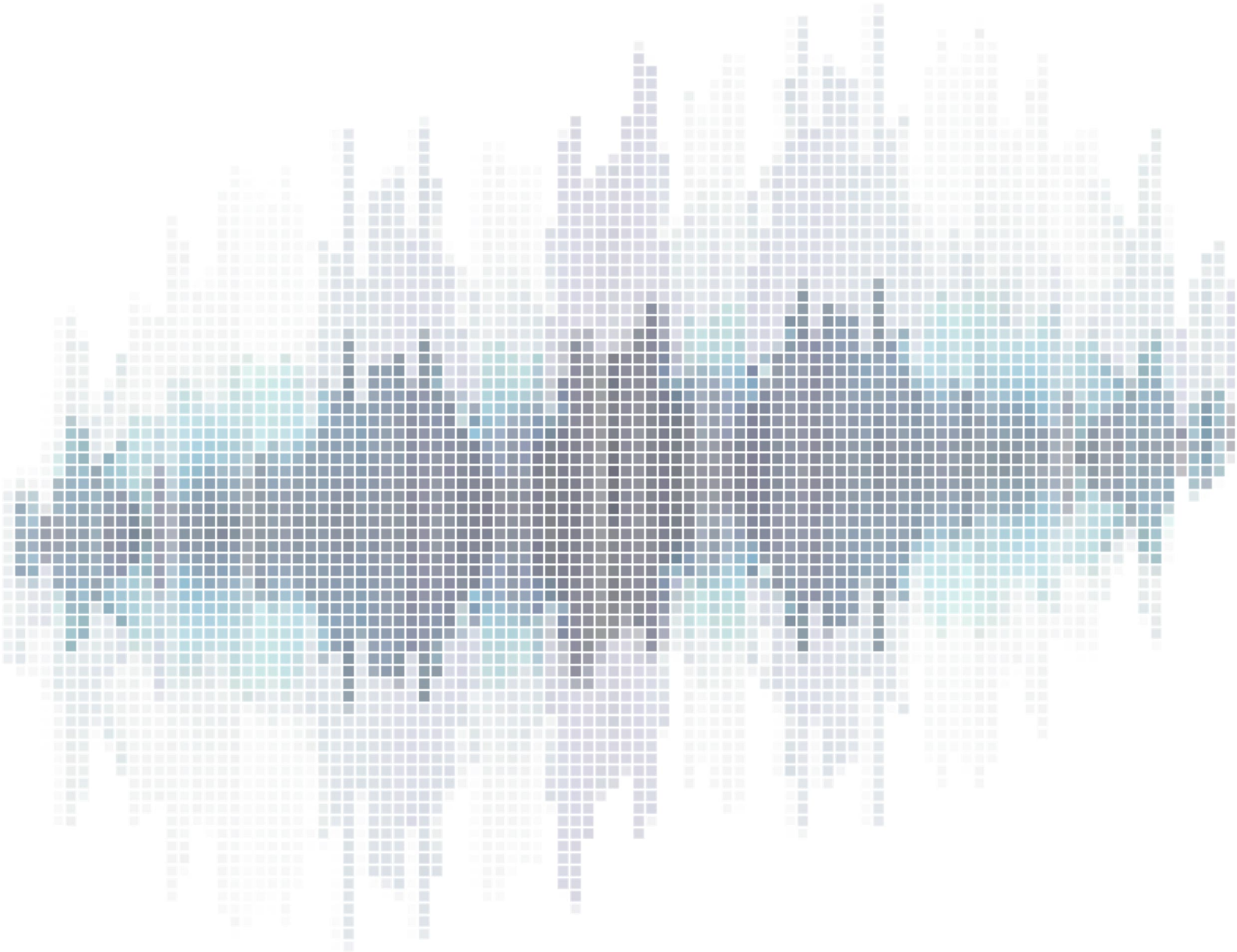
# Čtvrtletní přehled hrozeb pohledem NÚKIB

