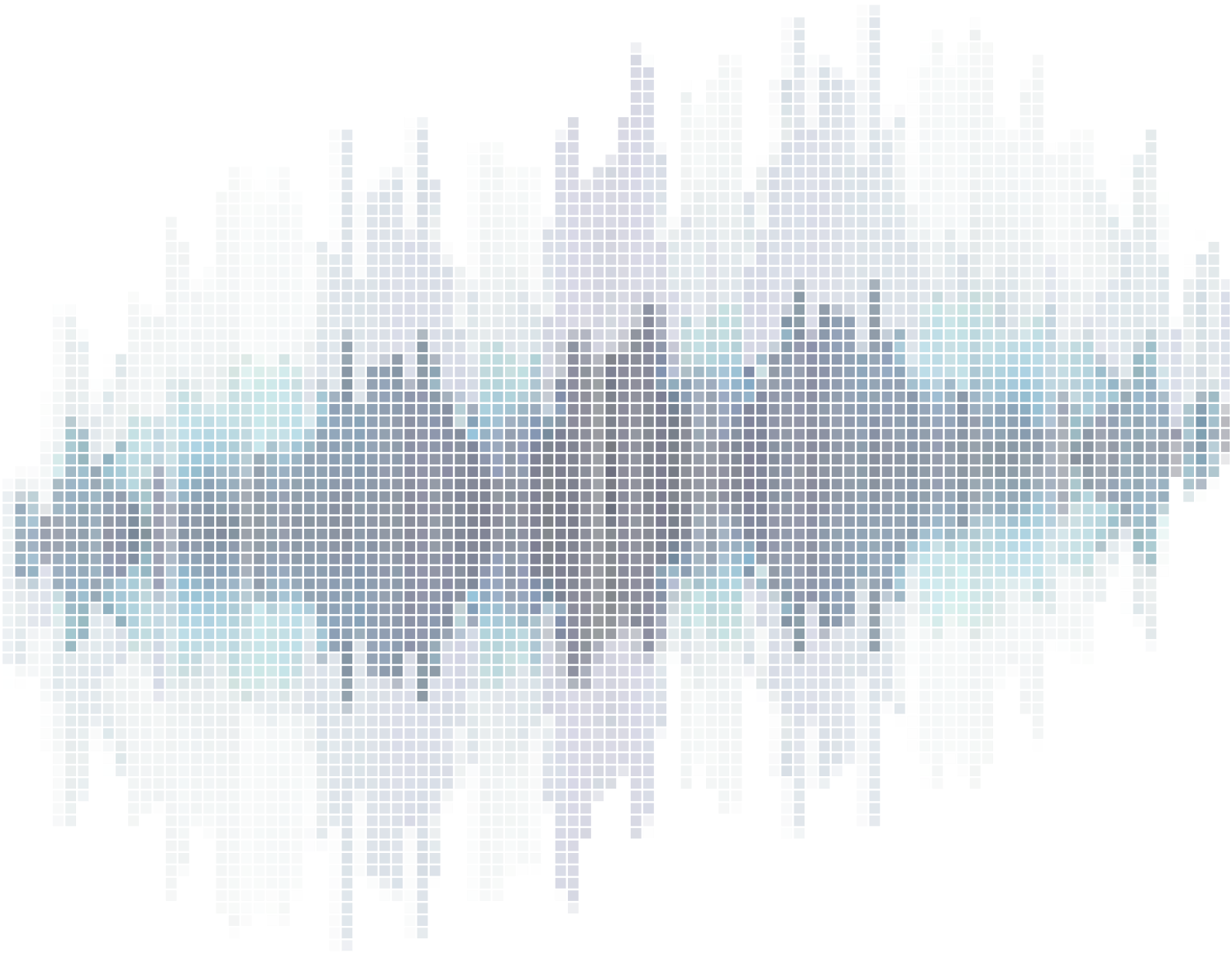
# Čtvrtletní přehled hrozeb pohledem NÚKIB

## Q2 2026



Národní úřad
pro kybernetickou
a informační bezpečnost

## Shrnutí uplynulého čtvrtletí[1]

Za druhé čtvrtletí roku 2026 NÚKIB evidoval celkem 44 kybernetických incidentů, což představovalo nejnižší hodnotu za poslední rok. Oproti prvnímu čtvrtletí tak došlo k poklesu téměř o polovinu. Z evidovaných incidentů bylo 6 označeno jako významných, tedy stejně jako v předchozím čtvrtletí. Na rozdíl od prvního čtvrtletí, kdy NÚKIB evidoval jeden velmi významný incident, tentokrát žádný incident této závažnosti zaznamenán nebyl.

