

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **148** ze dne **1.7.2026**

Kyberzločinci drtí evropský průmysl. Výkupné přesahuje milion dolarů.

Výrobní sektor čelí agresivnímu tlaku kyberzločinců. Digitální transformace, chytré továrny a komplexní dodavatelské řetězce dělají z výrobních organizací velmi lákavý cíl. Podle údajů společnosti Check Point se počet ransomwarových (vyděračských) útoků na výrobní průmysl prudce zvýšil o 56 % z 937 incidentů v roce 2024 na 1 466 v roce 2025. Výroba je tak vůbec nejčastěji vydíraným odvětvím.

"Jakékoli výpadky provozu mohou stát výrobní společnosti miliony a mohou mít dominový efekt s dopadem na další organizace po celém světě. Útočníci používají narušení výroby jako páku a tlak na zaplacení výkupného, nikoli jako vedlejší škodu," uvedl Peter Kovalčík, regionální ředitel, Security Engineer Eastern Europe z kyberbezpečnostní společnosti Check Point Software Technologies.

Nejčastěji jsou zasažené výrobní společnosti v USA. Vysoký počet incidentů sledujeme i v Indii, Německu nebo Spojeném království.

"Průměrné výkupné, které kyberzločinci při útoku na evropské výrobní společnosti požadují, je 1,16 milionu dolarů, což je více než dvojnásobek oproti předchozímu roku. V roce 2025 jsme viděli řadu incidentů, které narušily automobilový, letecký nebo dopravní průmysl v řadě zemí," upozornil Kovalčík.

Spojené státy jsou jednoznačně nejčastějším terčem ransomwarových útoků, ale průměrné výkupné je "jen" 500 000 dolarů. Naopak v regionu APAC se průměrné výkupné vyšplhalo až na 1,35 milionu dolarů.

Roste i cena ukradených přihlašovacích údajů. Přístupové údaje do průmyslových společností se prodávají na darknetových trzích za 4 000 až 70 000 dolarů.

V roce 2025 dominovalo útokům na výrobní odvětví několik ransomwarových skupin. Akira se stala jednou z finančně nejúspěšnějších skupin, když do konce roku 2025 vygenerovala dle odhadů příjmy ve výši 244 milionů dolarů. Mimo jiné napadla významného německého výrobce kabelů a před zašifrováním ukradla 27 GB citlivých dat. Qilin je ruská skupina, která nabízí ransomware jako službu. V roce 2025 ukradla například 29 843 souborů z výrobní a logistické firmy, což ohrozilo řadu dalších organizací.

Vedle ransomwarových skupin se na průmyslové organizace zaměřili i hacktivisté, jako nechalvě známá skupina NoName057(16), a čínské destruktivní skupiny.

Proč jsou výrobci zranitelní?

Výrobní organizace často spoléhají na starší provozní technologie. Řada řadičů, SCADA systémů a průmyslových IoT zařízení byla vytvořena bez ohledu na moderní hrozby a rizika. Zařízení pak obsahují neopravené známé zranitelnosti, které mohou útočníci snadno zneužít.

Kyberzločinci stále častěji napadají menší dodavatele, poskytovatele spravovaných služeb nebo SaaS platformy, aby získali nepřímý přístup k velkým průmyslovým cílům. Nárůst komplexnosti dodavatelských řetězců zkrátka vytváří nové bezpečnostní výzvy, na které řada společností nezvládá reagovat.

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **148** ze dne **1.7.2026**

Zároveň významně roste sofistikovanost hrozeb a obchod s útočnými nástroji. Ransomware je prodáván jako služba, takže si kdokoli může pronajmout profesionální infrastrukturu, lokalizovat útočné kampaně a přizpůsobit je cílům pro maximální úspěšnost.

"Organizace musí přehodnotit svoje priority, klást důraz na zabezpečení, zálohování, využívat princip nulové důvěry, pečlivě ověřovat identity, poskytovat jen ta nejnutnější oprávnění a segmentovat síť. Záplaty a aktualizace musí být instalované v řádu hodin, nikoli dnů nebo dokonce týdnů. Nutné je také monitorovat, zda už nedošlo k úniku přihlašovacích údajů, například prostřednictvím AI služeb, a neobchoduje se s nimi na darknetových trzích. Současně je potřeba řešit nejenom vlastní zabezpečení, ale klást důraz i na bezpečnost partnerů a dodavatelů," uzavřel Peter Kovalčík

AV centrum ČR