## Q3 2025



Národní úřad
pro kybernetickou
a informační bezpečnost

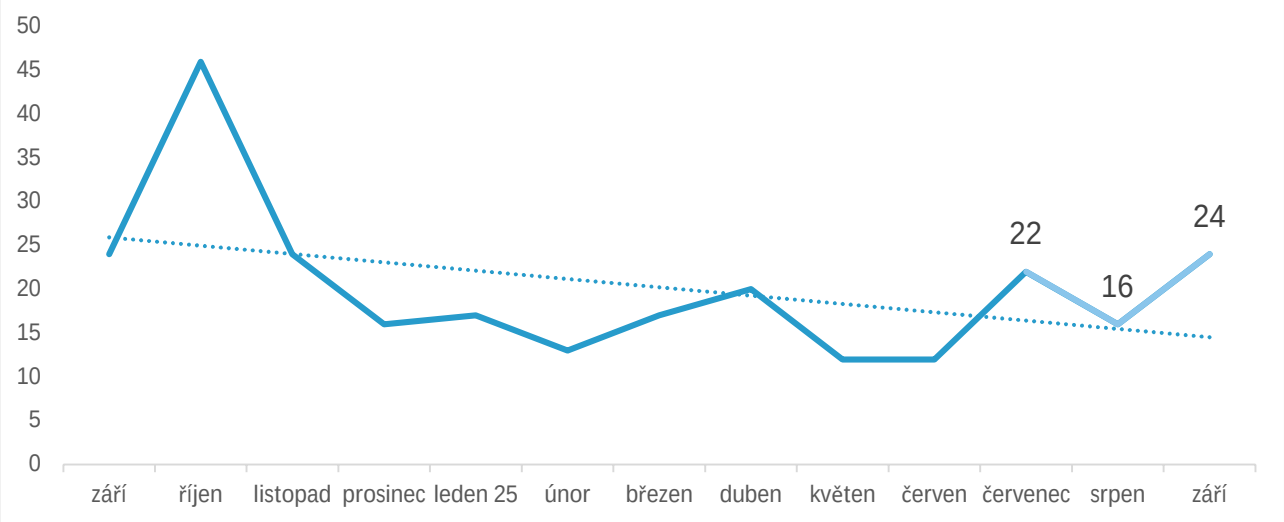
## Shrnutí uplynulého čtvrtletí[1]

Třetí čtvrtletí roku 2025 se ve srovnání se dvěma předchozími vyznačovalo vyšším počtem evidovaných kybernetických incidentů. Za vysokými hodnotami stojí zejména obnovená aktivita proruských hacktivistických skupin a jejich DDoS útoky, ale také poměrně vysoký počet provozních výpadků či kompromitací účtů. K nárůstu činnosti hacktivistů došlo s menším odstupem po úspěšné mezinárodní operaci Eastwood, které se účastnila i Česká republika a jejímž cílem bylo zneškodnění skupiny NoName057(16). Přinejmenším některé DDoS útoky přitom přímo reagovaly na tuto operaci a byly označovány za odplatu. Většina z nich cílila na státní instituce či samosprávy.

Vyšší počet výpadků (13) pak do velké míry souvisel s červencovými výpadky dodávek elektrické energie. Naopak aktivní celosvětové zneužívání nové zranitelnosti typu remote code execution (RCE) v platformě Microsoft SharePoint, kterou blíže popisujeme v rámci kapitoly Kybernetické hrozby s bezprostředním dopadem na Českou republiku, se do počtu incidentů promítlo minimálně (2).

