Vydali jsme čtvrtletní přehled hrozeb NÚKIB - Q1 2026

22.4.2026 - | Národní úřad pro kybernetickou a informační bezpečnost

V prvním čtvrtletí roku 2026 zaznamenal Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) výrazný nárůst kybernetických incidentů, který způsobila především lednová vlna DDoS útoků vedených proruskými hacktivistickými skupinami a relativně vysoký počet incidentů v kategorii Průnik. Celkem bylo evidováno více než 70 incidentů, což představuje nejvyšší hodnotu za posledních dvanáct měsíců. S celkovým počtem incidentů mírně vzrostla také jejich závažnost. NÚKIB evidoval celkem sedm významných incidentů, ostatní byly méně závažné.

Ve sledovaném období nebyl zaznamenán žádný ransomwarový útok u subjektů v režimu vyšších povinností spadajících pod působnost NÚKIB; případy tohoto typu se však týkaly subjektů v režimu nižších povinností, jejichž řešení koordinuje Národní CERT (CSIRT.CZ).

NÚKIB v lednu upozornil na zvýšenou aktivitu proruských hacktivistických aktérů, která se projevila vlnou DDoS útoků a zvýšeným zájmem útočníků o útoky na VNC rozhraní PLC zařízení se slabými nebo žádnými hesly a zneužívání dalších provozovaných služeb otevřených do internetu. V obou případech neměly aktivity výraznější dopady na české subjekty.

S nedostatečně zabezpečenými VNC službami vystavenými do internetu souviselo také březnové upozornění, kdy v daném období došlo k výraznému nárůstu počtu zařízení kompromitovaných botnetem REDHEBERG na území České republiky. V době psaní Čtvrtletního přehledu hrozeb pohledem NÚKIB bylo v České republice stále evidováno přes 3200 kompromitovaných zařízení.

Do situačního přehledu kybernetických hrozeb, které nemají bezprostřední dopad na bezpečnost České republiky, ale mohou mít přímý či nepřímý vliv na kyberbezpečnost českých subjektů, v prvním čtvrtletí spadá globální kyberšpionážní kampaň vedená přes aplikaci Signal, rozsáhlé využívání pokročilého nástroje pro kompromitaci zařízení iPhone označovaného jako Coruna nebo kyberšpionážní spear-phishingová kampaň proti evropským státům zneužívající zranitelnost v softwaru Microsoft Office.

Co se týká spolupráce a sdílení informací, v březnu se uskutečnily hned dvě mezinárodní kyberbezpečnostní akce. První z nich, NATO Cyber Champions Summit, se zúčastnili seniorní představitelé spojeneckých zemí NATO a klíčových partnerů z indo-pacifického regionu s cílem posílit mezinárodní spolupráci v oblasti kybernetické bezpečnosti a obrany. Na tuto akci navazovala Prague Cyber Security Conference 2026, která potvrdila svou roli významné evropské platformy pro strategickou debatu o kybernetické bezpečnosti.

Celý dokument naleznete zde:
https://nukib.gov.cz/download/publikace/vyzkum/2026-Ctvrtletni-prehled-hrozeb_Q1.pdf

https://nukib.gov.cz/cs/infoservis/aktuality/2399-vydali-jsme-ctvrtletni-prehled-hrozeb-nukib-q1-2026