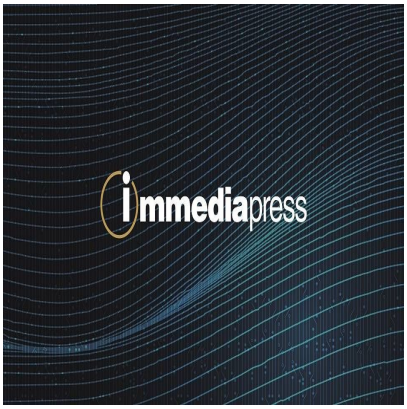

Incidenti ad alto rischio in calo: Kaspersky segnala una diminuzione costante nel corso degli anni

Descrizione

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

Secondo il report â??Anatomy of a Cyber World: Global Report by Kaspersky Security Servicesâ?•, negli ultimi anni si Ã¨ registrato un calo significativo della percentuale di incidenti ad alta gravitÃ . Se nel 2021 si Ã¨ toccato il valore piÃ¹ elevato (14,3%), nel 2025 Ã¨ stato registrato il dato piÃ¹ basso degli ultimi sei anni, pari ad appena il 3,8%. Questa tendenza indica che molti tentativi di attacco sono stati rilevati rapidamente ed efficacemente mitigati dagli esperti MDR di Kaspersky, impedendo che la loro gravitÃ superasse livelli medi.

Gli incidenti ad alta gravitÃ sono definiti come attacchi che comportano un coinvolgimento diretto da parte di persone e che provocano un impatto significativo sullâ??infrastruttura IT del cliente. Nel 2025, il numero di questi incidenti rilevati da Kaspersky MDR Ã¨ diminuito del 19% rispetto al 2024, evidenziando i miglioramenti nelle capacitÃ di rilevamento precoce e lâ??efficacia delle misure collettive adottate dai clienti.

Da unâ??analisi approfondita delle cause alla base di questi incidenti avvenuti nel 2025 emergono le seguenti conclusioni:

Gli attacchi perpetrati da persone hanno rappresentato circa il 23% degli incidenti di grave entitÃ . Sebbene si tratti di un leggero calo rispetto al 2024, questa tipologia di attacco continua a essere la principale causa delle violazioni piÃ¹ gravi. Kaspersky ha rilevato attacchi di questo tipo quasi il 21% dei clienti, a dimostrazione del fatto che aggressori determinati riescono ancora a eludere le difese automatizzate. Nonostante i progressi degli strumenti di rilevamento automatico, questi attori altamente

qualificati trovano infatti ancora modi per aggirare le misure di sicurezza.

Le esercitazioni informatiche confermate, come il Red Teaming, hanno rappresentato oltre il 23% degli incidenti. Quando queste attivitÃ vengono verificate nellâ??ambito dei test di sicurezza, sono spesso classificate come falsi positivi dellâ??infrastruttura. Tuttavia, i clienti richiedono spesso che queste attivitÃ vengano segnalate come incidenti, al fine di monitorare lâ??efficienza del servizio MDR.

Il social engineering si colloca al terzo posto, risultando responsabile di oltre il 15% degli attacchi ad alta gravitÃ e interessando quasi il 18% delle aziende. Questi attacchi vengono classificati come critici quando vanno a buon fine e non vengono risolti automaticamente, portando spesso a raccomandazioni in materia di sensibilizzazione alla sicurezza.

Gli incidenti legati al malware si attestano a meno del 12%, mentre in oltre il 7% dei casi sono stati rilevati residui di attacchi passati causati da esseri umani, o tracce di APT. Il rilevamento delle vulnerabilitÃ , pur non essendo lâ??obiettivo principale di Kaspersky MDR, Ã¨ stato segnalato in meno del 5% degli incidenti.

â??Il calo degli incidenti ad alta gravitÃ evidenzia lâ??importanza fondamentale di adottare una strategia di sicurezza informatica proattiva. Le soluzioni basate sullâ??intervento umano, come il Managed Detection and Response (MDR) e lâ??Incident Response, restano essenziali per contrastare le minacce sofisticate e di origine umana. Per migliorare ulteriormente lâ??efficacia e lâ??efficienza dei team di sicurezza interni, le aziende dovrebbero integrare soluzioni avanzate e automatizzate come lâ??Extended Detection and Response (XDR), che offrono maggiore visibilitÃ e consentono risposte piÃ¹ rapide. Inoltre, avvalersi dei servizi di consulenza SOC puÃ² aiutare a costruire da zero un solido Security Operations Center o a ottimizzare quello esistente per ottenere le massime performance. Un approccio integrato alle operazioni di sicurezza ibrida consente alle aziende di rilevare le minacce in anticipo, contenerle rapidamente e, in ultima analisi, impedire che si verifichino gravi violazioniâ?•, ha commentato Sergey Soldatov, Head of Security Operations di Kaspersky.

Per contrastare gli attacchi perpetrati da persone, gli esperti di Kaspersky raccomandano di:

Per ulteriori informazioni sulle tattiche e tecniche utilizzate dagli autori degli attacchi, sulle caratteristiche degli incidenti rilevati e sulla loro distribuzione a livello regionale e settoriale, Ã¨ possibile consultare il report completo.

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
Marzo 25, 2026
Autore
redazione