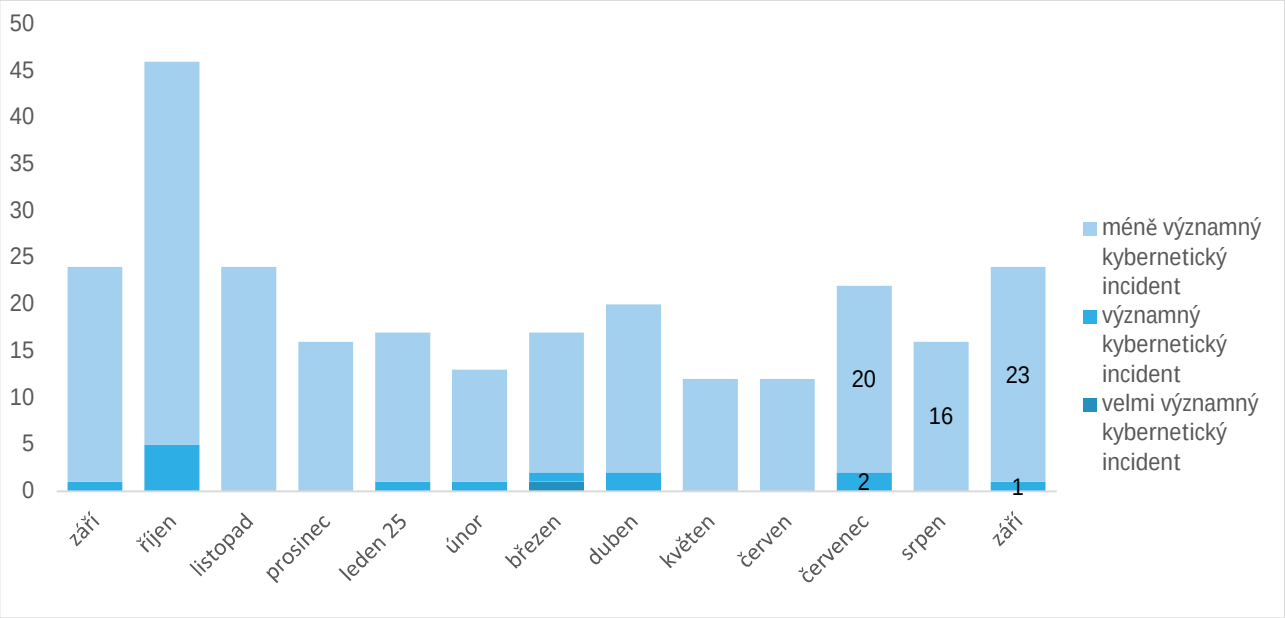
Aktuální čtvrtletní přehled se mimo jiné věnuje dvěma vydaným varováním a upozornění na aktivity čínského aktéra Salt Typhoon, který kompromituje sítě po celém světě. NÚKIB se s ohledem na globální rozsah této kampaně připojil ke společné analýze amerických bezpečnostních vládních agentur a dalších mezinárodních partnerů. V rámci přehledu se rovněž věnujeme shrnutí zpráv a událostí v celosvětovém kontextu s přesahem do kybernetické bezpečnosti v tuzemsku. Z uplynulého čtvrtletí zmiňujeme například aktivity proruských hacktivistů, ruských aktérů či ransomwarový útok vedoucí k narušení provozu evropských letišť. Závěrem přinášíme ohlédnutí za 11. ročníkem konference Cyber_Con a účastí českého týmu na NATO Cyber Champions Summit 2025, jehož další ročník bude ČR hostit.

### Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB



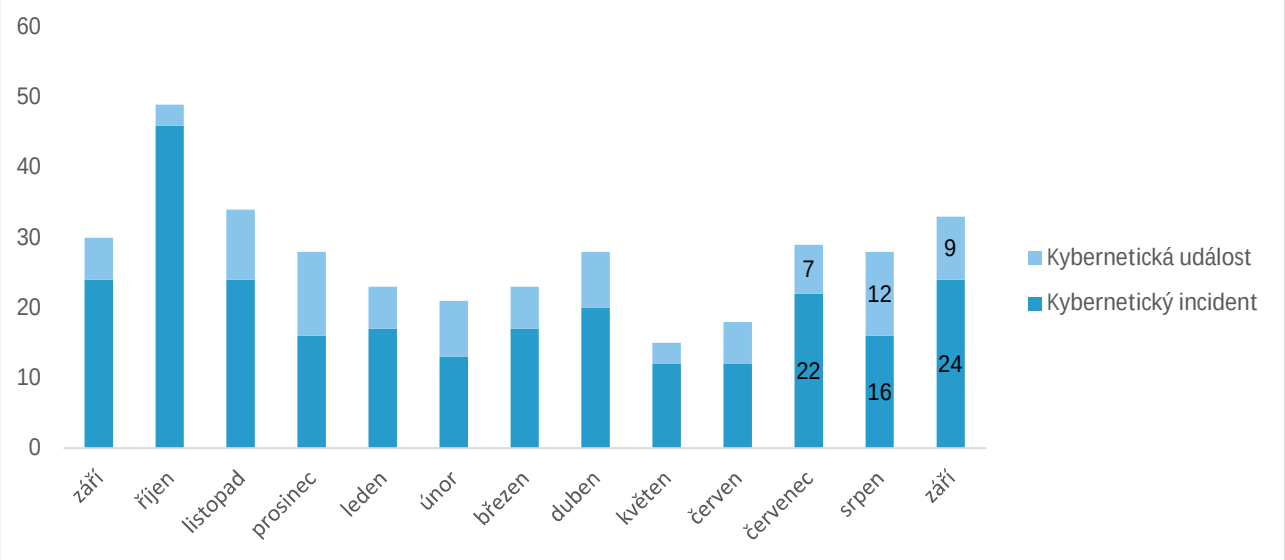

[1] Následující přehled shrnuje dění uplynulého čtvrtletí. Informace a závěry obsažené v této analýze vycházejí z veřejně dostupných informací a z informací získaných v rámci činnosti NÚKIB v době publikace. Připomínky a náměty na zlepšení reportu můžete posílat na adresu komunikace@nukib.gov.cz.

## Závažnost řešených kybernetických incidentů[2]




## Podíl kybernetických incidentů a událostí zaznamenaných NÚKIB[3]

NÚKIB v rámci své činnosti přijímá, zpracovává a vyhodnocuje hlášení kybernetických incidentů. Na základě provedené analýzy může být hlášení klasifikováno jako kybernetický incident, kybernetická událost nebo jako nerelevantní podnět. Graf níže ukazuje podíl kybernetických incidentů a kybernetických událostí.




[2] Závažnost kybernetických incidentů je definována ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, a v interní metodice NÚKIB.

[3] Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.
Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.
Oba pojmy definuje zákon o kybernetické bezpečnosti.

# Kybernetické hrozby s bezprostředním dopadem na Českou republiku

## NÚKIB vydal varování před některými produkty společnosti DeepSeek a před hrozbou spočívající v předávání dat a ve výkonu vzdálené správy z Čínské lidové republiky

NÚKIB v uplynulém čtvrtletí vydal dvě varování. První z nich před hrozbou v oblasti kybernetické bezpečnosti spočívající ve využívání produktů, aplikací, řešení, webových stránek a webových služeb, včetně aplikačního programového rozhraní (tzv. API), poskytovaných společností DeepSeek nebo jakoukoli její předchůdkyní, nástupnickou, mateřskou, dceřinou či přidruženou společností na zařízeních přistupujících k informačním a komunikačním systémům kritické informační infrastruktury, informačním systémům základní služby a významným informačním systémům. Simultánně s tímto varováním Vláda ČR rozhodla o zákazu používání produktů společnosti DeepSeek ve státní správě.

Druhé varování se týkalo hrozby v oblasti kybernetické bezpečnosti spočívající v předávání systémových a uživatelských dat do Čínské lidové republiky a ve vzdálené správě technických aktiv vykonávané z území Čínské lidové republiky.

