

Gestione del rischio cyber 2026: rilevare l'invisibile per mitigare la superficie di attacco



La gestione del rischio cyber 2026 è al centro dell'Osservatorio Cyberoo, la ricerca annuale con cui Cyberoo mappa l'evoluzione del cyber crime e delle minacce digitali che colpiscono organizzazioni pubbliche e private. Un punto di osservazione privilegiato, che quest'anno restituisce un quadro più complesso del previsto, e più inquietante.

Esiste un paradosso silenzioso al centro della cybersecurity contemporanea: più le organizzazioni investono in strumenti di protezione, più cresce la complessità che faticano a governare. Ogni nuovo sistema aggiunto all'infrastruttura introduce un potenziale punto cieco. Ogni integrazione con un fornitore esterno estende la superficie esposta. Ogni identità digitale non censita diventa un varco potenziale. Il perimetro, nella sua accezione tradizionale, non esiste più, eppure molte strategie di sicurezza continuano a ragionare come se esistesse ancora.

Il 2026 impone un cambio di prospettiva radicale: non si tratta di difendersi meglio da ciò che si conosce, ma di sviluppare la capacità di vedere ciò che ancora non si vede. Il rischio più pericoloso non genera un allarme, scorre silenzioso sotto la soglia di osservazione, nei margini dell'ecosistema digitale che nessuno ha mai mappato davvero.

Il rischio cyber nel 2025: cosa rivelano i dati dell'Osservatorio Cyberoo

Il rischio cyber nel 2026 non può più essere interpretato attraverso modelli lineari. Le minacce sono meno osservabili, più distribuite e in grado di propagarsi lungo le interdipendenze tecniche e operative delle organizzazioni. Limitarsi a catalogare vulnerabilità o ad aggiungere controlli non è più sufficiente. La cybersecurity richiede la capacità di leggere un ecosistema complesso, in cui l'esposizione reale non è pienamente rappresentata dalle *dashboard*.

I dati del 2025 raccolti dall'Osservatorio Cyberoo lo dimostrano chiaramente. Sono stati individuati 320 nuovi *threat actor*, molti dei quali caratterizzati da tattiche aggressive e specializzate. Il monitoraggio ha generato oltre 1.300 segnalazioni alle autorità per *phishing* e frodi digitali e portato al rilevamento di 38.654 domini sospetti. Ancora più rilevante è l'emersione di più di 2.700 CVE univoche associate ai fornitori monitorati, un segnale forte della fragilità strutturale della *supply chain*.

Vettori di attacco in evoluzione: dal DDoS al phishing potenziato dall'AI

Nel corso dell'anno si è osservato un ritorno degli attacchi DDoS, impiegati per saturare i sistemi di difesa e facilitare compromissioni parallele. Il *phishing* si è trasformato grazie all'AI generativa: *deepfake* vocali e video rendono credibili messaggi che in passato sarebbero stati facilmente riconoscibili. Parallelamente sono aumentate la circolazione di credenziali rubate e le *exploitation* dirette, incluse le *zero day*.

L'analisi dei settori più colpiti mostra che il *manufacturing* rappresenta il 29% degli attacchi analizzati, a conferma della

crescente pressione sugli ambienti industriali. Sul piano temporale, dicembre emerge come il mese più critico, complice la riduzione dei presidi operativi.

La materia oscura cibernetica: il rischio cyber che non si vede

Questi fenomeni rivelano un problema più profondo dell'aumento delle minacce: l'esistenza di un'ampia area di rischio non osservata. Cyberoo la definisce *materia oscura cibernetica*, ossia *asset* non censiti, identità non umane prive di *governance*, API dimenticate, sistemi obsoleti e superfici non monitorate. È qui che si concentra la parte più rilevante dell'esposizione ed è qui che gli attaccanti trovano spazio per muoversi senza essere rilevati.

Gestione del rischio cyber: visibilità, governance e resilienza come priorità 2026

Per affrontare il 2026 non serve moltiplicare i livelli di protezione, ma aumentare visibilità, *governance* e resilienza. Servono modelli *identity first*, *patching* basato sul rischio, monitoraggio continuo, *backup* verificati e *playbook* operativi. È altrettanto essenziale una gestione dell'AI che prevenga manipolazioni e automatismi non supervisionati. La resilienza non nasce dalla reazione agli incidenti, ma dalla capacità di anticipare le dinamiche che li rendono possibili.

Cyberoo alla Cyber Crime Conference 2026: scarica l'Osservatorio Cyberoo

In vista della Cyber Crime Conference 2026 e dell'intervento di Luca Bonora, Cyberoo Evangelist, previsto per mercoledì 6 maggio alle ore 11:40, Cyberoo mette a disposizione il *download* dell'Osservatorio Cyberoo 2026 tramite questo link. Per maggiori informazioni è possibile visitare il nostro sito,

contattarci a info@cyberoo.com o al numero 0522 388111.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/notizie/gestione-del-rischio-cyber-2026-osservatorio-cyberoo/>