Téměř 25 % průmyslových firem hlásí škody z kyberútoků vyšší než 5 milionů dolarů

6.6.2025 - | PROTEXT

Nedávná společná studie společností Kaspersky a VDC Research s názvem Securing OT with Purpose-built Solutions (Zabezpečení OT pomocí specializovaných řešení) přináší hloubkovou analýzu současného stavu kybernetické bezpečnosti operačních (provozních) technologií (OT). Studie, založená na průzkumu mezi více než 250 osobami s rozhodovací pravomocí z oblasti energetiky, veřejných služeb, výroby, dopravy a dalších odvětví, nabízí cenné poznatky o klíčových podnikatelských a technických trendech ovlivňujících průmyslové organizace a také o nejúčinnějších strategiích zaváděných k řešení bezpečnostních problémů.

Průzkum upozorňuje, že finanční dopad narušení kybernetické bezpečnosti OT je komplexní a mnohostranný. Organizace musí zvážit široké spektrum nákladů, včetně ušlých příležitostí k dosažení příjmů, neplánovaných prostojů ve výrobě, ztrát kvůli zmetkům nebo nedokončeným výrobkům a škod na zařízení nebo majetku. Kromě toho zahrnuje celková finanční zátěž také přímé náklady související s narušením bezpečnosti, jako je reakce na incidenty, ať už řešené interně nebo externími poskytovateli služeb, a případné platby výkupného.

Po započítání všech těchto faktorů téměř 25 % respondentů průzkumu odhadlo, že každý kybernetický útok by mohl během dvou let způsobit škody přesahující 5 milionů dolarů. Rozložení těchto nákladů se u jednotlivých organizací a incidentů výrazně liší, ale obecně to má dopad na více oddělení a ovlivňuje jak tržby, tak ziskovost.

Zpráva uvádí, že reakce na incidenty tvoří asi 21,7 % celkových nákladů souvisejících s narušením bezpečnosti, za nimiž následují ušlé příjmy s 19,4 %, neplánované prostoje s 16,9 %, opravy a výměny zařízení nebo majetku s 16,8 %, platby výkupného s 12 % a zmetky nebo ztráty zásob z rozpracované výroby s 11,9 %. Jako jeden z nejvýznamnějších faktorů se jeví zejména neplánované výpadky, které podle sdělení 70 % respondentů trvají obvykle čtyři až 24 hodin. Taková narušení provozu mohou vést k podstatným ztrátám příjmů, úzkým místům v interních procesech a snížené důvěře zákazníků, což podtrhuje zásadní význam robustních opatření kybernetické bezpečnosti OT.

"*Neplánované prostoje mohou připravit organizace o miliony dolarů, což z nich dělá kritický problém pro průmyslové a výrobní firmy. Strategie údržby pro boj s nežádoucími odstávkami sice pomáhají, pro posílení kybernetické bezpečnosti je však nezbytná prevence narušení, která mohou vést k nákladným poruchám a výpadkům zařízení. Podceňování kybernetických rizik podkopává snahy o eliminaci prostojů a dosažení zisků,*" komentuje **Andrej Strelkov**, vedoucí produktové řady pro průmyslovou kybernetickou bezpečnost ve společnosti Kaspersky.

Společnost Kaspersky nabízí zákazníkům používajícím OT jedinečný ekosystém, který kombinuje technologie podnikové úrovně, odborné znalosti a rozsáhlé expertizy. Srdcem tohoto ekosystému je nativní XDR platforma Kaspersky Industrial Cybersecurity (KICS) určená pro ochranu kritické infrastruktury a průmyslových podniků. KICS zajišťuje ucelené pokrytí infrastruktury, opatření pro bezpečnou reakci, centralizovanou správu aktiv, hodnocení rizik a provádění auditů a podporuje také škálovatelné zabezpečení napříč komplexními, distribuovanými prostředími pomocí jednotné platformy.

Celý dokument Securing OT with Purpose-built Solutions si můžete přečíst na těchto webových

stránkách. O řešení Kaspersky Industrial Cybersecurity se můžete dozvědět více zde.

O společnosti VDC Research

Společnost VDC Research byla založena v roce 1971 a má sídlo v Southborough ve státě Massachusetts. Zabývá se průzkumem trhu a odbornými konzultacemi se zaměřením na AutoID, mobilní infrastrukturu, průmyslovou automatizaci, loT a vestavěné technologie a poskytuje podrobné analýzy dodavatelům technologií, koncovým uživatelům a investorům po celém světě. Patří mezi nejvýznamnější organizace v tomto oboru a pomáhá svým klientům činit správná zásadní rozhodnutí na základě detailních informací. Nabízí také syndikátní zprávy a klientské konzultace. Díky svým metodikám dokáže přesně předvídat směr vývoje, což jí zajišťuje bezkonkurenční vedoucí postavení v technických oborech. Mezi její přednosti patří také pozornost k detailům a blízké osobní vztahy s klienty, kterým přináší unikátní vhled do problematiky.

http://www.ceskenoviny.cz/tiskove/zpravy/temer-25-prumyslovych-firem-hlasi-skody-z-kyberutoku-vyssi-nez-5-milionu-dolaru/2683260