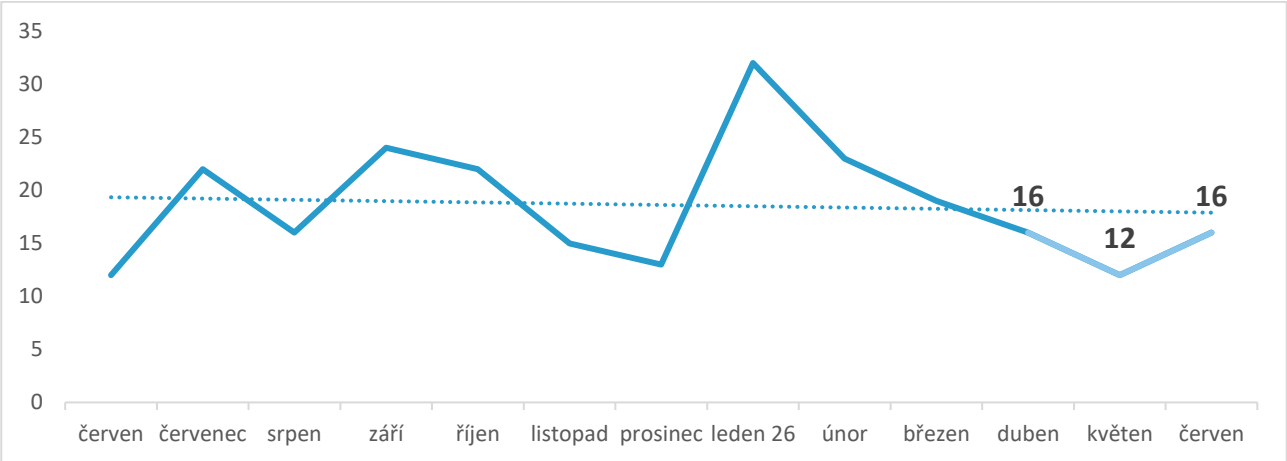
Zatímco v absolutním množství se významné a velmi významné incidenty dlouhodobě drží na podobné úrovni, vzhledem k celkovému poklesu počtu incidentů jejich podíl ve druhém čtvrtletí mírně narostl. Výrazně ubylo zejména DDoS útoků, přičemž poslední vlna DDoS útoků proruských hacktivistů proběhla v lednu 2026. Ačkoli útoky na dostupnost zcela nezmizely, jsou sporadičtější a nevykazují znaky systematických kampaní.

Výrazně naopak narostl podíl incidentů v rámci kategorie Průnik, které se tak v druhém čtvrtletí staly nejčastějším typem kybernetického bezpečnostního incidentu. Došlo ke kompromitacím účtů, firewallů či aplikačních serverů. Tyto incidenty zasáhly zejména instituce z veřejné správy, vzdělávacího sektoru anebo také zdravotnictví.

### Nový zákon o kybernetické bezpečnosti, který nabyl účinnosti 1. 11. 2025, výrazně navýšil množství subjektů, které se musí řídit regulací v oblasti kyberbezpečnosti. Počet incidentů ale prozatím výrazně nenarůstá, proč?

