnanců představují simulované phishingové kampaně, významná část organizací však své zaměstnance netestuje vůbec.



Graf 11: Testujete odolnost vašich zaměstnanců proti kybernetickým hrozbám?



KYBERNETICKÉ HROZBY A AKTÉŘI

KYBERNETICKÉ HROZBY A AKTÉŘI

STÁTNÍ AKTÉŘI

Atribuce a mezinárodní spolupráce: součást reakcí na aktivity čínských a ruských aktérů

Čínští a ruští státem sponzorovaní aktéři dlouhodobě představují nejvýznamnější hrozbu pro český kyberprostor a jejich aktivity vůči českým subjektům neustávaly ani v roce 2025. ČR tyto hrozby kontinuálně monitoruje, analyzuje a aktivně na ně reaguje, mj. prostřednictvím oficiálního označení původců útoku a jejich odsouzení. Významnou roli v tomto úsilí hrála také mezinárodní spolupráce a výměna informací, která je zcela klíčovým prvkem při zajišťování kybernetické bezpečnosti a reakcí na závažné hrozby v kyberprostoru.

Čínská lidová republika

Zásadní událostí roku 2025 byla atribuce kybernetického útoku na Ministerstvo zahraničních věcí skupině APT31 napojené na čínskou zpravodajskou službu. Závěry analýzy provedené NÚKIB, Vojenským zpravodajstvím (dále jen „VZ“), Bezpečnostní informační službou (dále jen „BIS“) a Úřadem pro zahraniční styky a informace jednoznačně ukazují, že za touto dlouhodobou škodlivou kampaní trvající od roku 2022 stojí ČLR a velmi pravděpodobně (75–85 %) skupina APT31 (známá též jako Zirconium nebo Judgment Panda), která je spojována s celou řadou útoků proti politickým a jiným cílům, mj. v Evropské unii (dále jen „EU“) či Severoatlantické alianci (dále jen „NATO“). **Česká vláda jednoznačně odsoudila tuto škodlivou kybernetickou kampaň proti své kritické infrastruktuře a vyzvala ČLR, aby dodržovala zásady a principy odpovědného chování států v kybernetickém prostoru, které podpořily všechny státy Organizace spojených národů.** V souvislosti s kybernetickým útokem proti ČR vyjádřila EU a její členské státy, stejně jako všichni spojenci v NATO, solidaritu a podporu.

Výše uvedený kyberútok však nebyl zdaleka jedinou aktivitou čínského státu, na kterou ČR v uplynulém roce reagovala. **NÚKIB se spolu s americkými bezpečnostními vládními agenturami a dalšími mezinárodními partnery připojil ke společné analýze (tzv. Joint Cyber Security Advisory, dále jen „JCSA“) upozorňující na aktivity částečně se překrývající s činností aktéra nejčastěji označovaného jako Salt Typhoon.** Tyto aktivity zahrnovaly průniky do sítí po celém světě s cílem získat k nim dlouhodobý přístup a využívat je pro špionážní činnost. Útočníci se zaměřovali na páteřní routery velkých poskytovatelů telekomunikačních služeb a routery na hranici sítě poskytovatele (provider edge) a zákazníka (customer edge) a využívali kompromitovaná zařízení či důvěryhodná propojení k dalšímu průniku do sítí.

Ruská federace

Ze strany aktérů hrozeb spojovaných s Ruskem byla nejviditelnější dlouhodobá kampaň ruského aktéra APT28 spadající pod tamní vojenskou rozvědku GRU. Reakcí na tuto kampaň bylo společné JCSA, na němž se spolu s partnery ze Spojených států, Spojeného království, Německa, Polska, Austrálie, Kanady, Dánska, Estonska, Francie a Nizozemska podílely české bezpečnostní instituce včetně NÚKIB, BIS a VZ. **Kampaň aktéra APT28 cílila zejména na logistické a technologické firmy zapojené do zahraniční pomoci Ukrajině, ale dotkla se i státních institucí jednotlivých států či IP kamer na hraničních přechodech nebo železničních uzlech na Ukrajině a v přilehlých státech.**

Na konci roku 2025 se NÚKIB společně s dalšími národními partnery připojil k JCSA amerického Federálního úřadu pro vyšetřování na kybernetické útoky proruských hacktivistických skupin mířených na kritickou infrastrukturu. **Na rozdíl od pokročilých státních aktérů tyto skupiny využívají méně sofistikované metody s nižším dopadem, které ale mohou vést k poškození napadených systémů.** Skupiny přitom často nerozumí procesům, jež se snaží narušit, což může vést k nechtěným dopadům, včetně fyzického poškození systémů.

Podvodná schémata aktérů spojených s Korejskou lidově demokratickou republikou

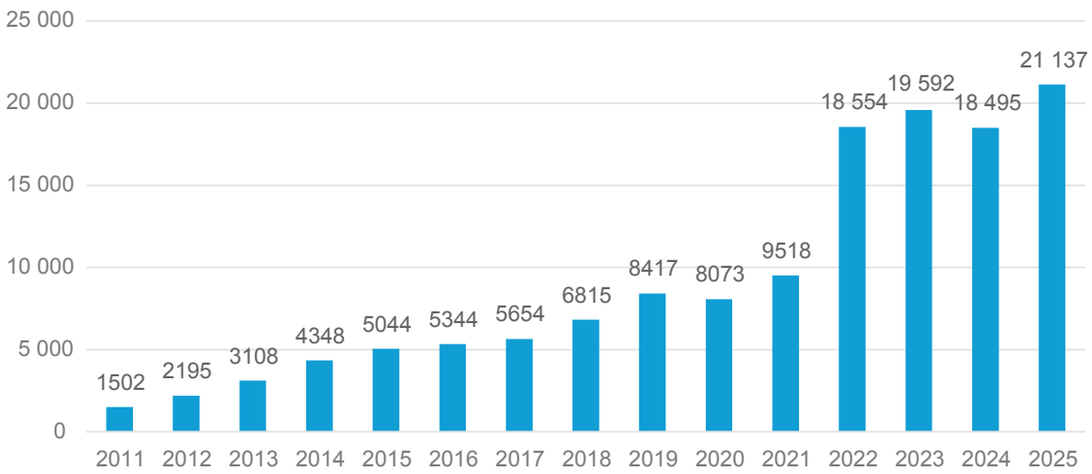
Podvodné schéma, v jehož rámci se občané Korejské lidově demokratické republiky (dále jen „KLDR“) vydávají za legitimní pracovníky v oboru informačních technologií z jiných zemí a nechávají se zaměstnávat na pozicích vykonávaných na dálku, je inovativní strategie, kterou severokorejští aktéři úspěšně využívají k získání finančních prostředků pro tamní režim. Zároveň může dojít i ke krádeži dat a následnému vydírání, popř. ke kyberšpionáži. Celé schéma je pečlivě uzpůsobeno tomu, aby potenciální zaměstnavatel při náboru nepojal žádné podezření. **Tato hrozba se v minulém roce rozšířila i do Evropy, kde byla zaznamenána mj. v Německu, Polsku či Maďarsku.** ČR v seznamu států, které se staly cílem této kampaně, nefiguruje, nicméně do budoucna zájem KLDR o tuzemské společnosti nelze vyloučit (40–50 %).

ÚROVEŇ KYBERKRIMINALITY

V roce 2025 došlo k meziročnímu nárůstu o 14 % v počtu trestných činů v kyberprostoru oproti roku 2024. Konkrétně se jednalo o 2642 skutků.

V porovnání s obdobím 2023–2024, kdy počet evidovaných skutků meziročně klesl téměř o 6 %, došlo k opětovnému zvyšování, které je – až na drobné výchylky – dlouhodobě patrné za celou dobu sledování.

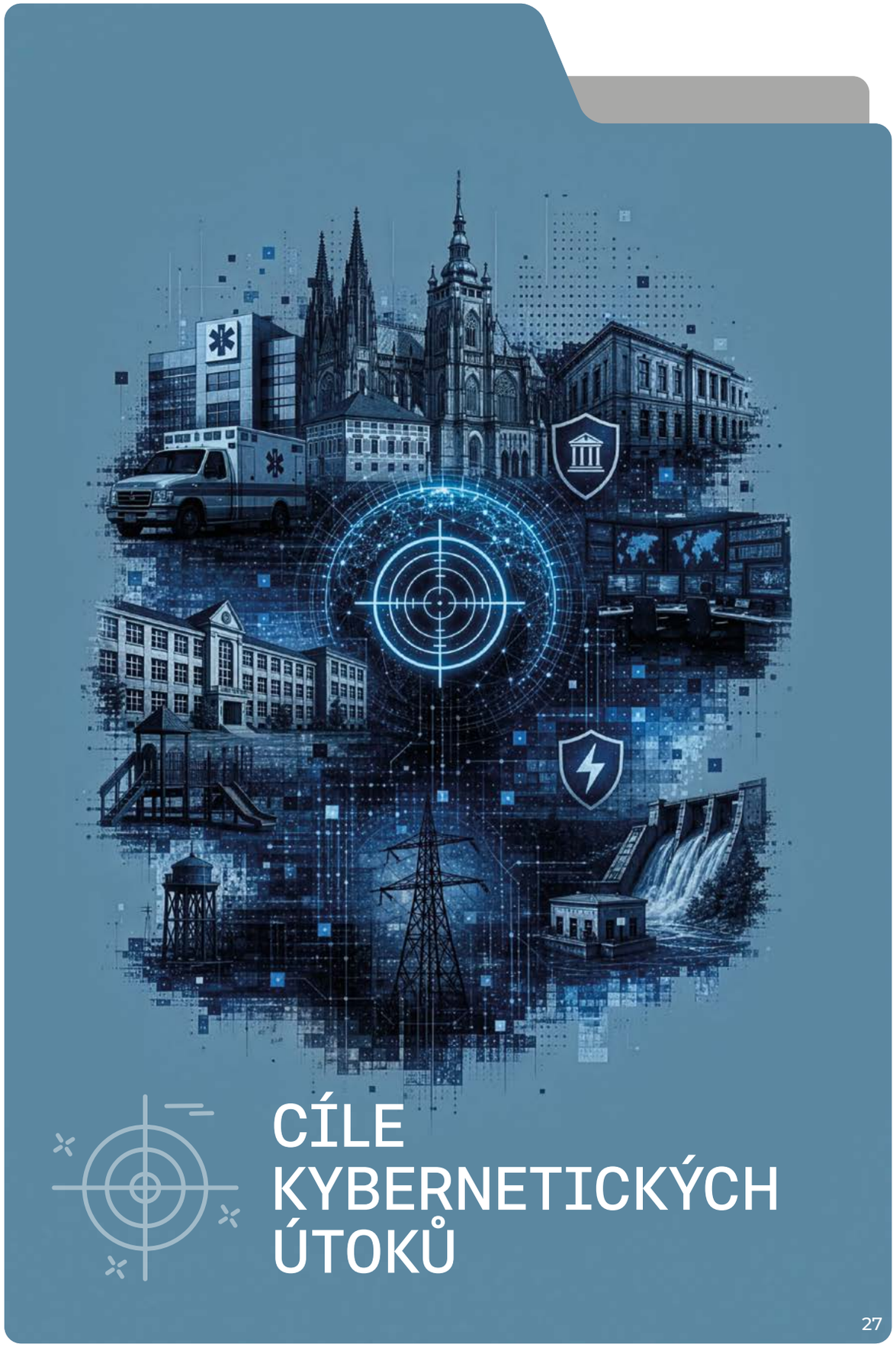
V roce 2025 byl opět zaznamenán nárůst počtu skutků trestné činnosti v kyberprostoru, jedná se o nejvyšší počet od počátku, kdy byl tento typ kriminality poprvé zaznamenán.



