NÚKIB vydal Zprávu o stavu kybernetické bezpečnosti České republiky za rok 2024

22.8.2025 - | Národní úřad pro kybernetickou a informační bezpečnost

Významnou část evidovaných incidentů tvořily DDoS útoky. Za většinou z nich stály ruskojazyčné hacktivistické skupiny, zejména NoName057(16), jejíž škodlivé aktivity však nadále nepůsobily zasaženým cílům škody nad rámec krátkodobých výpadků napadených webů. Nově zaznamenaným trendem byl nárůst počtu hacktivistických skupin, které cílily na slabě zabezpečené systémy operačních technologií a SCADA systémy průmyslových podniků v západních zemích. Přestože sofistikované kampaně státních aktérů spojovaných s Ruskou federací nebo Čínskou lidovou republikou tvoří velmi malé procento celkového počtu incidentů, jejich závažnost je obvykle vysoká.

V roce 2024 i nadále přetrvávala hrozba ransomwarových útoků ze strany kyberkriminálních skupin. V posledním čtvrtletí loňského roku došlo k jejich strmému nárůstu a v říjnu 2024 jich NÚKIB zaregistroval 7, což je nejvyšší evidovaný počet za měsíc. Hactivistické skupiny cílily primárně na instituce veřejného sektoru, kdežto kyberkriminální skupiny spíše na soukromé společnosti s cílem získat finanční prostředky.

Dlouhodobým pozitivním trendem v posledních třech letech je navyšování rozpočtů alokovaných na kybernetickou bezpečnost organizací. To může značit jak mírně se zlepšující finanční situaci organizací, tak i jejich rostoucí porozumění důležitosti ochrany před kybernetickými hrozbami a důraz na kybernetickou bezpečnost. Jako problematický se ukazuje nedostatek kvalifikovaných odborníků v kyberbezpečnosti.

Rok 2024 byl zlomový pro návrh nového zákona o kybernetické bezpečnosti. Jeho návrh projednala Legislativní rada vlády, poté ho vláda schválila a postoupila jej Poslanecké sněmovně Parlamentu České republiky. V Poslanecké sněmovně byl zákon projednán ve Výboru pro bezpečnost, Výboru pro obranu a v Hospodářském výboru. K návrhu zákona byly ve výborech a při druhém čtení načteny pozměňovací návrhy. V současné chvíli je legislativní proces téměř dokončen, a zákon čeká pouze poslední krok, kterým je nabytí účinnosti právní úpravy, k čemuž dojde 1. listopadu 2025.

NÚKIB se v minulém roce aktivně zapojoval do vyjednávání nařízení o kybernetické odolnosti, které představuje průlomovou unijní legislativu. Její cíl je zvýšit bezpečnost pomocí zavedení požadavků na kybernetickou bezpečnost softwarových a hardwarových produktů. V roce 2024 NÚKIB dále dokončil přípravu návrhu Národní politiky koordinovaného zveřejňování zranitelností, jejímž cílem je podporovat nalézání zranitelností v ICT produktech napříč subjekty v ČR bez hrozby negativních právních dopadů pro objevitele zranitelností.

V roce 2024 NÚKIB ve spolupráci s partnery pokračoval v práci na projektu BIVOJ (Bezpečný, Inovativní, pro Veřejnou správu, Odolný, Jednotný). Cílem projektu je vytvoření jednotné, funkční a bezpečné sdílené platformy poskytující bezpečnostní a komunikační služby, do které budou postupně připojeny instituce veřejného sektoru.

V roce 2024 NÚKIB provedl 22 auditů a kontrol podle zákona o kybernetické bezpečnosti. Nad rámec běžných kontrolních činností se NÚKIB stejně jako v předchozích letech věnoval také metodické podpoře především u povinných subjektů formou odpovídání na dotazy, vydávání podpůrných materiálů a provádění auditů u vybraných subjektů.

Každoroční zpráva o stavu kybernetické bezpečnosti neposkytuje vyčerpávající seznam všech aktivit v oblasti kybernetické bezpečnosti. Účelem dokumentu je popsat a vyhodnotit hrozby v kybernetickém prostoru, s nimiž se ČR v roce 2024 potýkala, stejně jako aktivity, které napomáhají jejich zmírnění.

https://nukib.gov.cz/cs/infoservis/aktuality/2291-nukib-vydal-zpravu-o-stavu-kyberneticke-bezpecnosti-ceske-republiky-za-rok-2024