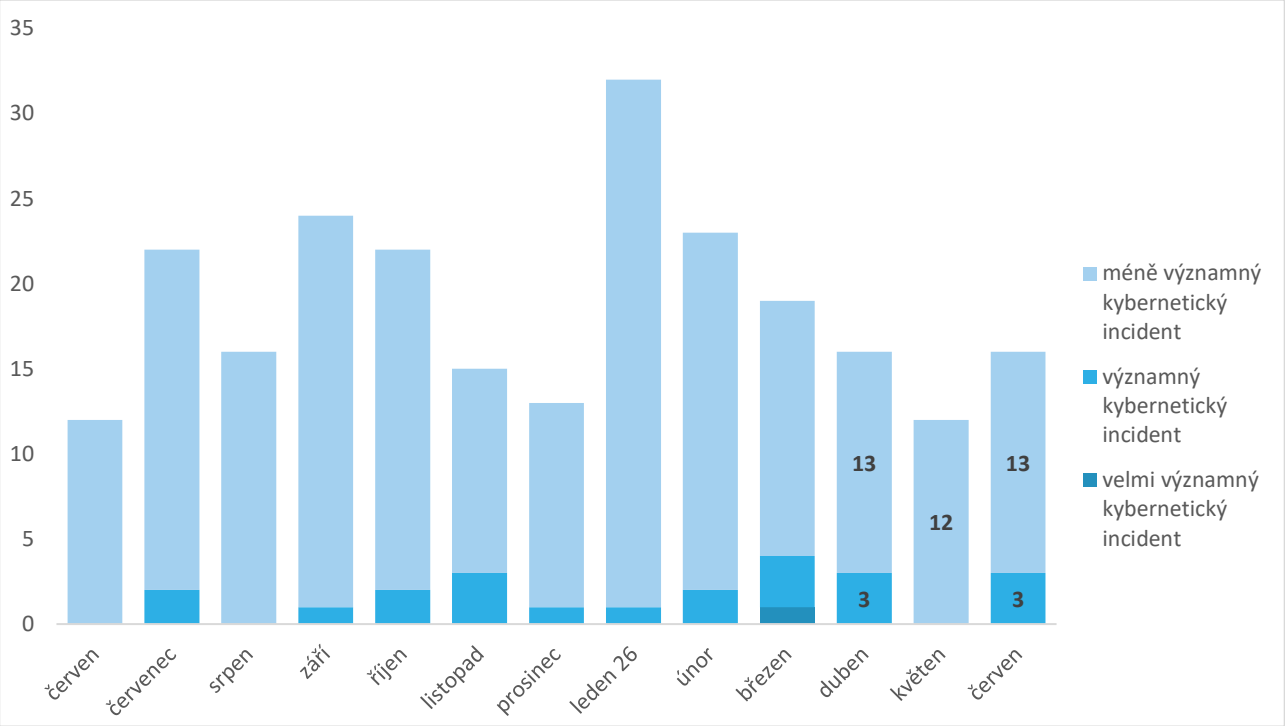
Poskytovatelé regulovaných služeb mají od doručení rozhodnutí o registraci rok na to, aby incidenty začaly NÚKIB hlásit. Dopad nové regulace se tak nemusí výraznějším způsobem projevit přinejmenším do přelomu roku 2026 a 2027. Povinnost nahlašovat všechny zaznamenané incidenty mají zároveň pouze poskytovatelé regulovaných služeb v režimu vyšších povinností. Subjekty v režimu nižších povinností řešení kybernetických bezpečnostních incidentů koordinují s Národním CERT (CSIRT.CZ), NÚKIB (GovCERT.CZ) je nahlašují pouze v případě, že je sami vyhodnotí jako významné.

## Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB



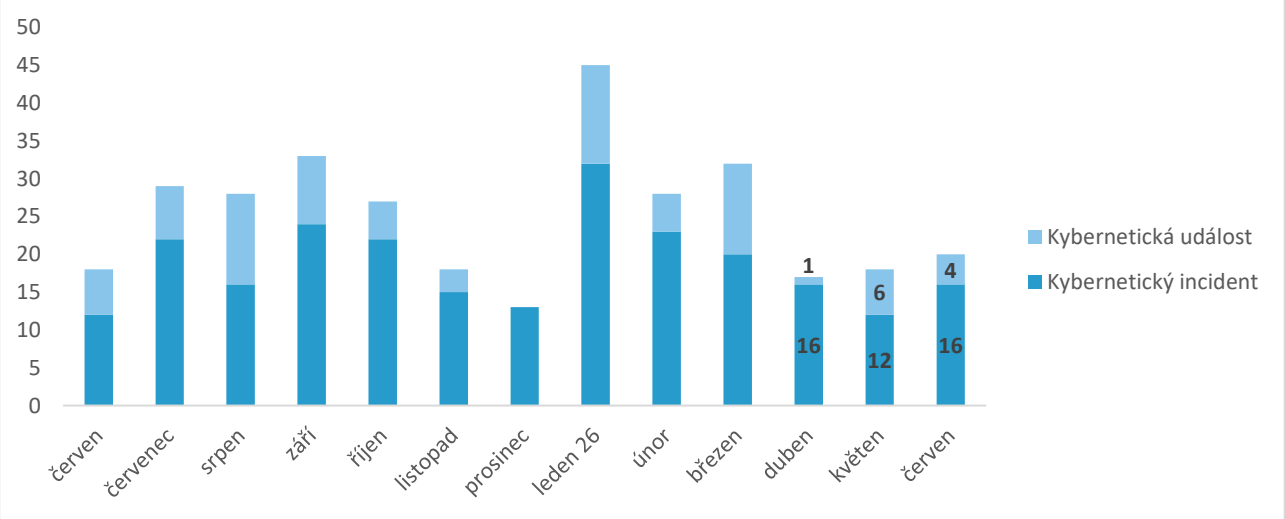

[1] Následující přehled shrnuje dění uplynulého čtvrtletí. Informace a závěry obsažené v této analýze vycházejí z veřejně dostupných informací a z informací získaných v rámci činnosti NÚKIB v době publikace. Připomínky a náměty na zlepšení reportu můžete posílat na adresu komunikace@nukib.gov.cz.

## 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 buď 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

## Ruský státní aktér APT28 kompromitoval routery TP-Link, české Vojenské zpravodajství provedlo aktivní zásah

Ruský státní aktér APT28, spadající pod ruské vojenské zpravodajství GRU, vybudoval podle zprávy amerického ministerstva spravedlnosti a Federálního úřadu pro vyšetřování (FBI) globální síť kompromitovaných routerů pro malé a domácí kanceláře (tzv. SOHO routery). Cílem aktivity skupiny APT28 byla kyberšpionáž a největší riziko se týkalo zařízení, která používala výchozí administrátorská hesla. Na zprávě se podílelo i české Vojenské zpravodajství, které v rámci mezinárodní operace vedené USA provedlo aktivní zásah spočívající v úpravě nastavení části globálně zneužívané infrastruktury a zabezpečení potenciálně zneužitelných zařízení na území ČR. O věci blíže informovalo na svých webových stránkách.

Kampaň ruského 85. hlavního centra speciálních služeb GRU (85. GTsSS), která dle zprávy FBI probíhá minimálně od roku 2024, se od předchozích liší způsobem provedení. APT28 (též známý jako Fancy Bear, Forest Blizzard či Sofacy Group) využil při průniku do routerů zranitelnost CVE-2023-50224 v modelu TP-Link TL-WR841N, která umožňuje obejít autentizaci a získat neoprávněný přístup k routerům. Prostřednictvím této zranitelnosti aktér upravil jejich konfiguraci, kterou převzala i další zařízení připojená na kompromitované routery.

Útočník následně mohl monitorovat dotazy na doménová jména a pro vybrané domény a služby jako např. MS Outlook Web Access vracet podvržené DNS odpovědi a provádět tzv. adversary-in-the-middle útoky na šifrovanou komunikaci. Tímto způsobem APT28 získávala hesla, autentizační tokeny a další citlivé informace (včetně obsahu e-mailů či webové komunikace), které by za normálních okolností chránilo šifrování SSL/TLS. Skupina kompromitovala široký okruh zařízení ve Spojených státech i dalších státech, včetně ČR. Z nasbíraných dat se zaměřovala zejména na informace týkající se armádních a vládních institucí či organizací z oblasti kritické infrastruktury.

**Přehled organizací, které se na oznámení FBI podílely**

## Kampaň Fortibleed zasáhla na 74 tisíc firewallů Fortinet

Nezávislý ukrajinský výzkumník Volodymyr Diachenko upozornil na probíhající kampaň neznámé rusky mluvící finančně motivované skupiny zaměřenou na firewally společnosti Fortinet. V době odhalení útočníci získali přihlašovací údaje k 73 932 unikátním firewall URL, tedy přibližně k polovině všech firewallů Fortinet vystavených do internetu. Kampaň, označovaná jako Fortibleed, mířila i na síťová úložiště Synology, firewally Sophos a MSSQL servery.