Na základě vydaných varování musí povinné osoby dle zákona o kybernetické bezpečnosti zohlednit hrozbu v analýze rizik a na zjištěná rizika reagovat přijetím přiměřených bezpečnostních opatření.

## NÚKIB spolu s NSA a dalšími americkými úřady a mezinárodními partnery upozorňuje na čínského aktéra Salt Typhoon, který kompromituje sítě po celém světě

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) se připojil ke společné analýze amerických bezpečnostních vládních agentur a dalších mezinárodních partnerů, tzv. Joint Cyber Security Advisory. Jedná se o upozornění týkající se aktivit kybernetických útočníků podporovaných Čínskou lidovou republikou (ČLR), kteří pronikají do sítí po celém světě s cílem získat k nim dlouhodobý přístup a využívat je pro špionážní činnost. Tyto aktivity částečně odpovídají činnosti APT aktéra nejčastěji označovaného jako *Salt Typhoon*. Útočníci se zaměřují na páteřní routery velkých poskytovatelů telekomunikačních služeb a routery na hranici sítě poskytovatele (provider edge, PE) a zákazníka (customer edge, CE) a využívají kompromitovaná zařízení či důvěryhodná propojení k dalšímu průniku do sítí. Aktéři přitom routery často modifikují tak, aby si zajistili trvalý přístup. Jedná se tedy de facto o útoky na dodavatelský řetězec, kdy útočník nejprve kompromituje jeden subjekt, aby získal přístup k řadě dalších. Podle vyšetřování jsou operace tohoto aktéra napojeny na tři čínské společnosti poskytující služby a produkty armádě a Ministerstvu státní bezpečnosti ČLR.

Bezpečnostní instituce zapojené do upozornění

Cílem této analýzy je zejména sdílení technických detailů a doporučení pro mitigaci, zvyšování povědomí o těchto hrozbách a odstrašení útočníků v kyberprostoru. Autoři upozornění vyzývají správce sítí a bezpečnostní týmy, aby aktivně vyhledávali škodlivé aktivity dle instrukcí uvedených v upozornění a aplikovali doporučená opatření.

## Evropské bezpečnostní složky zneškodnily hacktivistickou skupinu NoName057(16)

V červenci 2025 došlo k významnému zásahu evropských bezpečnostních složek proti proruské hacktivistické skupině NoName057(16). V rámci mezinárodní operace Eastwood byla zneškodněna infrastruktura této skupiny, která podle Europolu využívala stovky systémů napříč kontinenty pro vedení DDoS útoků. Operace se účastnilo 12 států včetně ČR prostřednictvím Národní centrály proti terorismu, extremismu a kybernetické kriminalitě (NCTEKK). Operace vedla k odstavení velké části centrální infrastruktury skupiny i k identifikaci osob včetně klíčových členů pobývajících v Rusku. Zároveň byli zadrženi dva jednotlivci ve Francii a Španělsku.

Mapa zobrazující země, které se zapojily do operace Eastwood


NoName057(16) patří k velmi aktivním hacktivistickým skupinám napříč Evropou, ale i v tuzemsku, přičemž historicky stojí za velkou částí DDoS útoků směřujících právě vůči českým subjektům. Zatímco během července, kdy operace Eastwood proběhla, NÚKIB neevidoval žádný DDoS útok spojený s proruskými hacktivisty, v srpnu došlo k jejich opětovnému nárůstu. Za velkou částí těchto útoků přitom stála samotná NoName057(16) a další proruská hacktivistická skupina Server Killers. Většina těchto útoků přitom byla prezentována jako odplata za operaci Eastwood.

