

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **81** ze dne **5.9.2024**

Průzkum Acronis hlásí 293% nárůst e-mailových útoků

Zpráva Acronis Cyberthreats Report H1 2024 zjistila, že e-mailové útoky zaznamenaly 293% nárůst ve srovnání se stejným obdobím roku 2023. Rostl také počet detekovaných ransomwarových útoků, který od 4. čtvrtletí 2023 do 1. čtvrtletí 2024 narostl o 32 %.

Zpráva Acronis Cyberthreats Report H1 2024 využívá data z více než milionu unikátních koncových bodů po celém světě, aby získala přehled o globálních trendech v oblasti kybernetické bezpečnosti.

Ransomware nadále představuje velkou hrozbu pro malé a střední podniky (SMB), zejména v kritických odvětvích, jako jsou státní správa a zdravotnictví. V 1. čtvrtletí 2024 zaznamenala společnost Acronis deset nových skupin ransomwaru, které si dohromady připsaly 84 kybernetických útoků po celém světě. Mezi deseti nejaktivnějšími rodinami ransomwaru, které byly v tomto období zjištěny, vynikají především tři vysoce aktivní skupiny, které jsou dohromady zodpovědné za 35 % útoků: LockBit, Black Basta a PLAY.

Zpráva si zejména všímá, jakým způsobem jsou napadáni a ohrožováni poskytovatelé řízených služeb (MSP). Jako nejúspěšnější techniky používané k prolomení kybernetické ochrany MSP byly označeny phishing a sociální inženýrství, zneužití zranitelností, zneužití přístupových údajů a útoky na dodavatelské řetězce (supply chain).

"V důsledku rostoucí kvantity a komplexnosti kybernetických hrozeb, které v současném prostředí kybernetické bezpečnosti stále odhalujeme, je nanejvýš důležité, aby MSP zaujali systematický přístup k zabezpečení dat, systémů a digitálních infrastruktur svých zákazníků," uvedla Irina Artioli, autorka zprávy a expertka na kybernetickou ochranu v divizi Acronis Threat Research Unit. "Aby byl efektivní, doporučujeme MSP přijmout komplexní bezpečnostní strategii, včetně povinných školení o bezpečnostních hrozbách a plánování reakce na incidenty. A rovněž nasadit pokročilá řešení ochrany koncových bodů, jako je rozšířená detekce a reakce (XDR), vícefaktorová autentizace a další."

Kromě toho se zpráva zaměřuje na nové trendy v oblasti kybernetické bezpečnosti a zdůrazňuje rostoucí využívání generativní umělé inteligence (AI) a velkých jazykových modelů (LLM). Konkrétně zdůrazňuje AI, která je využívána při útocích sociálního inženýrství a automatizaci. Mezi nejčastější útoky generované umělou inteligencí patří škodlivé e-maily, deepfake podvody elektronické pošty (BEC), deepfake vydírání, obcházení KYC ověřování a generování skriptů a malwaru.

- **Mezi další klíčová zjištění zprávy patří:**

- E-mailová komunikace
- Organizace zaznamenaly prudký nárůst e-mailové komunikace, přičemž počet e-mailů na organizaci vzrostl o 25 %.
- Počet e-mailových útoků zjištěných v první polovině roku 2024 vzrostl o 293 % ve srovnání s první polovinou roku 2023.
- 27,6 % všech přijatých e-mailů byl spam a 1,5 % obsahovalo malware nebo phishingové odkazy.

MEATEST spol. s r.o. - sdělení pověřence pro ochranu osobních údajů číslo **81** ze dne **5.9.2024**

- Ransomware
 - V 1. čtvrtletí 2024 bylo na sledovaných koncových bodech zablokováno 28 milionů URL adres.
 - V 1. čtvrtletí 2024 bylo veřejně nahlášeno 1 048 případů ransomwaru, což představuje 23% nárůst oproti 1. čtvrtletí 2023.
 - V prvním čtvrtletí roku 2024 výzkumníci společnosti Acronis zaznamenali deset nových skupin ransomwaru, které si dohromady vyžádaly 84 kybernetických útoků po celém světě.
 - Počet detekcí ransomwaru se od 4. čtvrtletí 2023 do 1. čtvrtletí 2024 zvýšil o 32 %.
- Útoky na MSP
 - Útoky na MSP probíhaly soustavně od ledna do května 2024, přičemž data odhalila, že útočníci nejčastěji využívali e-mailové phishingové kampaně.
 - Phishingové útoky tvořily 30 % všech útoků, 24 % pak útoky přes vzdálený protokol (RDP), 23 % neošetřené zranitelnosti a 15 % zneužití přístupových údajů.
 - S pokusy o phishing využívající škodlivých URL adres se setkala 26 % uživatelů.
- Útoky s podporou AI
 - Kyberzločinci nadále využívají škodlivé nástroje AI jako WormGPT a FraudGPT.
 - Umělá inteligence může útočníkům pomáhat v každé fázi kybernetického útoku, lze ji však využít i jako obranný mechanismus, protože umožňuje nepřetržitou detekci útoků a jejich hlášení bezpečnostním expertům schopným reagovat vhodnými opatřeními k zajištění kontinuity provozu.

Zdroj: AVcentrum ČR