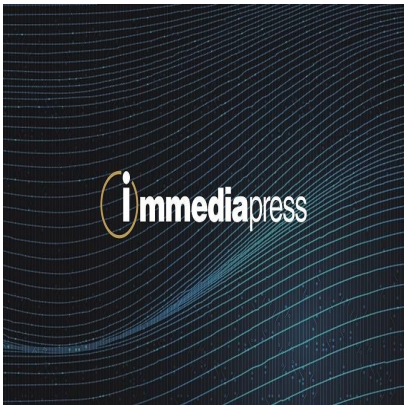

Kaspersky e VDC Research: nel 2025 gli attacchi ransomware potrebbero causare potenziali perdite di oltre 18 miliardi allâ??industria manifatturiera globale

Descrizione

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

Kaspersky, in collaborazione con VDC Research, ha svelato che nei primi tre trimestri del 2025 gli attacchi ransomware alle aziende manifatturiere potrebbe causare oltre 18 miliardi di dollari di perdite. Questa cifra riflette solo il costo diretto della manodopera inattiva durante i periodi di fermo, mentre lâ??impatto operativo e finanziario complessivo supera di gran lunga tale somma. Le stime sono state elaborate per le regioni APAC, Europa, Medio Oriente, Africa, CSI e LATAM sulla base della percentuale di aziende manifatturiere in cui sono stati rilevati e prevenuti tentativi di ransomware, del numero totale di aziende manifatturiere in ciascuna regione, delle ore medie di inattivitÃ dopo attacchi reali, del numero medio di dipendenti per azienda e della retribuzione

Secondo Kaspersky Security Network, da gennaio a settembre 2025, Medio Oriente (7%) e America Latina (6,5%) hanno guidato la classifica per numero di rilevamenti di ransomware nelle aziende manifatturiere. Seguono APAC (6,3%), Africa (5,8%), CSI (5,2%) ed Europa (3,8%). La stima delle potenziali perdite mostra lâ??impatto finanziario che questi attacchi avrebbero avuto se avessero avuto successo.

Quando si verifica un attacco ransomware, le linee di produzione si fermano, causando perdite economiche immediate dovute allâ??inattivitÃ della forza lavoro e perdite a lungo termine a causa della riduzione della produzione. La durata media di un attacco Ã¨ di 13 giorni (secondo il Kaspersky Incident Response Report). Di conseguenza, i costi di manodopera non impiegata a causa del ransomware nei primi tre trimestri del 2025 potrebbero aver raggiunto:

Le reali perdite economiche avrebbero potuto essere significativamente piÃ¹ elevate se si fossero considerate anche le interruzioni della supply-chain, il danno alla reputazione e le spese di ripristino.

â??La nostra ricerca fornisce una stima dellâ??impatto finanziario che il ransomware potrebbe aver avuto sul settore manifatturiero a livello mondiale. La crescente complessitÃ degli ambienti di produzione, insieme al sempre maggiore divario di competenze e alle continue sfide in materia di forza lavoro, rende difficile per la maggior parte delle organizzazioni gestire efficacemente la sicurezza informatica, ma il mancato raggiungimento di questo obiettivo puÃ² comportare gravi danni finanziari, seguiti anche da quelli reputazionali. La collaborazione con fornitori di sicurezza informatica di comprovata esperienza Ã¨ fondamentale per una protezione efficace di IT, OT e IIoTâ?•, ha dichiarato Jared Weiner, Research Director, Industrial Automation & Sensors di VDC Research.

â??Nessuna zona Ã¨ al sicuro dai ransomware: che si tratti di Medio Oriente, America Latina, Asia-Pacifico, CIS, Africa o Europa, ogni centro di produzione Ã¨ costantemente preso di mira. Anche i produttori di medio livello, che in passato erano stati trascurati dagli autori delle minacce, sono ora tra gli obiettivi, poichÃ© i loro budget per la sicurezza sono inferiori e gli effetti di interruzione della catena di approvvigionamento possono essere piÃ¹ gravi di quanto si pensi. Il settore manifatturiero e tutte le altre organizzazioni hanno bisogno di sistemi di difesa affidabili e comprovati e di una formazione continua degli operatoriâ?•, ha aggiunto Dmitry Galov, Head of Research Center for Russia and CIS del GReAT di Kaspersky.

Maggiori informazioni sulle minacce ransomware nelle diverse regioni sono disponibili nello State of Ransomware Report 2025 di Kaspersky.

Kaspersky suggerisce alle aziende di seguire queste best practice per proteggersi dal ransomware:

Contatti:
Kaspersky
kaspersky@noesis.net

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

ResponsabilitÃ editoriale di Kaspersky

â??

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione
Novembre 19, 2025
Autore
redazione