Graf 12: Registrované skutky trestné činnosti v ČR páchané v kyberprostoru za období 2011–2025

Podle klasifikace jednotlivých typů trestných kyberkriminánních činů pak tvořilo nejvyšší podíl podvodné jednání, a to již několikáté období v řadě. To je zřejmě dáno využíváním stále propracovanějších technik, přičemž oběťmi podvodů se nestávají pouze osoby, ale i instituce, jako mj. případ dobročinné organizace Tady a teď z roku 2025.

Počet skutků trestné činnosti v kyberprostoru tak stoupá, a to i přes vynaložené prostředky na osvětové i edukační kampaně. V obecné rovině souvisí tento nárůst s přesouváním trestné činnosti do kyberprostoru, což lze nicméně pozorovat celosvětově.



CÍLE KYBERNETICKÝCH ÚTOKŮ

CÍLE KYBERNETICKÝCH ÚTOKŮ

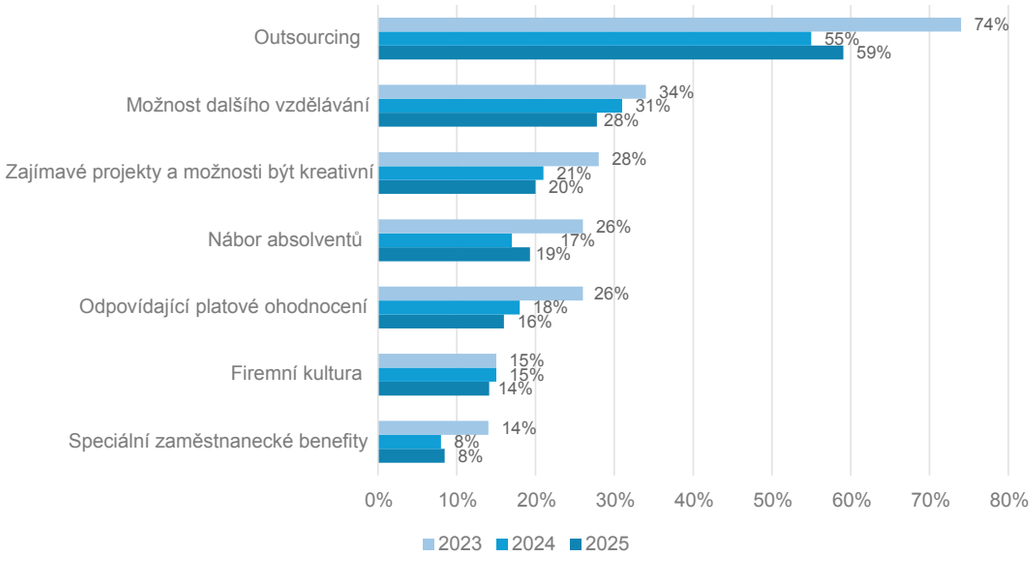
VEŘEJNÝ SEKTOR: STABILNĚ HLAVNÍ CÍL KYBERÚTOKŮ, VÝRAZNĚ PŘIBYLO TĚCH PROSTŘEDNICTVÍM DODAVATELE SLUŽEB

Z dotazníkového šetření plyne, že veřejný sektor i v roce 2025 představoval nejčastější cíl kybernetických útoků, oproti roku 2024 však jejich počet zůstal obdobný. **Mezi nejčastěji zaznamenané typy útoků opět patřil phishing, podvodné e-maily, škodlivý obsah či scanning.** Tento stav mohl odrážet fakt, že navzdory deklarovanému očekávání nedošlo ve veřejném sektoru v roce 2025 u více než poloviny respondentů ke zvýšení rozpočtu na kybernetickou bezpečnost. Ve většině případů tento rozpočet zůstal stejný, nicméně oproti očekáváním dokonce vzrostl počet subjektů, u nichž se rozpočet na kybernetickou bezpečnost snížil.

Oproti minulým letům ubylo detekovaných spear-phishingových útoků a ransomwaru, nicméně pozoruhodně vzrostlo množství útoků skrze dodavatele služeb. Tato skutečnost je v souladu s širším globálním trendem. **Důvodem nárůstu počtu případů u respondentů může být i úspěšnost kyberútoků proti softwarovým službám dodavatelů těchto služeb, případně vůči důvěrnosti dat, které tito dodavatelé, jimiž mohou být i velké nadnárodní společnosti, uchovávají.** Zda se v českém prostředí jedná o anomálii, či nový trend, bude možné vyhodnotit až v budoucnu.

Stejně jako v roce 2024, i v tom minulém platilo, že zaznamenané útoky neměly ve většině případů závažné dopady: nejčastějším praktickým důsledkem bylo omezení dostupnosti služeb.

Nejčastější typy útoků zůstávají stejné, ubylo spear-phishingu a ransomwaru, naopak vzrostl počet útoků prostřednictvím dodavatele služeb.



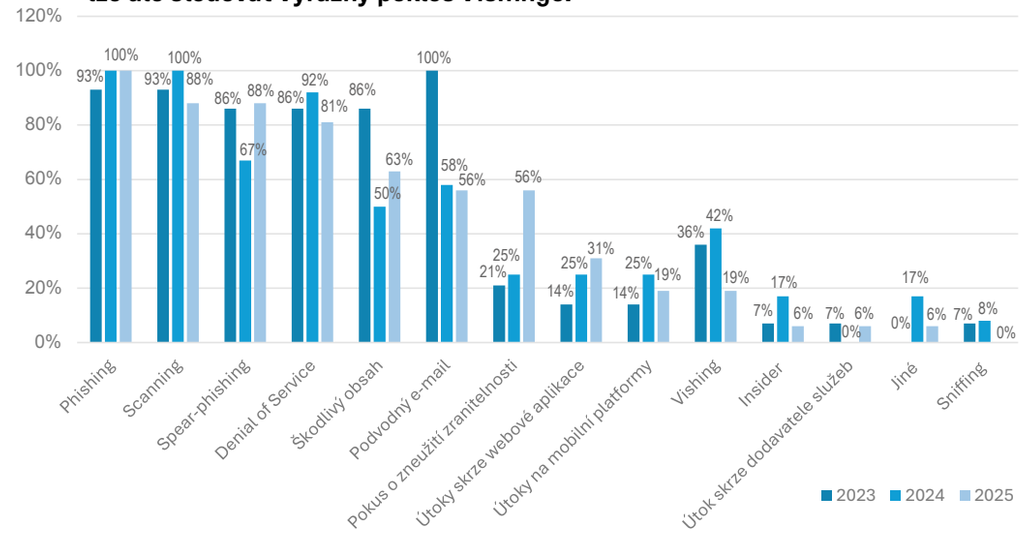
Graf 13: Jaké typy útoků na vaši organizaci nebo pokusů o ně jste v minulém roce zaznamenali?

FINANČNÍ SEKTOR: EXPONOVANÝ SEKTOR S VELKÝM MNOŽSTVÍM ÚTOKŮ, ALE I S DOBROU ODOLNOSTÍ A PROSTŘEDKY

Čtvrtina respondentů v tomto sektoru uvedla, že byla v průběhu roku cílem velkého množství pokusů o kybernetický útok (tedy 101 a více). To je o 9 % více než průměr napříč sektory. Na druhou stranu lze ve srovnání s rokem 2024 pozorovat zlepšení, kdy 101 a více pokusů o útok evidovalo 33 % subjektů. Pozitivním trendem byl také nárůst pokusů o útok, které nevedly k žádným následkům. V roce 2025 nevyústilo v incident 50 % všech pokusů, což představuje zlepšení o 8 p. b. ve srovnání s rokem 2024. **Tyto pozitivní trendy velmi pravděpodobně (75–85 %) souvisely s důrazem finančních institucí na kybernetickou bezpečnost, který se promítl do rozpočtů, a tedy i kapacit a schopností.**

V rámci finančního sektoru považovalo 81 % respondentů svůj rozpočet na kybernetickou bezpečnost za dostatečný, což je vysoko nad celkovým průměrem 54 %. Dominantní formu útoku stále představoval phishing. Výrazné zůstaly i další útoky postavené na sociálním inženýrství, jako spear-phishing nebo podvodné e-maily. Oproti tomu vishing zaznamenal výrazný pokles.

Útoky postavené na sociálním inženýrství stále dominují, lze ale sledovat výrazný pokles vishingu.



Graf 14: Jaké typy útoků na vaši organizaci nebo pokusů o ně jste v minulém roce zaznamenali?

Obecné hrozby související s finančním sektorem: krádeže kryptoměn

V roce 2025 byl pozorován rostoucí trend krádeží kryptoměn severokorejskými aktéry, kteří touto cestou významným podílem napomáhají financovat strategické projekty severokorejského režimu, včetně jaderného programu a vývoje balistických střel. Za dosud největší loupeží kryptoměn stojí severokorejská skupina Trader Traitor. Z dubajské kryptoměnové burzy Bybit v únoru 2025 odcizila kryptoměny v hodnotě přibližně 1,4 miliardy dolarů (30 miliard korun). Členové skupiny zneužili zranitelnosti během rutinních převodů peněženek a manipulovali s transakčními procesy, aby přesměrovali značné finanční prostředky na adresy pod jejich kontrolou.

