

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **130** ze dne **13.1.2026**

Počet kyberútoků na české společnosti meziročně klesl, přesto ČR nepatří mezi bezpečné země

Výzkumný tým společnosti Check Point zveřejnil zprávu Global Threat Intelligence Report, z níž vyplývá, že v listopadu čelila každá společnost v průměru 2 003 kybernetickým útokům týdně. Oproti říjnu jde o nárůst o 3 %. Zároveň výrazně vzrostl počet společností vydíraných ransomwarovými gangy.

"V České republice čelila každá společnost v průměru 2 025 kyberútokům týdně, což je meziroční pokles o 11 %. Přesto i nadále patří Česko mezi nejčastěji napadané evropské země. Evropský průměr je totiž 1 638 útoků na jednu společnost za týden. Většímu počtu útoků než ČR čelí například Portugalsko (2 215 kyberútoků týdně na jednu společnost), Itálie (2 291), Izrael (2 109) a Norsko (2 027). Vysoké riziko hrozí i ve Španělsku (1 940) nebo Švédsku (1 906). Naopak klidnější je situace v Německu (1 161), Francii (1 099), Švýcarsku (1 072) nebo Polsku (1 788). Vůbec nejmenšímu riziku čelí v Evropě finské společnosti (859 kyberútoků týdně na jednu organizaci). Naopak největší meziroční nárůst útoků (o 48 %) jsme zaznamenali v Řecku," řekl Tomáš Růžička, SE team leader z kyberbezpečnostní společnosti Check Point Software Technologies.

Nejčastějším terčem jsou s obrovským náskokem vzdělávací instituce s průměrným počtem 4 656 útoků týdně na jednu organizaci, což je meziroční nárůst o 7 %. Na druhém místě jsou vládní instituce, které zaznamenaly 2 716 útoků týdně (+2 % meziročně), těsně následované asociacemi a neziskovými organizacemi s 2 550 útoky týdně na jednu společnost, což představuje výrazný meziroční nárůst o 57 %. Tento prudký nárůst útoků je důkazem, že kyberzločinci se stále častěji zaměřují na odvětví s omezenými zdroji na bezpečnost, ale s vysoce cennými daty a veřejně dostupnými digitálními službami.

Největší počet útoků zaznamenaly organizace v Latinské Americe (3 048 útoků týdně na jednu organizaci), což je meziroční nárůst o 17 %. Naopak africké společnosti zaznamenaly pokles útoků o 13 %. V Evropě je celkový počet kyberútoků bez větších výkyvů a jedna evropská společnost čelí v průměru 1 638 kyberútokům týdně.

Nárůst rizik spojených s použitím generativní umělé inteligence

Nárůst obliby generativních AI nástrojů (GenAI) s sebou přináší i významná rizika úniku dat. V listopadu Check Point zjistil, že každý 35. prompt představoval vysoké riziko úniku citlivých dat, což mělo dopad na 87 % organizací, které GenAI pravidelně používají. Dalších 22 % promptů obsahovalo potenciálně citlivé informace, jako jsou interní komunikace, podniková data, proprietární kód nebo osobní údaje.

Organizace používají v průměru 11 různých GenAI nástrojů, z nichž většina pravděpodobně není pod dohledem a funguje mimo bezpečnostní rámec. Zvyšuje se tak pravděpodobnost náhodného úniku dat, což by mohlo kyberzločincům usnadnit napadení organizace.

Nárůst vyděračských útoků o 22 %

V listopadu došlo k dalšímu nárůstu ransomwarových útoků. Celkem bylo veřejně vydíráno 727 společností, což je meziroční nárůst o 22 %. Nejvíce útoků bylo v Severní Americe, 18 % obětí pochází z Evropy. Jedná se zejména o tlak na kritickou infrastrukturu a obchodní služby.

MEATEST spol. s r.o. - sdělení pověřence pro ochranu osobních údajů číslo **130** ze dne **13.1.2026**

Přes 12 % obětí bylo z oblasti průmyslové výroby. Útočníci se často snaží zneužívat zastaralé systémy. 11 % vydíraných společností se zaměřovalo na obchodní služby a 10 % obětí bylo ze sektoru spotřebního zboží a služeb. 8 % obětí bylo ze zdravotnictví, což znovu ukazuje, že kyberzločinci se chladnokrevně a vypočítavě snaží zneužívat i nejcitlivější místa společnosti.

Nejaktivnějšími ransomwarovými skupinami byly v listopadu Qilin a Clop (obě mají na svědomí 15 % vydíraných organizací), následovala skupina Akira (12 % vydíraných společností).

AV centrum ČR