NÚKIB vydal Zprávu o stavu kybernetické bezpečnosti ČR za rok 2025. Incidentů ubylo, sofistikovanost útočníků roste

21.8.2026 - | Národní úřad pro kybernetickou a informační bezpečnost

Vláda České republiky dne 17. srpna 2026 vzala na vědomí Zprávu o stavu kybernetické bezpečnosti České republiky za rok 2025, kterou každoročně zpracovává Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Dokument shrnuje vývoj kybernetických hrozeb, incidentů a klíčových trendů v oblasti kybernetické bezpečnosti v České republice. Vychází přitom z poznatků NÚKIB, dotazníkového šetření mezi regulovanými a významnými organizacemi, informací partnerských institucí a z veřejně dostupných zdrojů. Přestože po třech letech došlo k poklesu celkového počtu evidovaných kybernetických incidentů, jejich sofistikovanost vzrostla a Česká republika i nadále čelí aktivitám státních i kriminálních aktérů.

NÚKIB v roce 2025 evidoval celkem 203 kybernetických incidentů, což je o 65 méně než v roce předchozím. Nejvýrazněji poklesl počet incidentů souvisejících s DDoS útoky hacktivistických skupin. Z pohledu závažnosti počet velmi významných kybernetických incidentů, které mohou mít zásadní dopady na fungování institucí a poskytování služeb občanům, vzrostl z jednoho na dva, zatímco počet významných bezpečnostních incidentů se snížil z 18 na 12.

„Pokles počtu incidentů rozhodně neznamená, že by se kybernetické prostředí stávalo bezpečnějším. Naopak sledujeme pokračující trend rostoucí sofistikovanosti útočníků a nárůst závažnosti některých incidentů. Kybernetická bezpečnost proto zůstává jednou z důležitých podmínek fungování moderního státu i společnosti," uvedl ředitel NÚKIB Lukáš Kintr.

Nejčastějším typem incidentů zůstaly útoky zaměřené na dostupnost systémů, které tvořily 46 % všech případů. Z pohledu organizací byl nejrozšířenější hrozbou phishing. Devět z deseti respondentů dotazníkového šetření uvedlo, že se s phishingovými útoky v roce 2025 setkalo. Organizace zároveň upozorňovaly na rostoucí sofistikovanost těchto útoků a možné využívání nástrojů umělé inteligence při jejich přípravě. Přesto více než třetina organizací své zaměstnance vůči podobným hrozbám vůbec netestovala.

Významnou kapitolou uplynulého roku byly aktivity státních aktérů. Česká vláda v květnu 2025 vůbec poprvé veřejně provedla národní atribuci škodlivé kybernetické kampaně vedené proti Ministerstvu zahraničních věcí. Na základě šetření českých bezpečnostních institucí byla tato dlouhodobá kampaň připsána skupině APT31 napojené na Čínskou lidovou republiku. Česká republika zároveň v průběhu roku spolupracovala s mezinárodními partnery na odhalování aktivit dalších čínských a ruských aktérů působících v kyberprostoru.

Rok 2025 byl přelomový také z pohledu legislativy. Dne 1. listopadu nabyl účinnosti nový zákon o kybernetické bezpečnosti, který do českého právního řádu promítá požadavky evropské směrnice NIS2 a významně rozšiřuje počet regulovaných subjektů. Současně byl spuštěn nový Portál NÚKIB, který slouží jako centrální místo pro komunikaci regulovaných organizací s úřadem a plnění jejich zákonných povinností.

NÚKIB během roku vydal dvě významná varování. První se týkalo některých produktů společnosti DeepSeek. Druhé upozorňovalo na hrozbu spočívající v předávání dat a výkonu vzdálené správy z

Čínské lidové republiky. Toto varování představovalo nový přístup, protože není zaměřené na jednu technologii, ale upozorňuje na komplexní problém a je uplatnitelné na všechna odvětví, služby i zařízení.

Zpráva dále upozorňuje na pokračující růst kyberkriminality. V roce 2025 bylo v České republice evidováno 21 137 trestných činů v oblasti kyberkriminality a kriminality páchané prostřednictvím internetu, což představuje meziroční nárůst o 14 %. Mezi nejčastější formy patřily podvody využívající sociální inženýrství a manipulaci obětí.

Mezi pozitivní zjištění patří pokračující růst investic do kybernetické bezpečnosti. Více než polovina oslovených organizací uvedla, že svůj rozpočet na kybernetickou bezpečnost v roce 2025 navýšila, a 54 % respondentů považuje prostředky vyčleněné na tuto oblast za dostatečné. Nadále však přetrvává nedostatek kvalifikovaných odborníků. Nejčastější překážkou při jejich získávání je podle organizací nedostatečné finanční ohodnocení.

Součástí dokumentu je také výhled na roky 2026 a 2027. NÚKIB upozorňuje například na rizika zneužívání komunikačních platforem pro šíření škodlivého obsahu a kyberšpionáž či na možný vývoj v oblasti umělé inteligence a jejího vlivu na bezpečnostní prostředí.

Celá Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2025 je dostupná zde: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava-o-stavu-kyberneticke-bezpecnosti-CR-za-rok-2025.pdf

https://nukib.gov.cz/cs/infoservis/aktuality/2453-nukib-vydal-zpravu-o-stavu-kyberneticke-bezpecnosti-cr-za-rok-2025-incidentu-ubylo-sofistikovanost-utocniku-roste