CÍLE KYBERNETICKÝCH ÚTOKŮ

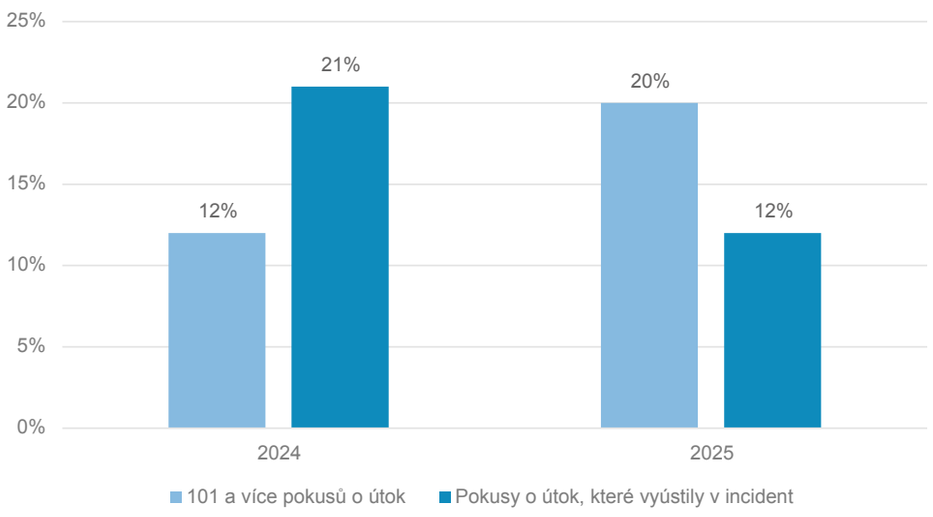
PRŮMYSL A ENERGETIKA: SEKTOR S NÁRŮSTEM DETEKOVANÝCH KYBERÚTOKŮ, ALE TAKÉ S POKLESEM JEJICH ÚSPĚŠNOSTI

V roce 2025 byl, podobně jako ve finančním sektoru, patrný výrazný nárůst počtu pokusů o kybernetický útok v průmyslovém a energetickém sektoru. Počet respondentů, kteří uvedli, že čelili více než 101 pokusu o útok, se v tomto sektoru zvýšil o 8 p. b. Současně však došlo k výraznému poklesu úspěšnosti těchto útoků, což dokládá snížení počtu pokusů, které vyústily v kybernetický incident o 9 p. b. **Lze proto konstatovat, že v roce 2025 pokračoval trend nárůstu počtu kyberútoků na průmyslový a energetický sektor, který však demonstroval vyšší odolnost.**

Tato skutečnost může souviset s tím, že podle většiny respondentů (68 %) došlo k navýšení jejich rozpočtu na kybernetickou bezpečnost, a to dokonce nad rámec očekávání stanovených pro rok 2024. **Zároveň mohl k tomuto pozitivnímu stavu přispět i fakt, že se v tomto sektoru meziročně zvýšil počet pracovníků kybernetické bezpečnosti a o přibližně 4 p. b. více respondentů (aktuálně tedy 87 %) uvedlo, že mají v rámci organizace definované a reálně jmenované kyberbezpečnostní role.**

Samotní respondenti pak ve většině případů uvedli, že úroveň zajištění kybernetické bezpečnosti své organizace považují za dostatečnou (84 % dotázaných) a že se úroveň kybernetické bezpečnosti od minulého roku zlepšila (95 % dotázaných).

Průmyslový a energetický sektor čelil v roce 2025 výrazně většímu množství kybernetických útoků, ale zároveň jim lépe odolával.

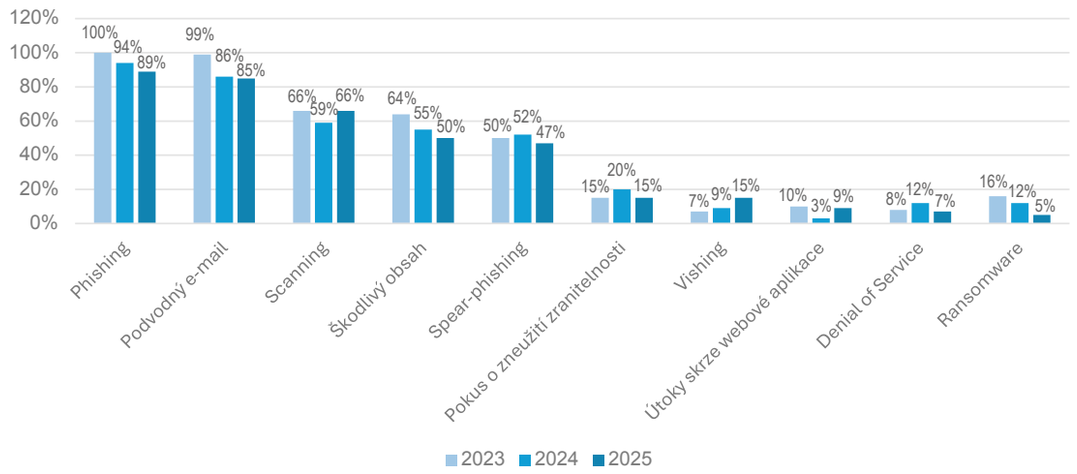


Graf 15: Kolik pokusů o útok detekovala vaše organizace v minulém roce? Kolik z těchto pokusů vyústilo v kybernetický incident?

ZDRAVOTNICTVÍ: MNOŽSTVÍ ÚTOKŮ SE SNÍŽILO, ALE ZÁVAŽNOST MOŽNÝCH NÁSLEDKŮ PŘETRVÁVÁ

Zdravotnický sektor se dlouhodobě řadí mezi nejvíce ohrožené, a to zejména kvůli útokům s vážnými důsledky, jako ransomware, které mohou přímo ovlivnit poskytování zdravotnické péče. V roce 2025 ransomwarový útok vedl k jednomu takovému incidentu i v ČR. Obecně bylo možné v loňském roce pozorovat hned několik pozitivních trendů. Přestože stále dominoval phishing a podvodné e-maily, u obou byl patrný v porovnání s předešlým rokem mírný pokles, tak jako u většiny typů útoků. **Výrazný nárůst zaznamenal vishing, tedy podvodné telefonáty.** Ty byly sofistikovanější a umožňovaly tak pachatelům vyvinout na oběť větší iluzi urgence. K tomu přispívají i nástroje AI, s jejichž pomocí lze vytvořit věrné kopie hlasu nebo tváře osob známých oběti.

Ačkoliv stále dominují phishing a podvodné e-maily, můžeme u nich ve srovnání s minulými roky sledovat pokles, tak jako ve většině kategorií.



Graf 16: Jaké typy útoků na vaši organizaci nebo pokusů o ně jste v minulém roce zaznamenali?

Ransomware vloni zasáhl českou nemocnici, v zahraničí prokazatelně přispěl k úmrtí pacienta

Ransomwarový útok na nemocnici v Nymburku na začátku července loňského roku na více než týden omezil fungování některých oddělení a služeb. Útok naštěstí neohrozil výkon akutní péče a neohrozil žádného z pacientů na životě. V Londýně však ransomwarový útok o měsíc dříve narušil provoz dvou nemocnic natolik, že přispěl k úmrtí pacienta. Incident způsobil zpoždění více než 10 000 vyšetření a taktéž klinické diagnostiky, zejména krevních testů. Podle nemocnice vedlo narušení laboratorních služeb k výraznému prodloužení čekací doby na klíčové výsledky, což se stalo jednou z příčin zmíněného úmrtí.

CÍLE KYBERNETICKÝCH ÚTOKŮ

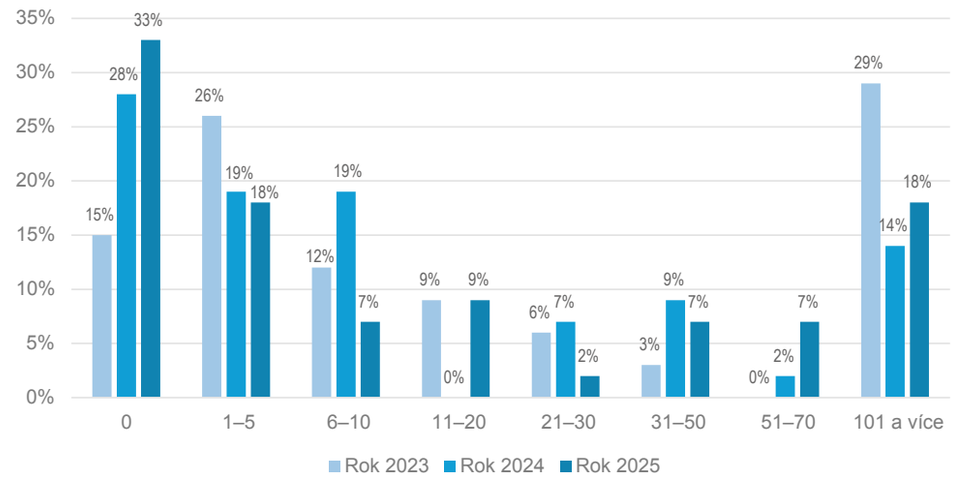
VZDĚLÁVACÍ SEKTOR: PŘEDLOŇSKÝ POKLES POČTU DETEKOVANÝCH KYBERÚTOKŮ SE NEPOTVRDIL JAKO TREND

Po významně menším počtu zaznamenaných pokusů o útok v roce 2024 přišel v roce 2025 opět mírný nárůst. Ten souvisel zejména s vyšším počtem respondentů, kteří uvedli, že zaznamenali více než padesát detekovaných pokusů o útok. O 5 p. b. více respondentů evidovalo 51–70 pokusů o útok, o více než 3 p. b. respondentů pak uvedlo, že evidovali 101 a více pokusů.
Stále je to však méně než v letech 2022 a 2023.

Zároveň platí, že v roce 2025 vyústilo méně pokusů o útok v reálný kybernetický incident. V tomto směru tak byla situace ve vzdělávacím sektoru příznivější než v roce 2024, a to i přesto, že u většiny respondentů nedošlo v roce 2025 ke zvýšení rozpočtu, navzdory deklarovaným očekáváním v roce 2024.

Očekávání na letošní rok jsou pak u většiny subjektů méně optimistická, neboť pouze 38 % respondentů uvedlo, že předpokládají navýšení rozpočtu na kybernetickou bezpečnost (v roce 2024 očekávalo navýšení rozpočtu v roce 2025 49 % respondentů), a 2 % respondentů dokonce předpokládají v roce 2026 snížení rozpočtu na kybernetickou bezpečnost (v roce 2024 takové očekávání nebylo zaznamenáno).

Po poklesu v roce 2024 počet detekovaných útoků opět vzrostl.



Graf 17: Kolik pokusů o útok detekovala vaše organizace v minulém roce?

OBECNÉ HROZBY SPOJENÉ SE VZDĚLÁVACÍM SEKTOREM: NELEGITIMNÍ OVLIVŇOVÁNÍ

Ovlivňování osob či procesů plynoucí z kriminálního jednání, lobbingu či vlivového působení cizí moci představuje hrozbu nejen pro světové, ale i české akademické instituce. Zvyšující se geopolitický význam výzkumu a inovací vytváří z těchto institucí vhodné cíle, přičemž principy jako otevřenost a internacionalizace, na kterých fungují, přispívají obecně k jejich zranitelnosti.

CITLIVÉ OBLASTI VÝZKUMU A VZDĚLÁVÁNÍ:

- kritické technologie pro ekonomickou bezpečnost EU,
- vybrané obory výzkumu a vzdělávání,
- vybraná spolupráce s třetími stranami,
- zboží a technologie dvojího užití a vojenský materiál,
- to, co se daná akademická instituce sama rozhodne do této oblasti zařadit.