## Microsoft SharePoint zasáhla vlna útoků využívající novou zranitelnost, byla zneužita třemi čínskými aktéry. Útoky se dotkly také ČR

Americká Agentura pro kybernetickou a infrastrukturní bezpečnost (CISA) v neděli 20. července varovala před aktivním zneužíváním nové zranitelnosti typu remote code execution (RCE) v platformě Microsoft SharePoint, označené jako CVE-2025-53770. Tato zranitelnost, veřejně známá

jako „ToolShell“, umožňuje neautentizovaným útočníkům plný přístup k on-premise serverům, včetně spouštění kódu a čtení interní konfigurace. CISA doporučuje mimo jiné instalaci aktualizací, aktivaci rozhraní AMSI a nasazení Microsoft Defender AV. Zranitelnost byla téhož dne zařazena do katalogu CISA KEV. Microsoft uvedl, že zranitelnost byla aktivně zneužívána čínskými aktéry Linen Typhoon (APT27), Violet Typhoon (APT31) a Storm-2603. Zatímco první dvě se zaměřují na špionážní aktivity, Storm-2603 šířil prostřednictvím zranitelnosti ransomware Warlock.

Bezpečnostní společnost Eye Security evidovala během prvních dnů více než 400 kompromitovaných systémů po celém světě. Společnost Symantec pak např. k 22. červenci zaznamenala více než 2 000 pokusů o zneužití zranitelnosti. Mezi napadenými subjekty figuruje například americké ministerstvo energetiky a jeho Národní úřad pro jadernou bezpečnost (NNSA). NÚKIB v souvislosti s touto zranitelností rovněž evidoval několik kompromitací.

# Situační přehled kybernetických hrozeb relevantních pro Českou republiku

NÚKIB dlouhodobě monitoruje relevantní hrozby, které nemají bezprostřední dopad na bezpečnost České republiky. I tyto hrozby však mohou mít přímý či nepřímý vliv na kybernetickou bezpečnost českých subjektů, ať již v současnosti, či budoucnu. Udržování situačního povědomí o aktuálních hrozbách je tak klíčovou součástí aktivit NÚKIB.

## Proruští hacktivisté v Norsku manipulovali s ventily tamní přehrady, Polsko zabránilo kyberútoku na dodávky vody

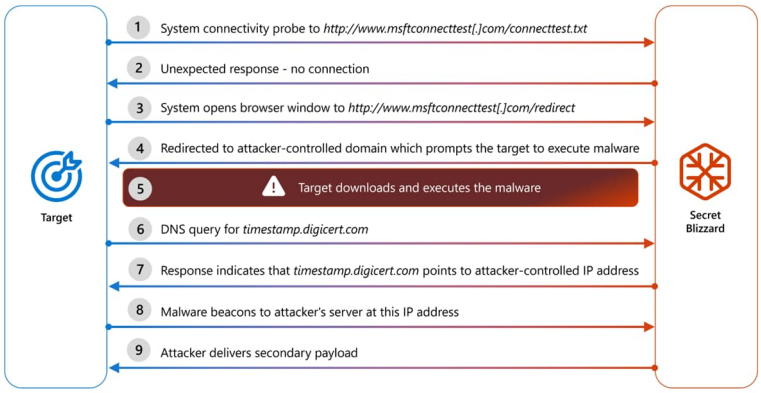
Norská Policejní bezpečnostní služba (PST) oznámila, že proruští hacktivisté v dubnu tohoto roku získali přístup k systémům přehrady v západním Norsku a otevřeli odtokové ventily. Útočníkům se během čtyř hodin podařilo vypustit 500 litrů vody za sekundu, než byli zastaveni. Incident nezpůsobil žádné zranění ani škody. Pachatelé měli v den útoku zveřejnit na Telegramu tříminutové video zobrazující průběh útoku. Ředitelka PST Beate Gangåsová uvedla, že cílem útoku bylo předvést schopnosti útočníků a vyvolat strach spíše než způsobit destrukci. Polsko pak v srpnu zabránilo vážnému kybernetickému incidentu, který mohl způsobit výpadek dodávek vody v tamním velkém městě. Útok se podařilo zastavit v počáteční fázi díky včasnému zásahu bezpečnostních služeb.

