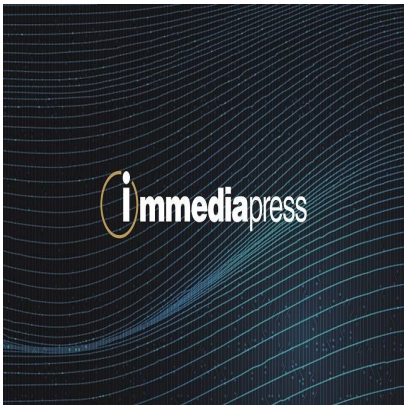

Kaspersky mette alla prova le aziende IT con nuove simulazioni di attacchi

Descrizione

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

Kaspersky ha ampliato la sua Kaspersky Interactive Protection Simulation (KIPS) con nuovi scenari avanzati di attacchi informatici pensati appositamente per le aziende IT. Lâ??aggiornamento introduce simulazioni realistiche di frodi basate su deepfake, compromissione della supply chain, attacchi alle relazioni di fiducia e malware distruttivi di tipo wiper, aiutando le aziende a testare la propria preparazione rispetto al complesso panorama delle minacce odierne.

Secondo lâ??Incident Response Analyst Report 2024 di Kaspersky, le aziende IT restano uno degli obiettivi piÃ¹ appetibili per i criminali informatici, rappresentando il 7,2% degli incidenti a livello globale. PoichÃ© gli aggressori combinano sempre piÃ¹ spesso tecniche di social engineering, manipolazione della supply chain e tattiche ransomware, le aziende necessitano di una formazione pratica e strategica che rifletta le dinamiche degli attacchi nel mondo reale.

Kaspersky Interactive Protection Simulation Ã¨ progettata per colmare il divario comunicativo tra CISO, team IT e alta dirigenza. Inserendo i partecipanti in scenari realistici di crisi informatiche, KIPS dimostra lâ??impatto operativo e commerciale degli attacchi in un formato accessibile e coinvolgente.

Attacchi reali in un ambiente di simulazione realistico

Lo scenario aggiornato, incentrato sullâ??IT in KIPS, espone i partecipanti alle moderne tecniche di attacco osservate dagli esperti di Kaspersky nelle campagne dannose attive che prendono di mira il settore IT.

I partecipanti potrebbero trovarsi ad affrontare:

Le aziende IT possono ora scegliere tra due scenari di attacco dedicati, testando il coordinamento, la gestione delle crisi e il processo decisionale sotto pressione. KIPS Ã¨ disponibile sia in formato live (fino a 100 partecipanti) sia online (fino a 1.000 partecipanti) e fornisce analisi dettagliate sulle decisioni dei partecipanti, sul coordinamento del team e sul benchmarking rispetto alle sessioni precedenti.

â??Per garantire la sicurezza, le aziende necessitano di una strategia di difesa a piÃ¹ livelli che combini tecnologia, processi e risorse umane. Tuttavia, investire solo negli strumenti non Ã¨ sufficiente. La resilienza informatica dipende dalla consapevolezza, dal coordinamento e dalla capacitÃ di rispondere efficacemente sotto pressioneâ?•,ha commentato Svetlana Kalashnikova, Security Awareness Expert di Kaspersky. â??Kaspersky Interactive Protection Simulation, parte di unâ??offerta completa di Security Awareness, aiuta le organizzazioni a sperimentare scenari di attacco reali in un ambiente controllato, rafforzando il processo decisionale, la collaborazione tra i team e la comprensione dei rischi di sicurezza informatica da parte dei dirigenti. Trasformando minacce complesse in esperienze di apprendimento pratiche, consentiamo alle aziende di costruire culture della sicurezza piÃ¹ solide e resilientiâ?•.

Maggiori informazioni su Kaspersky Interactive Protection Simulation sono disponibili qui.

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 2, 2026
Autore
redazione