Spektrum potenciálně využitelných informací a kontaktů je široké, jelikož i zdánlivě nedůležité střípky informací, např. o vnitřním fungování instituce, mohou představovat zpravodajsky cenná data.

Na konci roku 2025 přišel britský list The Telegraph s obsáhlou investigací, v níž popsal spolupráci předních britských univerzit s čínskými protějšky, která vedla k rozvoji čínských vojenských a zbrojních kapacit. ČLR udržuje státní dohled jak nad soukromým, tak akademickým sektorem, přičemž řada akademických institucí je zde přímo napojena na obranný sektor a armádu, a dochází tak k fúzi civilní a vojenské sféry. V tomto ohledu zvláště vyčnívá tzv. Sedm synů národní obrany, tedy sedm čínských univerzit, které se podílí na armádním výzkumu a vývoji. Některé z těchto univerzit v minulosti spolupracovaly i s institucemi v ČR.

ČASOVÁ OSA VYBRANÝCH UPOZORNĚNÍ A VAROVÁNÍ V ROCE 2025

KVĚTEN

Česká vláda provedla veřejnou atribuci kybernetických útoků ČLR

Vláda v květnu zveřejnila národní atribuci škodlivé kybernetické kampaně, kterou vedla skupina APT31 spojována s čínským Ministerstvem státní bezpečnosti. Tato skupina minimálně od roku 2022 útočila na jednu z neutajovaných sítí Ministerstva zahraničních věcí.

Upozornění na ruskou kybernetickou kampaň proti subjektům podporujícím Ukrajinu

Koncem května se NÚKIB spolu s BIS, VZ a dalšími zahraničními partnery přidal k upozornění na dlouhodobou kybernetickou kampaň vedenou ruským státem podporovaným aktérem APT28 proti logistickým a technologickým firmám zapojeným do zahraniční pomoci Ukrajině.

ZÁŘÍ

Varování před hrozbou spočívající v předávání dat a ve výkonu vzdálené správy z ČLR

V září 2025 vydal NÚKIB varování před hrozbou spočívající v předávání dat a ve výkonu vzdálené správy z ČLR. Na základě vydaného varování musí povinné osoby podle zákona o kybernetické bezpečnosti zohlednit hrozbu v analýze rizik a na zjištěná rizika reagovat přijetím přiměřených bezpečnostních opatření. Hrozba je hodnocena na úrovni „Vysoká“, tedy jako pravděpodobná až velmi pravděpodobná.

Varování bylo do značné míry přelomové. **Není zaměřené na jednu technologii, ale upozorňuje na komplexní problém a je uplatnitelné na všechna odvětví, služby i zařízení.** Varování je možné mimo jiné také zohlednit ve veřejných zakázkách a v případě nepřijatelných rizik upravit podmínky pro dodávky a dodavatele.

Jak je již zvykem, k varování byla vydána metodika, jak s ním dále pracovat.

ČERVENEC

Varování před některými produkty společnosti DeepSeek

V červenci NÚKIB vydal varování před používáním některých produktů společnosti DeepSeek. Produkty by se neměly používat na zařízeních majících přístup k systémům kritické informační infrastruktury, informačním systémům základní služby a významným informačním systémům. Obavy z možných bezpečnostních hrozeb vyplynuly především z nakládání s daty a z právního a politického prostředí ČLR, jemuž je společnost DeepSeek zcela podřízena.

SRPEN

NÚKIB se připojil ke společné analýze aktivit čínského státem podporovaného aktéra Salt Typhoon

NÚKIB se připojil ke společné analýze amerických bezpečnostních vládních agentur a dalších mezinárodních partnerů týkající se čínského státem podporovaného aktéra Salt Typhoon, který proniká do sítí po celém světě s cílem získat k nim dlouhodobý přístup a využívat je pro špionážní aktivity.

PROSINEC

NÚKIB podporuje upozornění Spojeného království na škodlivé kybernetické aktivity čínských společností I-SOON a Integrity Tech

V prosinci NÚKIB podpořil vyjádření partnerů ze Spojeného království, kteří upozornili na škodlivé aktivity čínských společností Anxun Information Technology a Beijing Integrity Technology působících v kyberprostoru. Zmíněné společnosti jsou součástí komplexního ekosystému soukromých subjektů v ČLR, které pro tamní zpravodajské a bezpečnostní složky mj. vyvíjejí ofenzivní nástroje a samy, s vědomím tamní vlády, provádějí ofenzivní kybernetické operace proti zahraničním cílům, včetně institucí v ČR.

NÚKIB se připojil k upozornění před útoky proruských hacktivistů

NÚKIB se spolu s dalšími národními partnery připojil k upozornění amerického Federálního úřadu pro vyšetřování na kybernetické útoky proruských hacktivistických skupin mířených na kritickou infrastrukturu.

NÁRODNÍ ÚROVEŇ KYBERNETICKÉ BEZPEČNOSTI

NOVÁ NÁRODNÍ STRATEGIE KYBERNETICKÉ BEZPEČNOSTI A PŘÍPRAVA AKČNÍHO PLÁNU K JEJÍMU NAPLNĚNÍ PRO OBDOBÍ 2026–2030

V září 2025 byla vládou schválena aktualizace Národní strategie kybernetické bezpečnosti (dále jen „NSKB“). Jedná se o vrcholný národní strategický dokument pro kybernetickou bezpečnost, který vytváří jednotný a koordinovaný rámec zaměřený na:

- bezpečnost a odolnost informačních a komunikačních systémů,
- kybernetickou obranu,
- kybernetickou diplomacii,
- boj s kybernetickou kriminalitou a posilování odolnosti společnosti vůči hrozbám v kyberprostoru.

Vizí NSKB je bezpečná a digitálně vyspělá ČR s odolnou infrastrukturou, vzdělanou a inovativní společností a silnými mezinárodními i domácími partnerstvími. Strategické cíle k realizaci vize staví na proaktivním přístupu k hrozbám, schopnosti reakce na rozsáhlé krize nebo rozvoji odborníků. Cíle budou naplňovány skrze konkrétní, měřitelné, dosažitelné a časově vymezené úkoly Akčního plánu, jehož přípravu i následné plnění úkolů koordinuje NÚKIB. Předložení Akčního plánu vládě je plánováno na první polovinu roku 2026.

IMPLEMENTAČNÍ PLÁN NÁRODNÍ POLITIKY KRYPTOGRAFICKÉ OCHRANY UTAJOVANÝCH INFORMACÍ

V návaznosti na schválení Národní politiky kryptografické ochrany utajovaných informací (dále jen „NP KOUI“) v závěru roku 2024 probíhala v roce 2025 práce na Implementačním plánu. Ten obsahuje konkrétní úkoly, které naplní cíle NP KOUI. Konkrétní znění úkolů je utajované, zahrnují ale tyto oblasti: řízení systému kryptografické ochrany, podpora domácích kryptografických prostředků, podpora personálních kapacit, připravenost na krize a jiné. Plánované období pro plnění úkolů je do roku 2030, s výhledem do roku 2040 u dlouhodobých rozvojových témat. Implementační plán byl v závěru roku 2025 předložen ke schválení Bezpečnostní radě státu.

KOORDINOVANÉ ZVEŘEJŇOVÁNÍ ZRANITELNOSTÍ

V roce 2025 probíhalo dokončení Národní politiky koordinovaného zveřejňování zranitelností (dále jen „CVD“) a nastavení souvisejících interních procesů NÚKIB (příjem hlášení, ověřování, komunikace s oznamovateli aj.). Z hlediska nasazení CVD v rámci NÚKIB pokračovala pilotní implementace na vybraných webových aplikacích a vyhodnocování získaných poznatků. Probíhaly i meziresortní konzultace k právně-procesnímu ukotvení tak, aby se po zveřejnění politiky dala rozšiřovat na další subjekty. Na konci roku 2025 byla CVD zveřejněna, v průběhu roku 2026 je v plánu zahájení osvěty ohledně nasazování CVD politik v organizacích v souvislosti s provázáním s osvětou a metodickou podporou.

PROJEKT KYBERLIGA

Projekt Kyberliga cílí na vytvoření komunity dobrovolníků složené z expertů a expertek na kybernetickou bezpečnost, která bude fungovat pod záštitou a ve spolupráci s NÚKIB. Hlavním cílem je podpora kybernetické bezpečnosti ČR a poskytování platformy pro bezpečnou, důvěryhodnou a aktivní komunitu, která bude sdílet nejlepší praxi, budovat know how a podporovat růst a rozvoj na osobní i systémové úrovni. V roce 2025 pokračovalo konceptuální rozpracování tohoto projektu (nastavení pravidel, procesů a konzultace s možnými členy). V průběhu podzimu pak došlo ke spuštění pilotního provozu v menším rozsahu členů s důrazem na ověření praktického fungování. Záměr je během roku 2026 Kyberligu postupně spustit do plného provozu.

NÁRODNÍ LEGISLATIVNÍ RÁMEC

Zákon č. 264/2025 Sb., o kybernetické bezpečnosti

Zákon byl Poslaneckou sněmovnou ve 3. čtení schválen 25. dubna 2025. Přítomno bylo 165 poslanců, z toho pro návrh bylo 159 a proti návrhu 0. Zákon v Poslanecké sněmovně strávil celkem 9 měsíců (od 25. července 2024 do 13. května 2025).

Následně byl návrh zákona postoupen Senátu, který jej schválil 66 hlasy pro, 1 proti.

Zákon č. 264/2025 Sb., o kybernetické bezpečnosti, je od 1. listopadu 2025 účinný, čímž se uzavřela téměř čtyřletá příprava tohoto klíčového předpisu. Konkrétně trvala 3 roky, 8 měsíců a 9 dní.

Od listopadu 2025 započala implementace ZKB. V roce 2025 šlo primárně o samoidentifikaci povinných osob, jejich registraci a přípravy na zavádění bezpečnostních opatření u těchto osob. Komplikaci pro NÚKIB při uvádění zákona v život představuje neschválení novely správního řádu, čímž nebylo umožněno automatizované podepisování rozhodnutí, tedy pečetění, což přineslo zvýšenou potřebu kapacit pro přípravu nových systémů a zavedení automatizace jiným způsobem. Povinných osob je očekáváno přes 6000 a v každém jednotlivém případě bude nutno vydat rozhodnutí o registraci. Manuální podepisování každého rozhodnutí oprávněnou osobou by tak bez technického řešení mohlo trvat řádově i roky.

V souvislosti se ZKB byla vytvořena a předložena dvě nařízení vlády provádějící tzv. mechanismus prověřování bezpečnosti dodavatelského řetězce. Tento nový institut má státu poskytnout strategickou kontrolu nad dodavatelským řetězcem nejkritičtějších, tzv. strategicky významných služeb. V rámci projednávání obou nařízení v meziresortním připomínkovém řízení vyvstaly rozpory, které doposud nebyly (i přes veškeré snahy NÚKIB) vypořádány a návrhy nařízení tak zůstávají v meziresortním připomínkovém řízení.