Úřady oficiálně neuvedly, které město bylo cílem, ani neoznačily pachatele útoku, nicméně dle některých informací je možnou obětí elektrárna ve městě Tczew na severu země, která byla napadena již letos v květnu. Polští analytici na základě sebraných dat hodnotí, že nynější útok měl vyšší dopad než ten květnový, zejména kvůli tomu, že údajně došlo k narušení činnosti.

## Ruský aktér Secret Blizzard podniká kyberšpionáž vůči tamním ambasádám na úrovni poskytovatelů internetových služeb

Státem sponzorovaná skupina Secret Blizzard (též známá jako Turla), spojovaná s ruskou Federální službou bezpečnosti (FSB), provádí od roku 2024 kyberšpionáž proti zahraničním ambasádám v Moskvě. Informovala o tom společnost Microsoft s tím, že tato kampaň je specifická využitím úrovně poskytovatelů internetových služeb (ISP). Skupina pravděpodobně využívá státní systémy zákonného odposlechu, jako je ruský SORM, k získání přístupu k síťovému provozu diplomatických institucí. Hlavní vektor útoku tak představuje technika adversary-in-the-middle (AiTM), kdy si útočník zajistí pozici mezi dvěma nebo více sítěmi, odkud může provádět další aktivity, včetně záchytu či podvrhování komunikace.

Infekční řetězec útoku Secret Blizzard (větší rozlišení)




Zdroj: microsoft.com

Secret Blizzard toho využívá mj. k nasazení malwaru ApolloShadow a sběru strategických informací. Výše uvedená zjištění implikují, že diplomatický personál využívající místní internetové nebo telekomunikační služby je s vysokou pravděpodobností terčem této kampaně. Microsoft zároveň vydal sadu doporučení, v rámci které institucím a společnostem působícím v Moskvě doporučuje směrovat veškerou komunikaci skrze šifrovaný tunel či používat VPN služby.

## Ransomwarový útok vedl k narušení provozu na řadě evropských letišť, Británie již zadržela prvního podezřelého

Dne 19. září došlo k ransomwarovému útoku na dodavatele softwaru Collins Aerospace, který vedl k narušení provozu řady významných evropských letišť. Útok ovlivnil funkčnost samoobslužného softwaru vMUSE, který podporuje odbavení cestujících, označování zavazadel a nástup do letadla. To vedlo k ochromení odbavovacích a zavazadlových systémů na evropských letištích, např. v Londýně, Bruselu, Berlíně a Dublinu, a tisíce cestujících musely čelit dlouhým frontám na manuální odbavení, stovkám zpoždění či zrušení letů.

Evropská agentura pro bezpečnost sítí a informací (ENISA) uvedla, že v rámci útoku byl použit ransomware, odmítla však specifikovat, o jakou variantu šlo. Britský Národní kriminální úřad (NCA) oznámil, že v souvislosti s útokem došlo k zadržení jednoho muže ze Západního Sussexu. Ten byl posléze propuštěn na podmínečnou kauci.

## Ruská kyberšpionážní skupina Static Tundra zneužívá zranitelná Cisco zařízení

Americký Federální úřad pro vyšetřování (FBI) spolu s bezpečnostním týmem Cisco Talos varovali před kyberšpionážní kampaní ruské státem sponzorované skupiny Static Tundra (též Berserk Bear či Dragonfly). V rámci této aktivity aktér zneužívá sedm let starou zranitelnost (CVE-2018-0171), na kterou byla dostupná záplata již v době zveřejnění zranitelnosti v roce 2018. Cílem této kampaně probíhající přinejmenším od roku 2021 jsou organizace v odvětvích výroby, telekomunikací a vysokoškolského vzdělávání v Severní Americe, Asii, Africe a Evropě, přičemž oběti jsou vybírány na základě strategického významu pro ruskou vládu. Součástí analýzy Cisco Talos je sada detekčních opatření i preventivních doporučení pro relevantní organizace.

