

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **124** ze dne **11.11.2025**

Kyberzločinci se stále častěji zaměřují na výrobní průmysl

Každá výrobní společnost čelí podle průzkumu společnosti Check Point v průměru 1 585 kybernetickým útokům týdně, což je meziroční nárůst o 30 %. Vůbec nejvíce útoků zaznamenaly výrobní podniky na Tchaj-wanu (v průměru 5 100 útoků týdně na jednu společnost) a nejvyšší nárůst zaznamenala Evropa, ze které pochází šest z deseti zemí s nejvyšším meziročním nárůstem útoků na výrobní sektor.

"Útočníci vědí, že každá hodina, kdy výroba neběží, může stát miliony. Proto ransomwarové skupiny považují tento sektor za lukrativní. Nemusí krást citlivá data, když mohou jednoduše zastavit provoz a požadovat výkupné. 22 % obětí vyděračských útoků v loňském roce pocházelo z výrobního sektoru. Nejčastěji jsou vydírané americké, německé a italské výrobní společnosti," uvedl Tomáš Růžička, SE Team Leader z kyberbezpečnostní společnosti Check Point Software Technologies. "Při ransomwarových útocích se nejedná jen o přímé finanční ztráty, ale vidíme i kaskádový efekt: ztrátu důvěry zákazníků, porušení smluv, zpoždění inovací a zvýšené kontroly. Pro mnoho výrobců jsou poškození pověsti a škody na konkurenceschopnosti stejně nákladné jako počáteční narušení provozu."

V letošním roce byl například Nucor, největší výrobce oceli v Severní Americe, nucen zastavit výrobu po kybernetickém útoku. Podobně ransomwarový útok na společnost Sensata Technologies ochromil přepravu a výrobu, což vedlo ke zpožděním a napětí ve vztazích se zákazníky. V roce 2024 ransomwarový útok narušil provoz německého výrobce Schumag AG, který kvůli tomu nakonec skončil v insolinci. V roce 2023 musela společnost Clorox přerušit provoz po útoku ransomwarového gangu, což vedlo k čtvrtletním ztrátám ve výši 356 milionů dolarů.

Nejslabším článkem je dodavatelský řetězec

"Výrobci nepracují izolovaně. Využívají rozsáhlé sítě dodavatelů, globálních partnerů, jsou závislí na IoT a OT systémech a to vše zvyšuje riziko. Specializované hackerské skupiny prodávají přístup do výrobních sítí, což ransomwarovým gangům usnadňuje práci. Jediný zranitelný dodavatel nebo nezabezpečené IoT zařízení může vyvolat dominový efekt, který paralyzuje klidně i celé odvětví," upozornil Růžička. "Poslední roky ukázaly, jak může útok na jednoho dodavatele spustit lavinu a mít dopad na tisíce navazujících podniků. V tomto konkurenčním odvětví mohou i krátké výpadky způsobit trvalý pokles tržeb, odliv zákazníků a nenávratně poškodit značku."

Výrobní průmyslu v centru kybernetických válek

Na výrobní průmysl se stále častěji zaměřují také národní hackerské skupiny financované státy. Cílem jsou krádeže duševního vlastnictví a narušení provozu strategických společností. V posledních dvou letech byly ukradeny plány dronů, pokročilých automobilových konstrukcí a technologie související s obranou. Útoky současně probíhají na společnosti spojené s kritickou infrastrukturou, velmi aktivní jsou i hacktivisté s politickými motivy.

Tyto incidenty ukazují, že bezpečnost výroby není pouze technickou otázkou, ale záležitostí národní konkurenceschopnosti a ekonomické stability. Výrobci se stále častěji ocitají uprostřed geopolitických sporů, obchodních válek a regionálních konfliktů. Vedení firem si proto musí uvědomit, že jejich společnosti mohou být vystaveny rizikům, které sahají daleko za rámec tradičních obchodních strategií.

MEATEST spol. s r.o. - sdělení pověřence pro ochranu osobních údajů číslo **124** ze dne **11.11.2025**

Výrobní průmysl je mimořádně zranitelný, protože musí balancovat mezi zastaralými systémy, rozvětvenými dodavatelskými řetězci a minimální tolerancí k výpadkům. Poselství je proto jasné. Správné zabezpečení je konkurenční výhodou. Je nutné přistupovat k obraně aktivně a zaměřit se na preventivní bezpečnostní technologie.

AV centrum ČR