Bez těchto nařízení mechanismus prověřování bezpečnosti dodavatelského řetězce, který je v ZKB obsažen, nefunguje, neboť nejsou stanoveny povinné osoby, které se jím mají řídit. Těmito projednávanými návrhy nařízení jsou:

- návrh nařízení vlády o nepominutelných funkcích stanoveného rozsahu a
- návrh nařízení vlády o regulovaných službách, které splňují podmínky strategicky významné služby, a o částech strategicky významných služeb tvořících nezbytný rozsah zajištění dostupnosti strategicky významných služeb (nařízení o strategicky významných službách).

Rok 2025 se nesl také ve znamení osvěty ohledně ZKB. Pracovníci Odboru regulace vystoupili na více než 80 veřejných konferencích, workshopech či obdobných akcích pro veřejnost. Byly rozeslány informační letáky na cca 35 podnikatelských svazů, sdružení a komor.

V souvislosti se snahou o hladkou implementaci ZKB byly vytvořeny videonávody, resp. videopřednášky, které pokrývají požadavky ZKB a jednotlivých povinností a bezpečnostních opatření i orientaci na Portálu NÚKIB. Tyto návody jsou publikovány na Portálu NÚKIB a na YouTube kanále NÚKIB, kde mají několik tisíc zhlédnutí.

REGULACE CLOUD COMPUTINGU VYUŽÍVANÉHO INFORMAČNÍMI SYSTÉMY VEŘEJNÉ SPRÁVY

V roce 2025 bylo posouzeno 41 poskytovatelů a 12 nabídek služeb.
Za celou dobu posuzování bylo posouzeno 187 poskytovatelů a 32 nabídek služeb.

Průběh posuzování je komplexní proces. Ačkoliv bylo v roce 2025 nově zapsáno do katalogu cloud computingu 12 nabídek, NÚKIB musel provést 63 samostatných posouzení. Zároveň došlo ke kompletní revizi prováděcích předpisů k této oblasti a v řadě oblastí byly podstatně zjednodušeny tak, aby byla v maximální možné míře odstraněna administrativní zátěž a zvýšil se uživatelský komfort adresátů norem.

ZÁKON O ODOLNOSTI SUBJEKTŮ KRITICKÉ INFRASTRUKTURY

Další podstatnou legislativou s přesahem do kybernetické bezpečnosti a fungování NÚKIB je zákon č. 266/2025 Sb., o odolnosti subjektů kritické infrastruktury a o změně souvisejících zákonů (zákon o kritické infrastruktuře). Tento zákon vstoupil v účinnost v roce 2025. NÚKIB se vedle konzultací v době přípravy tohoto zákona věnoval konstrukci části prováděcího nařízení vlády, které definuje kritéria pro povinné osoby v oblasti digitálních služeb. V budoucnu bude také z pozice garanta části odvětví digitální infrastruktury potvrzovat registrace subjektů kritické infrastruktury v tomto odvětví.

AKT O KYBERNETICKÉ BEZPEČNOSTI A JEHO REVIZE

Akt o kybernetické bezpečnosti (Cyber Security Act, dále jen „CSA“) zavádí dobrovolný systém certifikace kybernetické bezpečnosti pro produkty, služby a procesy informačních a komunikačních technologií (dále jen „ICT“) a pro řízené bezpečnostní služby. Díky jednotnému evropskému certifikačnímu rámci mohou výrobci prokazovat úroveň zabezpečení svých produktů způsobem, který je uznáván po celé EU, a posílit tak důvěru zákazníků i svých obchodních partnerů. Certifikace podle CSA je tak především nástrojem pro zlepšení reputace a transparentnosti. Nařízení je platné od roku 2019 a první certifikáty v rámci Evropského systému certifikace kybernetické bezpečnosti (dále jen „EUCC“) lze vystavovat od února roku 2025. V současné době probíhá na evropské úrovni revize tohoto nařízení, která byla představena v lednu 2026. NÚKIB se aktivně zapojoval v zasílání vlastních i společných vstupů k revizi CSA.

V rámci této agendy se NÚKIB připravoval na její zajišťování, zejména byla přijata interní směrnice obsahující veškeré klíčové postupy vnitrostátního orgánu certifikace kybernetické bezpečnosti, konzultoval s Českým institutem pro akreditaci zavedení služby akreditace podle EUCC (skrze schválení odborníků pro posuzování, revize interní dokumentace atd.) a dále zahájil komplexní přípravu na proces peer review (vzájemné hodnocení plnění požadavků Evropskou komisí a ostatními členskými státy plánované na říjen 2026).

AKT O KYBERNETICKÉ ODOLNOSTI

Akt o kybernetické odolnosti (Cyber Resilience Act, dále jen „CRA“) je horizontální legislativou stanovující požadavky na kybernetickou bezpečnost pro všechny produkty s digitálními prvky uváděné na trh EU. Cílem je zajistit bezpečnost po celou dobu životního cyklu produktu – od návrhu přes výrobu až po aktualizace. CRA ukládá výrobcům povinnost aktivně řídit zranitelnosti, hlásit incidenty a absolvovat proces posouzení shody.

V listopadu 2025 byl vyjednán a schválen důležitý implementační akt, který specifikuje technické definice významných a kritických produktů pod CRA, kde se NÚKIB do vyjednávání aktivně zapojoval.

Informace k oběma nařízením vč. podpůrných materiálů **je dostupná na Portálu NÚKIB.**

UNIJNÍ KRIZOVÉ ŘÍZENÍ

V červnu 2025 Rada EU přijala nový rámec pro kybernetické krizové řízení ve formě doporučení Rady o plánu EU pro řešení kybernetických bezpečnostních krizí – tzv. Cyber Blueprint, který aktualizuje a nahrazuje původní doporučení Komise z roku 2017. Cyber Blueprint stanovuje rámec pro koordinovanou reakci EU na kybernetické incidenty velkého rozsahu, včetně jasného rozdělení rolí relevantních kyberbezpečnostních aktérů na unijní úrovni, koordinace s dalšími unijními mechanismy krizového řízení a spolupráce s NATO.

SIMPLIFIKAČNÍ BALÍČEK

V listopadu 2025 zveřejnila Evropská komise tzv. digitální simplifikační balíček, který obsahuje legislativní i nelegislativní iniciativy v oblasti datových pravidel, ochrany osobních údajů a kybernetické bezpečnosti. Součástí balíčku je Digitální omnibus, který mj. navrhuje zřízení jednotného rozhraní pro oznamování incidentů – tzv. Single-Entry Point. NÚKIB se do projednávání materiálu od počátku aktivně zapojuje.

NETWORK CODE

Network Code je soubor technických pravidel, která harmonizují kybernetickou bezpečnost při provozu a řízení přeshraničních energetických sítí v EU s cílem nastavit společné minimální požadavky, plánování, monitorování, podávání zpráv a řízení krizí skrze závazné požadavky pro operátory soustav, výrobce i další účastníky trhu. Tato norma zavádí závazné kybernetické požadavky včetně řízení rizik a reakce na incidenty. V rámci této agendy se NÚKIB věnoval přípravě na implementaci a spolupráci s ostatními příslušnými orgány za účelem hladké implementace požadavků.

DIGITAL OPERATIONAL RESILIENCE ACT

Digital Operational Resilience (dále jen „DORA“) je nařízení EU, které zavádí jednotný rámec pro digitální provozní odolnost ve finančním sektoru s cílem posílit kybernetickou bezpečnost a schopnost finančních institucí (banky, pojišťovny, investiční společnosti, poskytovatelé kryptoaktiv atd.) odolávat kybernetickým útokům, efektivně na ně reagovat a rychle se zotavit. Stanovuje pravidla pro řízení rizik ICT, hlášení incidentů, testování odolnosti a dohled nad kritickými třetími stranami (dodavateli služeb informačních technologií). Jelikož některé subjekty spadající pod DORA spadají také pod ZKB, byla nutná koordinace a vyjasnění ohledně implementace obou předpisů s Českou národní bankou, která dohlíží právě na DORA.

DOZOROVÁ ČINNOST

V průběhu roku 2025 uskutečnil NÚKIB celkem 22 kontrol a auditů prováděných podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti, a jeho prováděcí vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, ve znění pozdějších předpisů.

Vedle vlastní kontrolní činnosti se i nadále zaměřoval na poskytování metodické podpory povinným osobám, která spočívala zejména v průběžném zodpovídání odborných dotazů, přípravě a publikaci podpůrných materiálů a realizaci auditů u vybraných subjektů.

V návaznosti na aktualizaci právních předpisů NÚKIB současně postupně vydává soubor metodických materiálů určených povinným subjektům. Cílem je usnadnit výklad nových a upravených povinností, sjednotit aplikační praxi a poskytnout praktickou podporu při zavádění požadovaných bezpečnostních opatření.

SPOLUPRÁCE NÚKIB S DALŠÍMI DOZOROVÝMI ORGÁNY V OBLASTI KONTROLY V ROCE 2025

V roce 2025 pokračovalo posilování spolupráce NÚKIB s ostatními dozorovými orgány. NÚKIB se zapojil do kontrolní činnosti Státního úřadu pro jadernou bezpečnost v roli přizvané osoby. Současně proběhla jednání se zástupci České národní banky, jejichž předmětem bylo vymezení dalšího postupu vzájemné spolupráce v souvislosti s dopady nové regulace na bankovní sektor i oblast kybernetické bezpečnosti.

NEJVÝZNAMNĚJŠÍ NEDOSTATKY ZJIŠTĚNÉ BĚHEM KONTROL V ROCE 2025

Systém řízení bezpečnosti informací nezahrnuje všechna aktiva, která jsou z hlediska kybernetické bezpečnosti relevantní.	Analýza rizik není prováděna dostatečně systematicky a ani v požadovaném rozsahu.	Procesy řízení dodavatelů v oblasti kybernetické bezpečnosti vykazují významné nedostatky.
Oblast řízení kontinuity činností není řešena odpovídajícím způsobem, případně je zcela opomíjena, což vede k nepřipravenosti organizací na zvládání dopadů kybernetických bezpečnostních incidentů.	Nejsou uplatňovány mechanismy vícefaktorové autentizace a současně nejsou nastavena dostatečně silná autentizační hesla.	Opatření na ochranu proti škodlivému kódu a schopnosti detekce kybernetických bezpečnostních událostí v interních sítích nejsou dostatečné.
Jsou provozována technická zařízení, která již nejsou výrobcem podporována a představují zvýšené bezpečnostní riziko.	Využívané kryptografické prostředky neodpovídají současným požadavkům na úroveň kryptografické odolnosti.	Zálohy nejsou v dostatečné míře testovány ani odpovídajícím způsobem chráněny.

