Vydali jsme čtvrtletní přehled hrozeb NÚKIB - Q2 2026

24.7.2026 - | Národní úřad pro kybernetickou a informační bezpečnost

Ve druhém čtvrtletí roku 2026 evidoval NÚKIB celkem 44 kybernetických incidentů, což představuje nejnižší hodnotu za poslední rok a téměř poloviční pokles oproti předchozímu čtvrtletí. Šest incidentů bylo vyhodnoceno jako významných, avšak nebyl zaznamenán žádný velmi významný incident. Výrazně ubylo DDoS útoků, které byly na začátku roku spojovány zejména s aktivitami proruských hacktivistických skupin. Naopak nejčastěji spadaly incidenty do kategorie Průnik, zahrnující kompromitace účtů, firewallů či serverů, především ve veřejné správě, školství a zdravotnictví.

Mezi nejvýznamnější události čtvrtletí patřilo odhalení rozsáhlé operace ruského státního aktéra, který zneužíval zranitelnost v routerech TP-Link a budoval síť kompromitovaných zařízení určenou pro kyberšpionáž. Do mezinárodní operace vedené Spojenými státy se zapojilo i české Vojenské zpravodajství. Významnou pozornost vzbudila také kampaň Fortibleed zaměřená na zařízení společnosti Fortinet. Útočníci získali přístupové údaje téměř k polovině veřejně dostupných firewallů Fortinet vystavených do internetu a mezi zasaženými organizacemi se objevily i české subjekty.

Další sledovaný případ se týkal čínského kyberšpionážního aktéra, který se pokusil kompromitovat český think-tank Evropské hodnoty prostřednictvím cíleného phishingového útoku. Případ ukázal, že zájmovým cílem státních aktérů nemusí být pouze státní instituce, ale také neziskové organizace.

NÚKIB upozorňuje na rychlý rozvoj pokročilých modelů umělé inteligence. Nové generace AI, například model Mythos společnosti Anthropic, podle úřadu výrazně zvyšují schopnost automaticky vyhledávat, ověřovat a zneužívat zranitelnosti. To může zkrátit čas mezi objevením zranitelnosti a jejím zneužitím, zatímco tempo oprav zůstává omezené lidskými a technickými kapacitami organizací. NÚKIB proto považuje za pravděpodobné, že nové AI nástroje v budoucnu přispějí k růstu počtu kybernetických incidentů, ať už přímo, nebo prostřednictvím útoků na dodavatelské řetězce.

Přehled dále upozorňuje na nově odhalený kyberšpionážní malware STOCKSTAY, který je spojován s aktérem podporovaným ruským státem, a informuje o nových souvislostech loňského rozsáhlého výpadku telekomunikačních služeb v Lucembursku způsobeném zneužitím zero-day zranitelnosti v routerech Huawei.

Celý dokument naleznete zde:
https://nukib.gov.cz/download/publikace/vyzkum/Ctvrtletni-prehled-hrozeb-pohledem-NUKIB-Q2-2026.pdf