Vydali jsme Čtvrtletní přehled hrozeb pohledem NÚKIB - Q3/2025

24.10.2025 - | Národní úřad pro kybernetickou a informační bezpečnost

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) vydal třetí čtvrtletní report věnovaný nejen evidovaným incidentům, ale také širšímu kontextu hrozeb relevantních pro Českou republiku či dlouhodobějším trendům. Třetí čtvrtletí roku 2025 se neslo ve znamení zvýšené aktivity proruských hacktivistických skupin, nárůstu počtu kybernetických incidentů a mezinárodní spolupráce v oblasti kybernetické bezpečnosti.

V uplynulém čtvrtletí NÚKIB vydal dvě varování. První se věnovalo hrozbě před některými produkty společnosti DeepSeek, druhé pak hrozbě spočívající v předávání dat a ve výkonu vzdálené správy z Čínské lidové republiky. NÚKIB se také spolu s americkými a dalšími mezinárodními partnery zapojil do společné analýzy aktivit čínského aktéra Salt Typhoon, který kompromituje sítě po celém světě. Report se také věnuje mezinárodní operaci Eastwood nebo nové zranitelnosti v Microsoft SharePoint.

Z pohledu kybernetických bezpečnostních incidentů se třetí čtvrtletí vyznačovalo zvýšeným počtem incidentů ve srovnání se dvěma předchozími kvartály. 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).

NÚKIB dlouhodobě sleduje kybernetické hrozby, které sice nemají bezprostřední dopad na Českou republiku, ale mohou ovlivnit její bezpečnost v budoucnu. V uplynulém čtvrtletí se jednalo například o skupinu Secret Blizzard (Turla) napojenou na ruskou FSB, která od roku 2024 provádí kyberšpionáž proti zahraničním ambasádám v Moskvě, ransomwarový útok, který vedl k narušení provozu na řadě evropských letišť, či ruskou kyberšpionážní skupinu Static Tundra.

Zajišťování kybernetické bezpečnosti není jen technické řešení incidentů, ale také aktivní spolupráce, sdílení zkušeností a informací mezi odborníky napříč sektory. Významnou událostí byl 11. ročník konference CYBER_CON 2025, pořádaný NÚKIB ve spolupráci s partnery. Konference nabídla prostor pro diskusi o aktuálních výzvách v kyberbezpečnosti, včetně nové Národní strategie a legislativních změn. Česká republika se také aktivně zapojila do mezinárodních aktivit – v září převzala štafetu pro pořádání NATO Cyber Champions Summit 2026. Delegace vedená NÚKIB se v Jižní Koreji účastnila řady konferencí, včetně cvičení APEX 2025, kde čeští experti spolupracovali s týmy z Jižní Koreje a Norska. Mezinárodní spolupráce je klíčovým prvkem efektivní obrany proti kybernetickým útokům.

Celý dokument naleznete zde:
https://nukib.gov.cz/download/publikace/vyzkum/Ctvrtletni%20prehled%20hrozeb%20pohledem%20NUKIB_Q3%202025.pdf

https://nukib.gov.cz/cs/infoservis/aktuality/2321-vydali-jsme-ctvrtletni-prehled-hrozeb-pohledem-nukib-q3-2025