CVIČENÍ KYBERNETICKÉ BEZPEČNOSTI

V roce 2025 se NÚKIB v oblasti cvičení zaměřil na koncepční činnost, která souvisela s přípravou a tvorbou dokumentu Národní koncepce cvičení kybernetické bezpečnosti. **Vizí dokumentu je vybudovat robustní, flexibilní a dlouhodobě udržitelný systém cvičení reagující na aktuální i budoucí výzvy v oblasti kybernetické bezpečnosti.** Tato vize bude naplňována prostřednictvím dvou pilířů – budování schopností a kapacit pro realizaci cvičení a systematizace a prohlubování spolupráce u cvičení.

Také v roce 2025 proběhla cvičení s mezinárodním přesahem, mezi něž již tradičně patří cvičení Locked Shields pořádané NATO Cooperative Cyber Defence Centre of Excellence v estonském Tallinnu, které se konalo v květnu. V prosinci pak proběhlo mezinárodní cvičení kybernetické bezpečnosti Cyber Coalition pořádané také pod hlavičkou NATO. NÚKIB se dále zapojil do aliančního cvičení orgánů krizového řízení. Pro spojence NÚKIB připravil a uspořádal cvičení zaměřené na schopnost podpory při kybernetických incidentech na dálku (VCISC – Virtual Cyber Incident Support Capability). Cílem bylo prověřit připravenost spojenců poskytovat si vzájemnou pomoc prostřednictvím mechanismu VCISC v případě vážných kybernetických incidentů.

PREVENCE, OSVĚTA A VZDĚLÁVÁNÍ

V průběhu roku 2025 byla připravena nová NSKB a návrh akčního plánu, kde byla zohledněna témata osvěty, vzdělávání a prevence pro roky 2026–2030. Klíčovou změnou oproti předchozímu období je požadavek na výrazně širší zapojení organizací veřejné sféry do realizace preventivních a vzdělávacích aktivit, včetně podpory regionálních iniciativ, školních programů a cílených kampaní pro různé skupiny obyvatel.

Vzdělávací portál NÚKIB nabízí osvětové kurzy pro školy, zdravotnictví, úřady i širokou veřejnost. Je autorem a garantem kurzu zaměřeného na základy kyberbezpečnosti Dávej kyber a kurzu pro managery kybernetické bezpečnosti Šéfuj kyber.

V minulém roce se NÚKIB připojil k informování veřejnosti před podvodnými telefony, ve kterých se neznámý útočník vydával za pracovníka důvěryhodné instituce a pod záminkou blokace účtu (a nutnosti převodu peněz na rezervní účet se snažil z lidí vylákat finanční prostředky.

MEZINÁRODNÍ SPOLUPRÁCE

SPOLUPRÁCE V RÁMCI NATO

Během roku 2025 NÚKIB inicioval a řídil jednání národních stakeholderů věnující se přípravě na implementaci NATO Integrated Cyber Defence Centre, jehož vznik byl oznámen v roce 2024. NÚKIB byl dále zapojen do interního hodnocení fungovaní NATO v oblasti kybernetické bezpečnosti a obrany.

NOVÉ STRATEGICKÉ VAZBY

V březnu 2025 došlo v rámci Prague Cyber Security Conference 2025 (dále jen „PCSC“) k podpisu memoranda o spolupráci mezi NÚKIB a ukrajinským State Service of Special Communications and Information Protection of Ukraine, jehož obsahem je zejména spolupráce na výměně informací a sdílení zkušeností a dobré praxe mj. v oblasti řešení incidentů, analýzy hrozeb a zvyšování úrovně kybernetické bezpečnosti kritické infrastruktury. **V návaznosti na toto memorandum NÚKIB uspořádal workshop, kde spolu s dalšími zahraničními partnery sdílel své zkušenosti z oblasti implementace požadavků směrnice NIS 2, unijní spolupráce v oblasti zvládání kybernetických bezpečnostních incidentů nebo řízení kybernetických krizí.**

V květnu se NÚKIB připojil k několika australským technickým dokumentům zaměřeným na základy moderní obranyschopné infrastruktury, bezpečnost hraničních síťových prvků nebo využívání platforem Security Information and Event Management (SIEM) a Security Orchestration, Automation, and Response (SOAR).

V září se NÚKIB připojil k dokumentu *A Shared Vision of Software Bill of Materials (SBOM) for Cybersecurity*, který vydala americká Agentura pro kybernetickou a infrastrukturní bezpečnost s Národní bezpečnostní agenturou spolu s dalšími mezinárodními partnery. Dokument má za cíl motivovat k širšímu využívání tohoto nástroje v praxi.

VZTAHY S USA

Rok 2025 se nesl především ve znamení nástupu nové americké administrativy a očekávání ohledně pokračování blízké spolupráce s USA a s evropskými partnery. Delegace NÚKIB absolvovala sérii jednání se zástupci amerických bezpečnostních institucí, včetně Národní bezpečnostní rady Bílého domu a Zvláštní komise pro strategické soupeření mezi USA a ČLR při Sněmovně reprezentantů, na kterých si obě strany potvrdily vůli i nadále úzce spolupracovat a vyměňovat si zkušenosti i informace na poli čelení kybernetickým hrozbám. Zástupci NÚKIB se účastnili *RSA* Conference, nejvýznamnější kyberbezpečnostní konference na světě, stejně jako po boku špiček americké administrativy a mezinárodních partnerů vystoupili na International Cyber Security Forum. Dobré vztahy obou zemí stvrdilo i jednání delegace českého Ministerstva zahraničních věcí v USA ke konci roku.

ROZVOJOVÁ SPOLUPRÁCE A BUDOVÁNÍ KYBERNETICKÝCH KAPACIT

NÚKIB se v roce 2025 zapojil do mnoha rozvojových projektů a sdílel své zkušenosti zejména s partnery v regionu západního Balkánu a Indo-Pacifiku, ale menší měrou také v Africe nebo Asii. **Západní Balkán však i nadále zůstává prioritním regionem pro směřování rozvojové pomoci.** Na rozvojových aktivitách NÚKIB i nadále spolupracuje s mezinárodními organizacemi (zejména NATO a EU) a klíčovými státy s obdobnými postoji, včetně Spojených států amerických (dále jen „USA“) a Estonska. Současně se však aktivně podílí na rozvojových projektech CyberVAC Ministerstva zahraničních věcí, v roce 2025 šlo především o projekty v Jordánsku a Bhútánu.

SPOLUPRÁCE V RÁMCI EU

ENISA SUPPORT ACTION

Pokračovaly aktivity v rámci projektu podpůrných služeb (ENISA Support Action), díky kterým byly vybraným subjektům poskytovány bezplatné služby penetračního testování, kybernetických cvičení a pomoci při analýze rizik.

SUPPLY CHAIN TOOLBOX

V rámci Skupiny pro spolupráci zřízené směrnicí NIS 2 byly dokončeny práce na souboru opatření pro zvýšení bezpečnosti dodavatelského řetězce ICT (tzv. ICT Supply Chain Security Toolbox). Toolbox byl zveřejněn 13. února 2026, společně se dvěma koordinovanými posouzeními rizik na unijní úrovni (připojená a autonomní vozidla a detekční vybavení), která využívají jeho strukturu.

KONFERENCE

PRAGUE CYBER SECURITY CONFERENCE 2025

V roce 2025 NÚKIB pořádal již šestý ročník mezinárodní PCSC, který opět propojil vládní představitele, odborníky i zástupce soukromého sektoru z desítek zemí světa. Hlavními tématy pod hlavičkou „Invisible frontlines“ byly neviditelné fronty kybernetických konfliktů, posilování odolnosti kritické infrastruktury, ochrana energetických a telekomunikačních sítí, dopady umělé inteligence (dále jen „AI“) a význam mezinárodní spolupráce v boji s kybernetickými hrozbami.

KONFERENCE CYBER_CON 2025

Jedenáctý ročník konference CYBER_CON 2025, kterou uspořádal NÚKIB ve spolupráci s partnery CZ.NIC, NIX.CZ, CESNET a dalšími, přilákal do prostor brněnského Výstaviště téměř 800 účastníků. Ve dnech 17. a 18. září 2025 se setkali techničtí a právní specialisté, akademici, manažeři i studenti, aby diskutovali o aktuálních výzvách a příležitostech v oblasti kybernetické bezpečnosti. Program konference byl postaven kolem NSKB a ZKB.

KONFERENCE EVROPSKÝCH CERTIFIKACÍ

NÚKIB 26. listopadu 2025 uspořádal druhý ročník Konference evropských certifikací. Tato událost se letos zaměřila na nadcházející legislativní změny, které zásadně ovlivní výrobce v celé EU. Hlavním tématem konference byl CSA, ovšem byly zde předneseny i novinky z oblasti CRA. Účastníci konference měli možnost prodiskutovat očekávané dopady CRA, procesy posuzování shody a dalších aspektů uvádění produktů s digitálním prvkem na vnitřní trh EU. Na konferenci bylo registrováno 112 účastníků a na místo dorazilo 71 z nich.

ČINNOST VLÁDNÍHO CERT

V roce 2025 Vládní CERT kromě běžné forenzní práce pokračoval v rozvoji aktivní pomoci zasaženým subjektům přímo na místě, a to během řešení následků kyberbezpečnostních incidentů přímo v jejich infrastruktuře. Dále byly tyto schopnosti uplatněny v proaktivní službě síťového threat huntingu. Ten je taktéž plánován dále rozvíjet a kombinovat s dalšími proaktivními přístupy pro zlepšení kybernetické odolnosti povinných subjektů.

PORTÁL NÚKIB

V průběhu let 2024 a 2025 probíhal intenzivní vývoj Portálu NÚKIB. Ten se stal od 1. listopadu 2025 klíčovým nástrojem pro implementaci ZKB a směrnice NIS 2 a představuje jednotné místo pro plnění zákonných povinností regulovaných subjektů vůči NÚKIB. Zároveň lze prostřednictvím Portálu hlásit kybernetické incidenty a bezpečně sdílet informace o zranitelnostech a hrozbách. Ve veřejné části Portálu pak mohou organizace nalézt metodiky, návody a podpůrné materiály potřebné k plnění nových povinností.

Portál byl navržen tak, aby významně přispěl ke snížení administrativní zátěže jak na straně NÚKIB, tak na straně regulovaných subjektů. **V listopadu 2025 získal 2. místo v celostátní kategorii v soutěži Egovernment The Best 2025.** Tato soutěž každoročně oceňuje nejúspěšnější projekty digitalizace veřejné správy v ČR. Za celý rok 2025 navštívilo Portál více než 252 tisíc návštěvníků.