## Spolupráce a sdílení informací v boji proti kybernetickým hrozbám

Zajišťování kybernetické bezpečnosti nezahrnuje pouze monitorování hrozeb a řešení kybernetických incidentů. Nezanedbatelnou součástí této činnosti je také vzájemná spolupráce, její rozvoj, sdílení zkušeností a informací o aktuálních hrozbách a způsobech, jak jim efektivně čelit.

### Na 11. ročníku CYBER_CON 2025 se potkali odborníci a zájemci o kyberbezpečnost

V rámci jedenáctého ročníku konference CYBER_CON 2025, pořádané NÚKIB ve spolupráci s partnery CZ.NIC, NIX.CZ, CESNET a dalšími, se navzájem setkali techničtí a právní specialisté, akademici, manažeři i studenti, aby diskutovali o aktuálních výzvách a příležitostech v oblasti kybernetické bezpečnosti. Program konference organizátoři postavili kolem témat Národní strategie kybernetické bezpečnosti a zákona o kybernetické bezpečnosti.

„Na letošním ročníku CYBER_CON se opět ukázalo, že kybernetická bezpečnost si žádá mezioborovou spolupráci a otevřený dialog. Jsem hrdý na to, že se nám podařilo vytvořit platformu, kde se setkávají odborníci z různých oblastí, sdílejí své zkušenosti a společně hledají řešení aktuálních i budoucích výzev. Osobně mám obrovskou radost z toho, že nadšení a práce lidí na NÚKIB má i takovéto výsledky a účast na CYBER_CON je pro mě vždy za odměnu," uvedl ředitel NÚKIB Lukáš Kintr.


### Česká delegace v Jižní Koreji převzala štafetu NATO Cyber Champions Summit 2026

Česká republika bude v roce 2026 hostit další ročník NATO Cyber Champions Summit. Pomyslnou štafetu převzali v září zástupci NÚKIB od Jižní Koreji. Česká delegace vedená NÚKIB se v Soulu aktivně účastnila několika konferencí a mezinárodních fór, kde sdílela české zkušenosti se zajišťováním kybernetické bezpečnosti. Prvním bodem programu byla konference Cyber Summit Korea, kde ředitel NÚKIB přednesl příspěvek s názvem From Legislation to Resilience: The Future of Cybersecurity in Czechia.

Na NATO Cyber Champions Summit, který slouží jako most mezi transatlantickým a asijsko-pacifickým prostorem, se delegace ČR aktivně zapojila do diskusí o nejaktuálnějších kybernetických hrozbách. Ředitel NÚKIB Lukáš Kintr následně akci uzavřel a zároveň oficiálně pozval účastníky na další ročník tohoto prestižního summitu, který bude v roce 2026 hostit Praha.

Součástí programu bylo také mezinárodní cvičení APEX (Allied Power Exercise) 2025, do kterého se zapojilo přes 200 účastníků z 25 zemí. Českou republiku reprezentovali experti z vládního CERT, kteří vytvořili společný tým s Jižní Koreou a Norskem.

Na okraj hlavních akcí se česká delegace zúčastnila uzavřeného kulatého stolu pro kybernetické bezpečnostní agentury, Counter Ransomware Initiative, a absolvovala také několik bilaterálních jednání. Hlavními tématy byly sdílení zkušeností s legislativními změnami a analýza aktuálního cyber threat landscape.

## Použité pravděpodobnostní výrazy

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 % |

## Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách NÚKIB). Informace je označena příznakem, který stanoví podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

| Barva | Podmínky použití |
|---|---|
| TLP:RED | Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace. |
| TLP:AMBER+STRICT | Informace může být sdílena pouze v rámci organizace příjemce, a to pouze osobám, které splňují need-to-know. |
| TLP:AMBER | Informace může být sdílena v rámci organizace příjemce a jejím partnerům, a to pouze osobám, které splňují need-to-know. |
| TLP:GREEN | Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace. |
| TLP:CLEAR | Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena. |