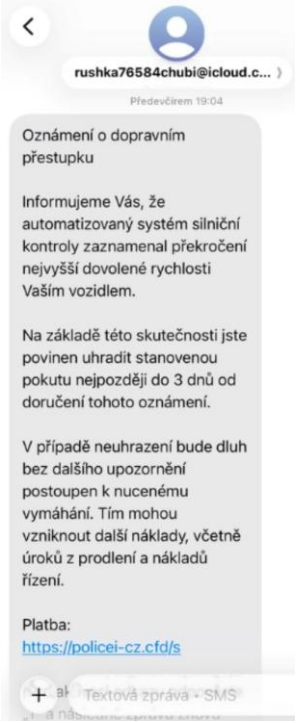
Zasaženy byly subjekty napříč sektory i regiony, včetně velkých společností jako Chevron, Samsung, Toyota či Fortinet samotný. Dle zveřejněných záznamů incident zasáhl i řadu českých subjektů. Je zdokumentováno i odcizení citlivých technických dat turecké zbrojní společnosti ASELSAN.

Z analýzy infrastruktury útočníků vyplývá, že k získávání přihlašovacích údajů nebyla zneužita žádná konkrétní zranitelnost. Údaje byly získány pomocí útoků hrubou silou (tzv. bruteforce) probíhajících pravděpodobně od poloviny května 2026. Po získání přístupu útočníci při útocích exfiltrovali další přihlašovací údaje v rámci kompromitované sítě. Doporučený postup k mitigaci vydala například americká agentura CISA.

## Upozornění na smishingovou kampaň, ve které se útočníci vydávají za Policii ČR

V květnu NÚKIB prostřednictvím svého Portálu vydal upozornění na smishingovou kampaň, v rámci které se útočníci skrze SMS zprávy vydávají za Policii České republiky s cílem získat platební údaje obětí.

**Příklad zprávy využité v rámci smishingové kampaně**




V rámci útoku oběť zpravidla obdrží SMS zprávu informující o údajném dopravním přestupku (např. překročení rychlosti) s výzvou k úhradě pokuty ve stanovené lhůtě (např. do tří dnů). Zpráva obsahuje odkaz na podvodnou stránku vydávající se za oficiální portál státní správy. Útočníci v rámci škodlivých odkazů používají různé obměny výrazů jako „police“, „gov“, „portal“, „euprava“, „listek“ v kombinaci s méně obvyklými koncovkami (.cfd, .bond, .xyz). Konkrétní podoba domén se může v čase měnit. Pokud oběť zadá svoje platební údaje, mohou být následně zneužity k neoprávněným finančním transakcím nebo dalším podvodným aktivitám.

**V souvislosti s kampaní je důležité zmínit, že Policie České republiky tímto způsobem nevyžaduje úhradu pokut, ani nezasílá odkazy k platbě prostřednictvím SMS zpráv.** Obecně NÚKIB v souvislosti s podvodnými kampaněmi doporučuje:

- neklikat na odkazy v nevyžádaných SMS zprávách (zejména pokud obsahují výzvu k úhradě pokuty),
- v případě otevření podobného odkazu nevyplňovat žádné osobní ani platební údaje,
- v případě nejistoty ověřovat podobná oznámení výhradně přes oficiální kanály Policie ČR nebo jiných institucí,
- v případě zadání údajů neprodleně kontaktovat svou banku a přijmout relevantní opatření (blokace karty, kontrola transakcí).

## Think-tank Evropské hodnoty se stal cílem čínského kyberšpionážního aktéra SparkyCarp

Český think-tank Evropské hodnoty (EH) se stal obětí čínského státem sponzorovaného kyberšpionážního aktéra SparkyCarp (neboli UNK_SparkyCarp). Ředitel EH Jakub Janda byl kontaktován přes e-mail osobou vydávající se za reálnou novinářku agentury AP Didi Tangovou, která jej po přesunu konverzace na aplikaci Signal urgovala k vyplnění informací přes Google formulář. Odkaz však směřoval k falešnému přihlášení k účtu Google. Cílem tohoto útoku bylo získat přístupové údaje a zřejmě i další přístup k interní komunikaci, kontaktům či analytickým materiálům organizace.

NÚKIB, jenž byl o celé věci informován, po přezkoumání spojil e-mail s širší kampaní zaměřenou na Tchaj-wan, o níž již dříve informovala soukromá kyberbezpečnostní firma Proofpoint. Identifikovaná infrastruktura mohla být využita také proti čínskému disentu a lidskoprávním organizacím ve světě. Tato kampaň poukazuje na skutečnost, že i nevládní organizace patří mezi zájmové cíle některých státních či státem podporovaných aktérů.