AKTIVNÍ SLEDOVÁNÍ ZRANITELNOSTÍ

Nově byla zahájena služba aktivního sledování zranitelností, kde se denně průměrně řeší přibližně 20 zranitelností. Průběžně jsou na síť X umisťována upozornění, přičemž měsíčně jich je okolo dvou desítek. U zranitelností s vysokým dopadem na ČR byla pak upozornění vydávána přímo na Portálu NÚKIB a u cílených dopadů byli cíleně informováni konstituenti. V roce 2025 bylo vydáno přes 140 takových upozornění.

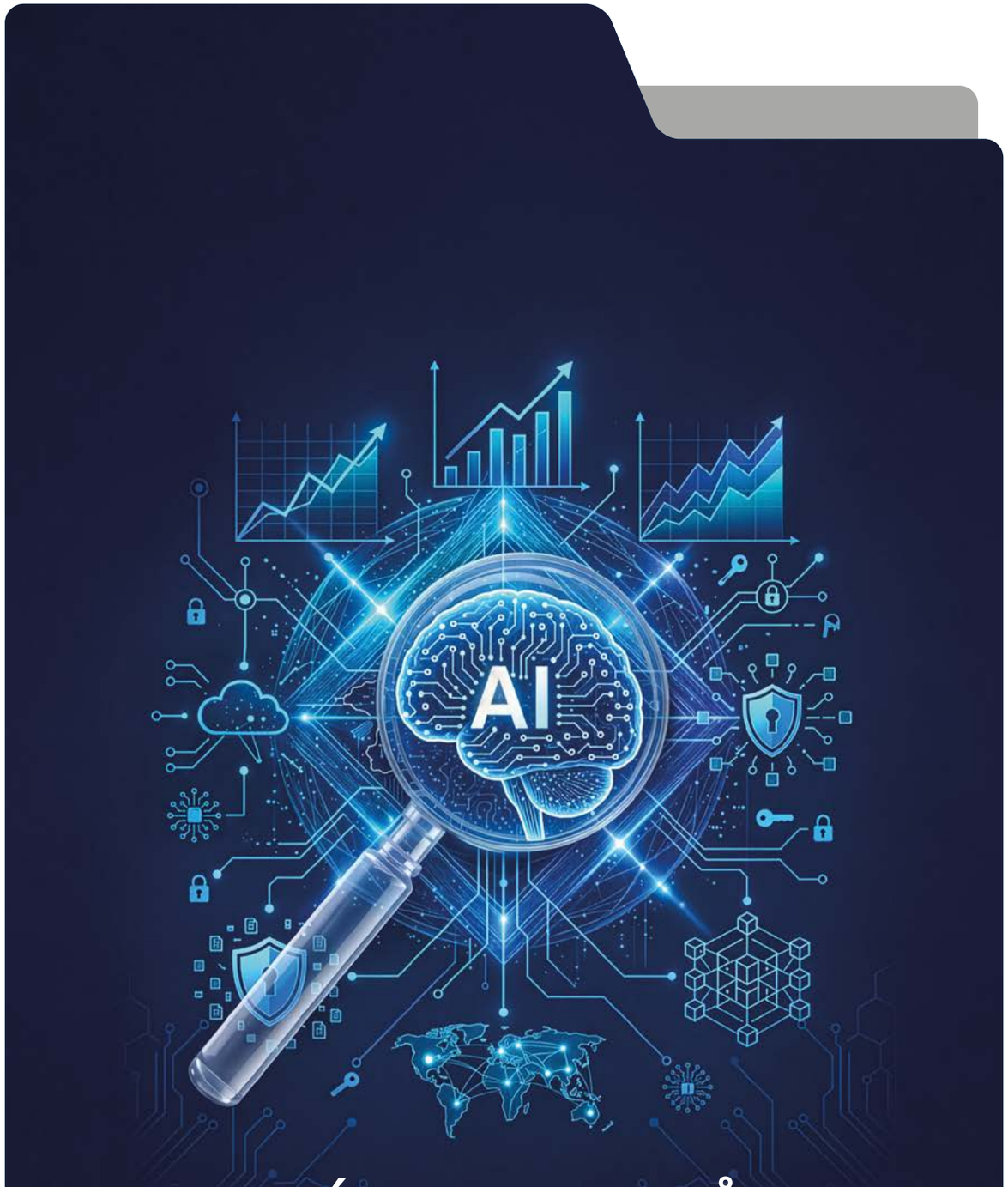
PENETRAČNÍ TESTOVÁNÍ

Celkem bylo otestováno 10 subjektů. Oproti předchozím rokům došlo k nárůstu poptávky po komplexních penetračních testech, které zahrnují fyzické testování, wi-fi infrastrukturu a phishingové kampaně. Ve srovnání s předchozím rokem se počet realizovaných penetračních testů zvýšil z 23 na 36, což představuje meziroční nárůst o přibližně 56 %.

V roce 2025 byla vytvořena pokročilá phishingová infrastruktura „Phishing 2.0“ umožňující obcházení dvoufaktorové autentizace. Současně probíhal proces výběru a nákupu nového skeneru zranitelností, který bude v souladu se ZKB umožňovat automatizované skeny většího počtu subjektů.

Pravidelně probíhá konzultace a testování nástroje PENTEREP ve spolupráci s VUT.

Za účelem dalšího rozvoje odborných schopností byla nasazena laboratorní infrastruktura GOAD, sloužící ke zvyšování praktických znalostí týmu a případně i ostatních týmů CERT.



VÝHLED TRENDŮ V KYBERNETICKÉ BEZPEČNOSTI V ČR NA ROKY 2026 A 2027

VÝHLED TRENDŮ V KYBERNETICKÉ BEZPEČNOSTI V ČR NA ROKY 2026 A 2027

HROZBA ZNEUŽITÍ KOMUNIKAČNÍCH PLATFOREM PRO ŠÍŘENÍ ŠKODLIVÉHO OBSAHU A KYBERŠPIONÁŽ

V průběhu roku 2025 bylo v Evropě zaznamenáno několik spear-phishingových kampaní, k jejichž realizaci byla zneužita komunikační platforma Signal, skrze níž byl šířen špionážní malware. Komunikace skrze Signal je díky integrovanému šifrování obecně považována za bezpečnou, nicméně nezaručuje autenticitu účastníků konverzace. Je nicméně populární i mezi novináři či pracovníky státních institucí, což vytváří potenciál pro zisk relevantních citlivých informací. V ČR sice nebyly v uplynulém roce obdobné útoky zaznamenány, nelze však vyloučit (25–50 %), že k nim v budoucnu dojde.

Část zaznamenaných útoků mířila na příslušníky ozbrojených sil Ukrajiny, přičemž za významnou částí těchto incidentů stáli na Rusko napojení či ruští státem sponzorovaní aktéři. Několik z těchto útoků pak bylo ukrajinským CERT a soukromými kyberbezpečnostními společnostmi přímo přisouzeno ruskému aktéru APT28. Lze konstatovat, že v uplynulém roce šlo o jeden z hojně využívaných modu operandi této skupiny.

Tento typ útoků se netýká pouze platformy Signal, v uplynulém roce byly zaznamenány obdobné případy kampaní např. i na platformě WhatsApp, ovšem z výše zmíněných důvodů představuje cílení skrze Signal specifickou hrozbu pro národní bezpečnost.
Na šíření špionážního malwaru skrze komunikační platformy v druhé polovině roku 2025 upozorňovala i americká Agentura pro kybernetickou a infrastrukturní bezpečnost.

AI: STABILIZUJÍCÍ SE TECHNOLOGIE S TĚŽKO UDRŽITELNÝM FINANCOVÁNÍM

V roce 2025 představovala AI stabilní technologii, u které se začaly projevovat známky stagnace. Uvedení páté verze ChatGPT nepřineslo dramatické zlepšení schopností služby tak jako u předchozích verzí a ani konkurenční služby nepřišly s výrazným posunem, který by nastavil nový standard v odvětví. Soupeření mezi Západem a ČLR na poli AI se nadále projevovalo na geopolitické úrovni, ale méně se již propsalo do přímé konkurence například na západních tržištích pro mobilní aplikace, kde po krátkém období zájmu o čínské AI modely opět dominovaly západní aplikace a čínské služby se spíše zaměřily na domácí trh.

Rok 2026 může ovšem přinést na poli AI zásadní zlomy. **Současná AI na bázi velkých jazykových modelů** (dále jen „LLM“) **ani po čtyřech letech od svého komerčního uvedení není zisková.** AI vyžaduje energeticky náročné výpočty na pokročilém hardwaru a její provoz není v současných podmínkách rentabilní. CEO OpenAI Sam Altman přiznal, že společnost finančně tratí na každém uživateli, včetně těch, kteří si platí nejvyšší prémiové předplatné v ceně více než 4 000 Kč měsíčně. Společnosti vyvíjející a provozující AI tyto ztráty kompenzují buď jinými zdroji příjmů, nebo z peněz investorů.

V současnosti ovšem lze pozorovat varovné signály, že další investice do AI sektoru mohou narazit, právě kvůli dnešní neziskovosti a absenci jasného plánu budoucí efektivní monetizace. Nynější přísun investic navíc kromě potenciální budoucí ziskovosti do značné míry stojí i na příslibu dalších průlomů na poli AI, vedoucích až k vývoji všeobecné umělé inteligence AGI, která dokáže překonat člověka. V současné době ovšem můžeme pozorovat nárust skepticismu, zda AI na bázi LLM může vůbec zmíněného stavu dosáhnout.

V roce 2026 je proto pravděpodobný (55–70 %) scénář, kdy dojde k poklesu investic. Klíčová je především situace kolem společnosti OpenAI, jakožto lídra a průkopníka současných AI služeb, který je ovšem většinově závislý na investorech. OpenAI se již dnes nachází ve finančních problémech, které řeší např. limitací portfolia služeb, jako zrušení generátoru videí Sora, nebo vkládáním reklam do služby ChatGPT. Je pravděpodobné (55–70 %), že během následujících let se tato situace bude dále zhoršovat a může dojít až ke krachu společnosti. Krach OpenAI by měl velmi pravděpodobně (75–85 %) dominový efekt na zbytek AI sektoru a podkopal by důvěru v budoucnost celého AI odvětví.[1] **Odliv peněz investorů by mohl znamenat výrazné omezení nebo zdražení současných AI služeb. Situace by následně mohla vést k posílení pozic čínských AI služeb, jako MinMax nebo DeepSeek.** Ačkoliv ty téměř jistě (90–100 %) taky operují se ztrátou, jejich investiční zdroje jsou odlišné a navázané na čínský režim. Ten proto může pokračovat v jejich financování, právě i s cílem vyplnit prostor po západních modelech.

České společnosti proto mohou být pravděpodobně (55–70 %) v následujících dvou letech ohroženy buďto výpadkem, zhoršením kvalit nebo citelným zdražením západních AI modelů. Následně mohou být pod tlakem nuceni přejít na modely čínské provenience, s riziky, které se s nimi pojí (např. zpracování a ukládaní dat v ČLR s rizikem průmyslové špionáže). Lze proto doporučit, aby firmy adoptovaly AI technologie střídmě, se schopností obnovit původní procesy.

