

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **151** ze dne **5.8.2026**

Téměř osm tisíc obětí ransomwaru za rok 2025: "kvantoví" útočníci sbírají šifrovaná data už dnes.

Počet potvrzených obětí ransomwaru se v roce 2025 podle Fortinetu vyšplhal na 7 831, což dokládá, jak rychle se kyberkriminalita industrializuje a jak agresivně útočníci dnes shromažďují a zneužívají citlivá data. Součástí trendu je i strategie "sbírej teď, dešifruj později", při které útočníci zachycují a ukládají aktuální data s cílem dešifrovat je až ve chvíli, kdy budou k dispozici dostatečně výkonné kvantové počítače.

"Zatímco takzvaný ‚Den Q‘ může být ještě několik let vzdálený, hrozba kvantových počítačů pro zabezpečení dat je již tady. Útočníci hromadně zachycují a ukládají dnes zašifrovaná vysoce hodnotná data. Čekají, až budou k dispozici dostatečně výkonné kvantové počítače, které jim umožní tato data dešifrovat a získat z nich citlivé informace," vysvětlil Ondřej Šťáhlavský, regionální seniorní ředitel společnosti Fortinet pro střední a východní Evropu.

Předpokládá se, že kvantové počítače prolomí dnešní šifrovací standardy během následujících deseti let. Podle Fortinetu je riziko obzvláště vysoké pro organizace uchovávající data, která musí zůstat důvěrná po mnoho let – například ve finančním sektoru, v telekomunikacích, obraně nebo státní správě. Ohrožena jsou také zdravotnická data a duševní vlastnictví, protože si musí zachovat důvěrnost po dlouhou dobu. Právě proto představují ideální cíl pro strategii "sbírej teď, dešifruj později".

Fortinet zdůrazňuje, že přechod na post-quantovou kryptografii (PQC) trvá řadu let, a proto je nutné začít s přípravou výrazně dříve, než se kvantové útoky stanou běžnou realitou. Odkládání této změny zvyšuje riziko, že data zachycená dnes bude možné v budoucnu dešifrovat. Fortinet proto doporučuje organizacím začít budovat kvantovou odolnost už nyní prostřednictvím několika technologických přístupů integrovaných přímo do síťové infrastruktury:

- Post-quantová kryptografie (PQC) s algoritmy schválené organizací NIST, jako jsou ML-KEM, doplněnými o algoritmy BIKE, HQC a Frodo.
- Quantum Key Distribution (QKD) pro bezpečnou výměnu kryptografických klíčů s možností detekce odposlechu.
- Algorithm stacking, tedy vrstvení více kryptografických algoritmů pro vyšší odolnost.
- Hybridní režim, který kombinuje klasickou kryptografii s post-quantovými metodami a umožňuje plynulý přechod.

"Organizace, které pracují s dlouhodobě citlivými daty – například vládní instituce, finanční sektor, zdravotnictví nebo telekomunikace – si nemohou dovolit čekat. Přechod na post-quantovou kryptografii je otázkou několika let, a proto je potřeba začít s přípravou už dnes. Jinak hrozí, že data zachycená nyní bude možné v budoucnu dešifrovat," shrnul Ondřej Šťáhlavský ze společnosti Fortinet.

AV centrum ČR