**E-mail, kterým byl navázán kontakt s ředitelem EH Jakubem Jandou**

Dear Director Janda,

My name is Didi Tang, and I'm part of the Asia coverage team at the AP Washington bureau, working on a story about U.S.-China relations.

We're currently preparing a piece on recent shifts in U.S.-China policy, and we'd greatly value your insights on the topic. Would you be available for a brief interview (15–20 minutes) sometime this week or next? We're happy to accommodate your schedule and preferred format.

Thank you very much for your time and consideration. I look forward to your response.

Best regards,

**Didi Tang**

Asian Affairs Reporter

--

AP
Didi Tang
Asian Affairs Reporter
The Associated Press

# 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.

## Nové AI frontier modely významně navyšují schopnost autonomně detekovat a zneužívat zranitelnosti. Zneužití škodlivými aktéry je otázkou času

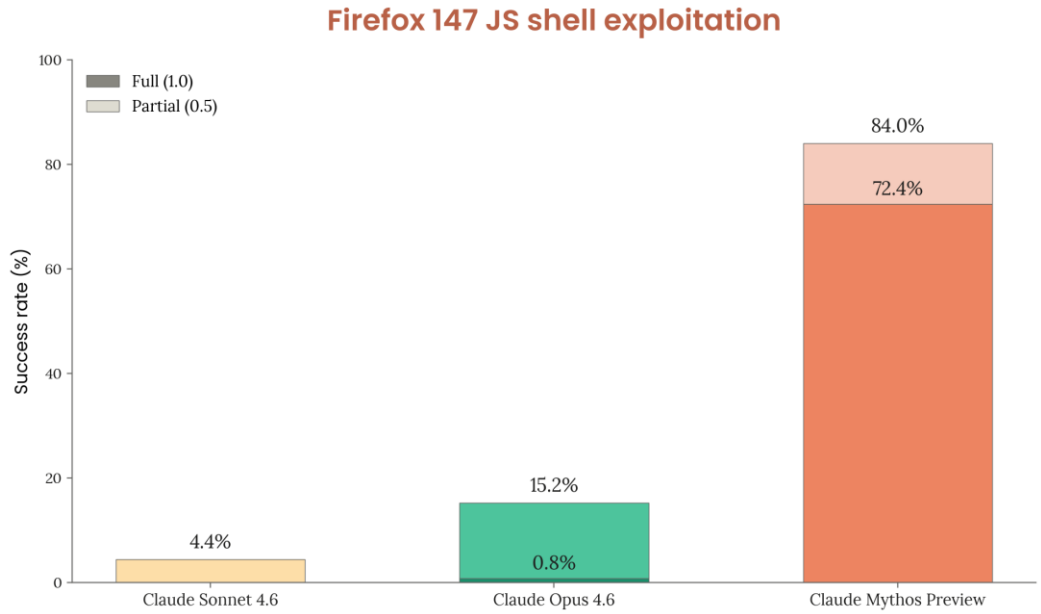
Společnost Anthropic v dubnu 2026 představila model umělé inteligence (AI) Mythos, který díky pokročilé automatizaci dokáže ve velkém rozsahu vyhledávat, ověřovat a zneužívat i dosud neznámé zranitelnosti výrazně účinněji než starší velké jazykové modely. Tato schopnost představuje reálné a závažné riziko pro kybernetickou bezpečnost. Jedná se o posun celého AI odvětví, v němž obdobných kapacit pro vyhledávání a zneužívání zranitelností dosahují i další společnosti. Téměř jistě se tyto kapacity dostanou i do rukou státních a nestátních útočníků, pokud jimi již nedisponují.

Tyto pokročilé frontier AI modely s využitím v kyberbezpečnosti velmi pravděpodobně výrazně zkrátí dobu mezi nalezením zranitelnosti a jejím zneužitím, protože automatizují vyhledávání, ověřování i řetězení zranitelností ve velkém měřítku. Tempo oprav ovšem zůstane nadále omezené lidskými a technickými kapacitami.

