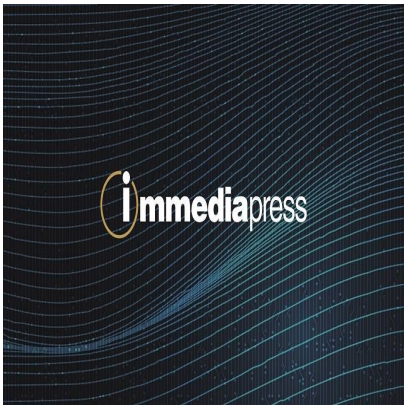

Kaspersky: le minacce cyber al settore delle telecomunicazioni continueranno anche nel 2026

Descrizione

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

Un nuovo report del Kaspersky Security Bulletin analizza i principali sviluppi che hanno caratterizzato la sicurezza informatica nel settore delle telecomunicazioni nel 2025 e le minacce che, con ogni probabilitÃ , continueranno a manifestarsi anche nel 2026. Nel corso dellâ??ultimo anno, attivitÃ APT, compromissioni della catena di approvvigionamento, interruzioni DDoS e frodi tramite SIM hanno continuato a esercitare una forte pressione sugli operatori. Parallelamente, lâ??adozione di nuove tecnologie ha introdotto ulteriori rischi di natura operativa.

Nel 2025, gli operatori di telecomunicazioni hanno dovuto affrontare quattro grandi categorie di minacce. Le intrusioni mirate (APT) hanno continuato a puntare allâ??ottenimento di un accesso furtivo agli ambienti degli operatori, finalizzato allo spionaggio a lungo termine e allo sfruttamento di posizioni privilegiate allâ??interno delle reti. Allo stesso tempo, le vulnerabilitÃ della catena di approvvigionamento sono rimaste un importante punto di ingresso: gli ecosistemi delle telecomunicazioni si basano infatti su numerosi fornitori, appaltatori e piattaforme strettamente integrate, rendendo le debolezze di software e servizi ampiamente utilizzati un potenziale canale di accesso alle reti degli operatori. Infine, gli attacchi DDoS hanno continuato a rappresentare un problema concreto in termini di disponibilitÃ dei servizi e capacitÃ delle infrastrutture.

I dati di Kaspersky Security Network mostrano che, tra novembre 2024 e ottobre 2025, il 12,79% degli utenti del settore delle telecomunicazioni Ã¨ stato soggetto a minacce web, mentre il 20,76% ha affrontato minacce sui dispositivi. Nello stesso periodo, il 9,86% delle organizzazioni di telecomunicazioni a livello globale ha subito attacchi ransomware.

Parallelamente, il settore delle telecomunicazioni sta passando da una fase di rapido sviluppo tecnologico a una di implementazione su larga scala. Secondo il report, questa transizione creerÃ nuove opportunitÃ ma anche nuovi rischi operativi nel corso del 2026. Kaspersky individua tre aree principali in cui le transizioni tecnologiche potrebbero causare interruzioni, soprattutto se implementate in modo non uniforme o senza controlli rigorosi. La prima riguarda la gestione della rete assistita dallâ??intelligenza artificiale, dove lâ??automazione puÃ² amplificare errori di configurazione o agire sulla base di dati fuorvianti. La seconda Ã¨ rappresentata dalla transizione verso la crittografia post-quantistica, in cui unâ??implementazione affrettata di approcci ibridi o post-quantistici potrebbe generare problemi di interoperabilitÃ e prestazioni negli ambienti IT, di gestione e di interconnessione. La terza area riguarda lâ??integrazione tra reti 5G e satellitari (NTN), dove lâ??estensione della copertura dei servizi e le dipendenze dai partner introducono nuovi punti di integrazione e potenziali modalitÃ di guasto.

â??Le minacce che hanno dominato il 2025 â?? campagne APT, attacchi alla catena di approvvigionamento e attacchi DDoS â?? non stanno scomparendo. Oggi, perÃ², si intrecciano con i rischi operativi legati allâ??automazione basata sullâ??IA, alla crittografia quantistica e allâ??integrazione satellitare. Gli operatori di telecomunicazioni devono avere visibilitÃ su entrambe le dimensioni: mantenere difese solide contro le minacce note e integrare la sicurezza in queste nuove tecnologie fin dal primo giorno. La chiave Ã¨ disporre di unâ??intelligence continua sulle minacce, che si estenda dallâ??endpoint allâ??edge fino allâ??orbitaâ?•, ha affermato Leonid Bezvershenko, Senior Security Researcher di Kaspersky GReAT.

Ã? possibile leggere il report completo dedicato alle telecomunicazioni del Kaspersky Security Bulletin 2025.

Per ridurre i rischi e rafforzare la resilienza, gli esperti di Kaspersky raccomandano:

Contatti:
Kaspersky
kaspersky@noesis.net

â??

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione
Gennaio 9, 2026
Autore
redazione