

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **109** ze dne **3.6.2025**

Dramaticky roste hrozba e-mailových útoků s využitím personalizovaných taktik na bázi AI

Společnost Acronis vydala svou pololetní zprávu Acronis Cyberthreats Report, H2 2024: The rise of AI-driven threats, která odhaluje výrazný nárůst kybernetických e-mailových útoků – ve druhé polovině roku 2024 byl zjištěn ohromující nárůst o téměř 200 % v porovnání se stejným obdobím roku 2023. Od července do prosince 2024 se téměř 50 % oslovených uživatelů stalo alespoň jednou terčem e-mailového útoku.

"Aktuální vydání upozorňuje na znepokojivý nárůst útoků generovaných umělou inteligencí a rostoucí sofistikovanost ransomwarových kampaní," řekl Gerald Beuchelt, CISO ve společnosti Acronis.

Zvýšil se také počet e-mailových útoků na poskytovatele řízených služeb (MSP). Není překvapením, že preferovaným vektorem útoku, kterým útočníci pronikali do sítí MSP, byl phishing – e-mailové phishingové kampaně zažilo 33 % z nich. Těsně za nimi následovalo zneužití protokolu RDP (Remote Desktop Protocol) a dalších nástrojů pro vzdálený přístup. To ukazuje, jak kyberzločinci využívají běžné MSP nástroje k získání neoprávněného přístupu a nasazení škodlivého malwaru.

Mezi klíčová zjištění aktuálního Acronis Cyberthreats Reportu patří:

- Počet e-mailových útoků odhalených ve druhé polovině roku 2024 vzrostl o 197 % ve srovnání s druhou polovinou roku 2023, zatímco průměrný počet útoků na jednu organizaci ve stejném časovém období vzrostl o 21 %.
- Ze všech typů e-mailových útoků je dominantní phishing se 74% podílem.
- V roce 2024 útočníci využívali personalizované taktiky a strategie řízené umělou inteligencí, aby zneužili zranitelnosti a požadovali vyšší výkupné. Tento trend odráží posun k sofistikovanějším útokům velkého rozsahu, jejichž cílem je maximalizovat dopady útoků a finanční zisk.
- 31,4 % všech e-mailů přijatých ve 2. pololetí 2024 tvořil spam, přičemž 1,4 % obsahovalo malware nebo phishingové odkazy.
- V roce 2024 došlo k 5% nárůstu útoků ransomwaru (bylo nahlášeno 1 712 případů napadení ransomwarem), přičemž mnohé z nich byly zaměřeny konkrétně na MSP poskytovatele a kritická odvětví, jako je doprava, zdravotnictví a výroba.

Zpráva upozorňuje na další zajímavý trend: s tím, jak se stále více rozšiřuje využití nástrojů pro vzdálené monitorování a správu (RMM), přinášejí kromě vyšší efektivity bohužel také významná rizika pro bezpečnost organizací. Telemetrické údaje Acronis odhalují, že mnoho organizací používá několik nástrojů RMM současně, což vytváří slepá místa, která mohou útočníci využít. Bez náležitých kontrolních mechanismů se nástroje RMM mohou stát vstupními body pro útoky ransomwaru, které kyberzločinci často využívají k napáchání ještě větších škod.

Zdroj: AVcentrum ČR