V krátkodobém horizontu mohou nové AI modely zvýšit počet kybernetických incidentů i v ČR, a to jak přímými útoky na české subjekty, tak nepřímo prostřednictvím globálních kompromitací velkých poskytovatelů služeb skrze dodavatelské řetězce.

NÚKIB publikoval analytický materiál, který se nástupu nových pokročilých AI modelů blíže věnuje.

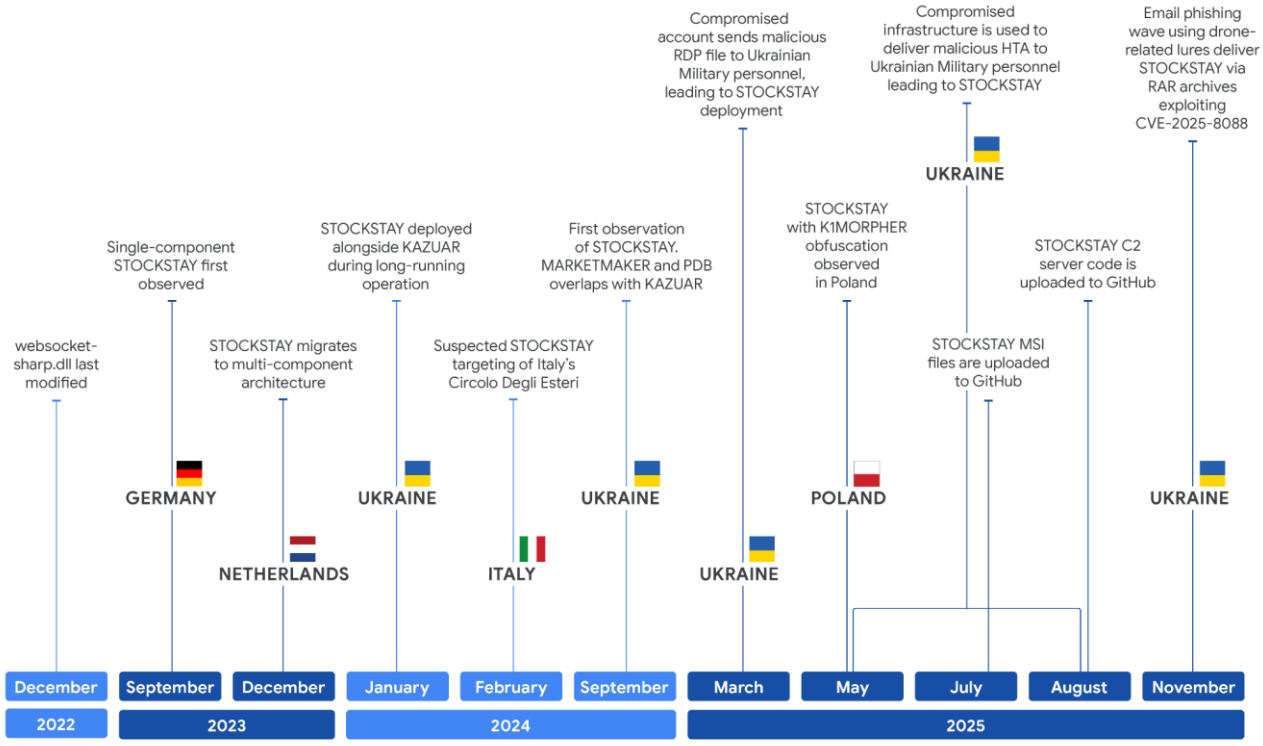
**Míra úspěšnosti modelu Mythos v odhalení zranitelnosti v prohlížeči Firefox ve srovnání s předchozími modely společnosti Anthropic** (vellum.ai)



## Google atribuoval backdoor STOCKSTAY ruskému státnímu aktérovi Turla

Kyberbezpečnostní experti Google Threat Intelligence Group (GTIG) atribuovali dosud nezdokumentovaný backdoor STOCKSTAY ruskému státem sponzorovanému aktérovi Turla (též známému jako Venomous Bear nebo Secret Blizzard), který je spojován s ruskou zpravodajskou službou s vnitřní působností FSB. Tento kyberšpionážní malware byl zaznamenán už v roce 2022, přičemž se vyskytl v různých evropských zemích (Německo, Polsko, Itálie), ale v posledním roce byl opakovaně nasazován zejména na Ukrajině. Zde byl šířen pomocí phishingu mířícího na vládní a vojenské instituce, maskovaného jako diplomatická či akademická komunikace. STOCKSTAY obsahuje několik komponent, které vzájemně komunikují přes vlastní (IPC) kanál. Tyto komponenty se dokázaly skrývat jako neškodné programy, např. jako blíže nespecifikovaný nástroj pro hledání údajů na burze.