1 Ačkoliv společnosti jako Meta nebo Google disponují vlastními zdroji příjmů (především z reklam), jsou obchodovány na burze a cena jejich akcií by byla zřejmě v důsledku výrazně oslabena.

PŘÍLOHA 1: VYHODNOCENÍ PLNĚNÍ CÍLŮ NÁRODNÍHO PLÁNU VÝZKUMU A VÝVOJE V KYBERNETICKÉ A INFORMAČNÍ BEZPEČNOSTI ZA ROK 2025

BUDOVÁNÍ NÁRODNÍHO KOORDINAČNÍHO CENTRA

V roce 2025 NÚKIB pokračoval v poskytování služeb Národního koordinačního centra podle nařízení Evropského parlamentu a Rady č. 2021/887. V této souvislosti NÚKIB uspořádal několik webinářů a školení, které se věnovaly aktuálním výzvám programu Digitální Evropa, službám Národního koordinačního centra či způsobu registrace do Komunity kompetencí podle ZKB.

NÚKIB nadále pokračoval v budování informačního zázemí, poradenství v oblasti čerpání finančních prostředků z rámcových programů EU a šíření výsledků výzkumu a vývoje v rámci ČR. Posilování vazeb mezi akademickým, soukromým a veřejným sektorem probíhalo především prostřednictvím pravidelných setkání Skupiny kyberbezpečnostního výzkumu a inovací CYRIS, která sdružuje přibližně 150 členů komunity výzkumu a vývoje. NÚKIB také zpracovává pravidelný newsletter zaměřený na aktuality ve výzkumu a vývoji v kybernetické bezpečnosti.

V rámci nástroje PROPED pro podporu ekonomické a vědecké diplomacie NÚKIB realizoval tři zahraniční vědecké mise s cílem prohloubit spolupráci v oblastech kybernetické bezpečnosti, kryptografické ochrany a vesmírných technologií.

PODPORA VÝZKUMNÝCH A VÝVOJOVÝCH PROJEKTŮ

Z pozice aplikačního garanta NÚKIB podpořil více než dvacet výzkumných a vývojových projektů financovaných z programů veřejných soutěží (například Technologická agentura ČR či bezpečnostní výzkum Ministerstva vnitra) s cílem zvýšit uplatnitelnost výsledků výzkumu a vývoje v praxi. NÚKIB se rovněž zapojil do mezinárodních řešitelských konsorcií – příkladem je projekt QARC podpořený z programu Horizont Evropa, jehož cílem je posílit přechod na kvantově bezpečnou kryptografii v úzké spolupráci akademické obce, podniků a veřejného sektoru.

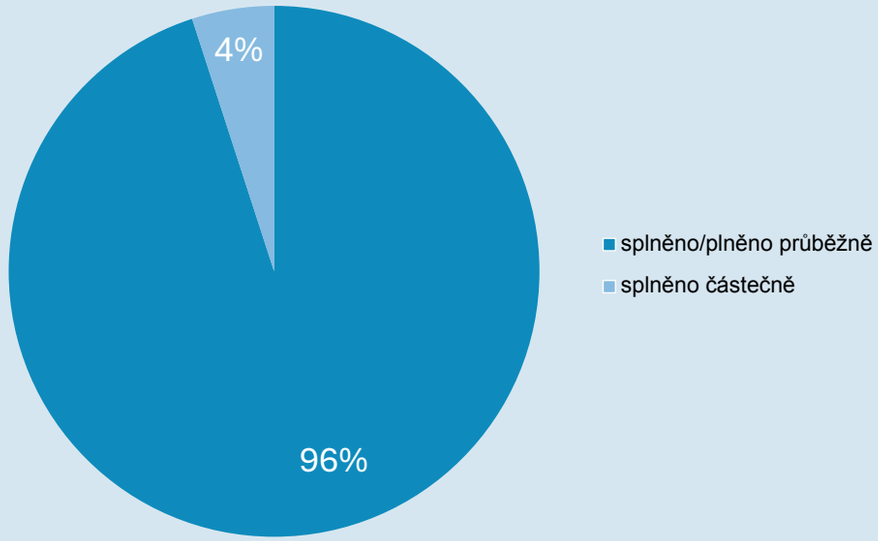
AKTIVITY NA ÚROVNI EU

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

PŘÍLOHA 2: NAPLŇOVÁNÍ AKČNÍHO PLÁNU K NÁRODNÍ STRATEGII KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY NA OBDOBÍ LET 2021 AŽ 2025

V roce 2025 bylo popáté vyhodnocováno plnění Akčního plánu k Národní strategii kybernetické bezpečnosti pro období let 2021–2025 (dále jen „Akční plán“). S ohledem na příchod nové NSKB a konec platnosti Akčního plánu se zároveň jedná o jeho poslední vyhodnocení.

Celkově bylo za rok 2025 předmětem vyhodnocení 83 úkolů. Z tohoto počtu byly 3 úkoly splněny pouze částečně, všechny ostatní úkoly byly vyhodnoceny jako splněné či plněné průběžně. Úspěšnost plnění úkolů tedy byla 96 % a jedná se o nejvyšší úspěšnost plnění za celé strategické období 2021 až 2025.



Pouze částečně splněny byly zejména komplexní úkoly, jejichž plnění je závislé na vnějších okolnostech mimo vůli jejich gestorů a často jsou opakovaně přenášeny do následujících let. Příkladem je úkol číslo 13: „Vytvořit metodiku pro strategickou komunikaci relevantních subjektů na národní úrovni pro případ reakce na kybernetické incidenty, útoky a jiné hrozby“, jehož původní termín splnění byl v roce 2022, ale dosud nebyl dokončen z důvodu nedostupných kapacit gestorů.

Přes dlouhodobě vysokou míru úspěšnosti plnění se malý podíl nedostatečně splněných úkolů objevil dosud v každém roce vyhodnocování Akčního plánu. Kromě uvedených kapacitních omezení je častým důvodem nedostatečného plnění také reprioritizace gestorovi svěřených agend. Zkušenosti z neúspěšně plněných úkolů jsou reflektovány při přípravě nového Akčního plánu na období 2026–2030, jehož úkoly rovněž navážou na některé nedokončené úkoly z předchozího období.

PŘÍLOHA 3: PROVÁDĚCÍ PŘEDPISY K NOVÉMU ZÁKONU O KYBERNETICKÉ BEZPEČNOSTI

Zákon je prováděn celkem 10 prováděcími předpisy, z čehož je 7 vyhlášek, 2 nařízení vlády a 1 prováděcí nařízení Evropské komise. Kromě nařízení vlády byly již všechny tyto prováděcí předpisy v roce 2025 přijaty. Konkrétně jde o:

- vyhlášku č. 408/2025 Sb., o regulovaných službách, která definuje identifikační kritéria pro povinné osoby,

- vyhlášku č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, která definuje bezpečnostní opatření pro povinné osoby ve vyšším režimu,

- vyhlášku č. 410/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností, která definuje bezpečnostní opatření pro povinné osoby v nižším režimu,

- vyhlášku č. 334/2025 Sb., o Portálu Úřadu a požadavcích na vybrané úkony, která definuje, jakým způsobem bude probíhat komunikace s regulátorem a jaké informace budou ohlašovány,

- vyhlášku č. 411/2025 Sb., o bezpečnostních úrovních informačních systémů veřejné správy, která souvisí s regulací využívání cloud computingových služeb u informačních systémů veřejné správy (dále jen „ISVS“) a pro tyto účely stanoví kritéria pro rozřazení ISVS do bezpečnostních úrovní podle jejich dopadu,

- vyhlášku č. 412/2025 Sb., o bezpečnostních pravidlech pro orgány veřejné správy využívající služby poskytovatelů cloud computingu, která definuje bezpečnostní pravidla, která je nutno zavést na straně orgánů veřejné správy, které využívají služeb cloud computingu pro zajištění provozu jejich ISVS,

- vyhlášku č. 505/2025 Sb., o některých požadavcích pro zápis do katalogu cloud computingu, která definuje bezpečnostní opatření, jež musí poskytovatel a služba cloud computingu splňovat, pokud chce dodávat cloudové služby do ISVS,

- prováděcí nařízení Komise (EU) 2024/2690 ze dne 17. října 2024, kterým se stanoví pravidla pro uplatňování směrnice (EU) 2022/2555, pokud jde o technické a metodické požadavky na opatření k řízení kybernetických bezpečnostních rizik a bližší upřesnění případů, v nichž se incident považuje za významný, pokud jde o provozovatele DNS, registry domén nejvyšší úrovně, poskytovatele služeb cloud computingu, poskytovatele služeb datových center, poskytovatele sítí pro doručování obsahu, poskytovatele řízených služeb, poskytovatele řízených bezpečnostních služeb, poskytovatele on-line tržišť, internetových vyhledávačů a služeb platforem sociálních sítí a poskytovatele služeb vytvářejících důvěru, dále stanovuje specifika regulace poskytovatelů digitálních služeb.

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.

O NÚKIB

NÚKIB V SOUČASNOSTI POMÁHÁ ZAJIŠŤOVAT KYBERNETICKOU BEZPEČNOST ČR A JEJÍCH OBYVATEL PROSTŘEDNICTVÍM:

Poskytování včasných, jasných a relevantních informací subjektům kritické informační infrastruktury, provozovatelům základní služby i orgánům veřejné správy.

Zajišťování bezpečnosti utajovaných informací v informačních a komunikačních systémech včetně kryptografické ochrany.

Vedení operativní reakce na kybernetické incidenty s využitím expertizy a přístupu k informacím pro efektivní zvládnutí incidentů.

Poskytování metodické podpory, vzdělávání a osvěty v tématech spojených s oblastí kybernetické bezpečnosti.

Pořádání tréninků a kybernetických cvičení na národní i mezinárodní úrovni.

Provádění výzkumu a vývoje v oblasti kybernetické bezpečnosti.

Zastupování ČR v orgánech mezinárodních organizací působících v oblasti kybernetické bezpečnosti.

Analýzy trendů v oblasti kybernetické bezpečnosti.

Poskytování technické pomoci a dalších služeb, např. prověření zabezpečení pomocí technik penetračního testování nebo poskytování skenů zranitelností.

Provádění kontroly dodržování požadavků zákona o kybernetické bezpečnosti u regulovaných osob.

Vyhodnocování rizik v oblasti kybernetické bezpečnosti a přijímání příslušných nápravných a preventivních opatření.

Přípravy národních bezpečnostních standardů, zákonů a podzákonných norem v oblasti kybernetické bezpečnosti.

Spolupráce s veřejným, soukromým a akademickým sektorem na národní i mezinárodní úrovni.