**Časová osa výskytu backdooru STOCKSTAY**




## Loňský výpadek telekomunikací v Lucembursku způsobila zero-day zranitelnost v routerech Huawei

Plošný výpadek telekomunikačních sítí v Lucembursku, ke kterému došlo v červenci 2025, způsobilo zneužití zero-day zranitelnosti v routerech Huawei. Narušena byla telekomunikační infrastruktura, a to včetně pevné linky, 4G, 5G i nouzové komunikace na více než tři hodiny. Útočníci použili speciálně vytvořený síťový provoz, kvůli kterému se routery Huawei opětovně restartovaly, čímž vyřadily klíčové části telekomunikační infrastruktury společnosti Post Luxembourg. Lucembursko původně označilo výpadek za mimořádně pokročilý kybernetický útok a později upřesnilo, že nešlo o typický DDoS útok. Důkazy rovněž nenaznačovaly konkrétní záměr namířený proti společnosti Post či Lucembursku. Společnost Huawei nezveřejnila zmíněnou zranitelnost, ale uvedla, že nebyla znovu zneužita.

# 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.

## NÚKIB se jako součást polsko-českého týmu umístil na 4. místě největšího kyberobranného cvičení Locked Shields 2026

Národní úřad pro kybernetickou a informační bezpečnost se ve dnech 21.–24. dubna 2026 zúčastnil prestižního mezinárodního kybernetického cvičení Locked Shields 2026, které je považováno za největší a nejkomplexnější kybernetické obranné cvičení na světě. Cvičení každoročně pořádá NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Polsko-český tým nakonec mezi šestnácti týmy vybojoval čtvrté místo.

Hlavním cílem cvičení Locked Shields 2026 bylo posílení a další rozvoj schopností kybernetické obrany zúčastněných států, podpora mezinárodního partnerství a spolupráce mezi veřejným a soukromým sektorem, stejně jako podpora inovací v oblasti kybernetické bezpečnosti.

Cvičení simulovalo rozsáhlý a realistický kybernetický konflikt v reálném čase a prověřovalo technické, operační i strategické schopnosti účastníků. Fiktivní scénář cvičení zahrnoval prvky geopolitického napětí, včetně porušování mezinárodních hranic a státní suverenity, výstavby umělých ostrovů i koordinovaných kybernetických útoků, které měly dopad na fungování státu i důvěru veřejnosti. Letos tvůrci do scénáře zařadili i problematiku zabezpečení voleb.


## Ředitel NÚKIB Lukáš Kintr jednal v Estonsku o posílení kybernetické spolupráce

Jako součást prezidentské delegace navštívil Estonsko v rámci červnové státní návštěvy ředitel NÚKIB Lukáš Kintr. Během dvoudenního programu v Tallinnu a Tartu proběhla řada jednání se strategickými partnery z veřejného, soukromého i akademického sektoru, která potvrdila silné a dlouhodobé partnerství obou zemí v oblasti kybernetické bezpečnosti a otevřela prostor pro jeho další prohloubení.

Jedním z klíčových bodů programu bylo jednání s e-Governance Academy (eGA), dlouhodobým partnerem České republiky v oblasti digitální transformace a kyberbezpečnosti. Jednání se zaměřilo zejména na další rozvoj projektů v oblasti budování kybernetických kapacit, včetně iniciativ jako Cyber Balkans 2 či projektů v rámci NATO Cyber Defence Capacity Building.

Další bilaterální jednání v Tallinnu proběhla se zástupci Státního úřadu pro informační systémy (RIA), kde se diskutovaly národní priority, aktuální výzvy v oblasti kybernetické bezpečnosti i rostoucí hrozby online podvodů. Delegace se zúčastnila také odborného setkání kybernetických expertů na půdě Univerzity v Tartu. Diskuse se zaměřily na spolupráci ve výzkumu a vývoji, propojení průmyslu s akademickou sférou i zkušenosti ze studentských výměnných programů.

## 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. |