# Cybersecurity: perché le Pmi sono il bersaglio perfetto

Nell'era digitale la sicurezza informatica non è più un tema per addetti ai lavori, ma una condizione essenziale per la continuità del business. E a ricordarlo è Konverto, che accompagna imprese e istituzioni nel loro percorso di trasformazione digitale

Con sedi a Bolzano e Trento, oltre 170 dipendenti e competenze che spaziano dalla cybersecurity al cloud, dal networking alla customizzazione software, Konverto rappresenta oggi uno dei principali poli tecnologici dell'Alto Adige e del Trentino. Oltre a sviluppare soluzioni It su misura, l'azienda gestisce progetti di intelligenza artificiale, piattaforme digitali per la collaborazione e servizi gestiti per il monitoraggio della sicurezza informatica.

«Negli ultimi anni il nostro lavoro è cambiato molto - racconta Stefan Laimer, security manager di Konverto -. Un tempo le imprese chiedevano connettività o supporto tecnico; oggi chiedono protezione. Hanno capito che la sicurezza è la base per poter crescere, innovare e restare affidabili agli occhi dei clienti».

*Stefan Laimer, security manager di Konverto*

Molti imprenditori, tuttavia, continuano a pensare che gli attacchi informatici riguardino solo i grandi gruppi. «È un errore frequente e pericoloso - avverte Laimer -. Proprio le piccole e medie imprese sono diventate i bersagli preferiti dei criminali informatici. Gli hacker cercano obiettivi più facili, con sistemi meno protetti ma capaci di generare profitto. Anche un piccolo riscatto può essere un guadagno sufficiente».

Le tecniche d'attacco più diffuse restano note, ma diventano ogni anno più sofisticate. Il phishing è ancora la porta d'ingresso più comune: un'e-mail apparentemente innocua che serve a rubare credenziali o installare ransomware, programmi che bloccano i dati aziendali finché non si paga un riscatto. A queste si aggiungono truffe come il business email compromise, in cui vengono manipolate comunicazioni interne per deviare pagamenti o ottenere informazioni riservate. «Un clic sbagliato può bastare per compromettere un'intera organizzazione - spiega Laimer -. Un account e-mail infetto può inviare messaggi a clienti e fornitori, danneggiando la reputazione. E senza backup aggiornati, il recupero dei dati diventa un percorso lungo e costoso. Un attacco non distrugge solo file e server: mina la fiducia che tiene in piedi le relazioni commerciali».

Molte vulnerabilità nascono da abitudini quotidiane: password deboli, software non aggiornato, assenza di autenticazione a più fattori, gestione non centralizzata della rete. «In diversi casi – osserva Laimer – manca una cultura della sicurezza. Le aziende investono in nuovi strumenti digitali, ma non nelle fondamenta che li rendono sicuri. È come costruire una casa moderna senza porte chiuse a chiave».

Per questo motivo, Konverto ha sviluppato un approccio alla sicurezza che parte dalla consapevolezza delle proprie debolezze. Questa filosofia si traduce in servizi concreti che aiutano le aziende a capire prima dove sono vulnerabili, per intervenire in tempo. È il caso, ad esempio, dei servizi di Exposure Check e Vulnerability Assessment, due strumenti complementari che permettono di fotografare la superficie d'attacco di un'organizzazione e pianificare le azioni di difesa. L'Exposure Check consente di individuare gli elementi esposti all'esterno — server, applicazioni, accessi o configurazioni non protette — che potrebbero rappresentare un punto d'ingresso per un attaccante. «È un po' come guardare la propria azienda con gli occhi di un potenziale hacker - spiega Laimer -, per scoprire quali porte sono rimaste aperte».

Il Vulnerability Assessment, invece, entra più in profondità: analizza le infrastrutture interne, valuta i software, le configurazioni e le reti, e stila un report dettagliato che classifica le vulnerabilità per gravità e priorità, suggerendo anche le azioni correttive. Questi strumenti, insieme al monitoraggio continuo offerto dai servizi gestiti di Konverto, rappresentano la base di una strategia di sicurezza proattiva e sostenibile. Oltre alla componente tecnica, l'azienda affianca ai propri servizi attività di formazione e sensibilizzazione, come corsi per i dipendenti e simulazioni di phishing, per costruire una cultura aziendale della sicurezza. «La tecnologia da sola non basta - ribadisce Laimer -. Serve un cambiamento di mentalità. La sicurezza inizia dalle persone».

E quando l'attacco avviene, la regola è mantenere la calma e agire in modo strutturato: isolare i sistemi infetti, mettere al sicuro i backup, informare subito gli esperti di sicurezza e le autorità competenti. Pagare il riscatto, invece, «deve essere sempre l'ultima risorsa e solo dopo una valutazione tecnica e legale, perché può risultare inutile o addirittura illegale».

Oggi, inoltre, gli attacchi evolvono rapidamente grazie all'uso dell'intelligenza artificiale. Gli hacker sfruttano algoritmi per generare e-mail di phishing più convincenti, creare deepfake vocali o video realistici, o automatizzare campagne di attacco su larga scala. Persino i sistemi di autenticazione multifattore possono essere presi di mira. «Per questo – spiega Laimer – stanno emergendo nuove tecnologie come i Passkey, che rendono le credenziali molto più difficili da rubare o replicare».

La conclusione è netta: non esiste più il "troppo piccolo per essere interessante". Ogni impresa, indipendentemente dalle dimensioni, deve considerare la sicurezza parte integrante del proprio modello di business. «Non è più una questione di se, ma di quando si verrà attaccati - afferma Laimer -. La differenza la fa la preparazione. Le aziende che oggi investono nella sicurezza saranno quelle che domani potranno continuare a crescere con fiducia, nel digitale e nel reale». • **Beatrice Guarnieri**

## SOC: IL CUORE PULSANTE DELLA SICUREZZA 24/7

Konverto sta investendo in modo importante nel potenziamento del proprio Security Operation Centre (SOC), il centro operativo dedicato alla gestione continua della sicurezza informatica dei clienti.

Il SOC è un'infrastruttura altamente specializzata che monitora in tempo reale reti e sistemi aziendali, rileva comportamenti anomali e coordina la risposta a potenziali attacchi. Grazie ai servizi di Managed Detection & Response (MDR) e Vulnerability Management, il team Konverto è in grado di intervenire tempestivamente, isolando le minacce prima che provochino danni.

«Non vogliamo solo reagire agli attacchi - afferma Laimer -, ma anticiparli. Il monitoraggio costante e la risposta rapida sono ciò che permette di trasformare la sicurezza da costo a investimento strategico».

Il SOC di Konverto rappresenta il punto di sintesi tra tecnologia, competenza e vigilanza. Un presidio attivo 24 ore su 24 che offre alle imprese del territorio – piccole o grandi – la tranquillità di sapere che qualcuno veglia costantemente sui loro sistemi informativi.


**Sempre vigili.** Con uno sguardo attento a ogni minima anomalia, i nostri esperti di sicurezza monitorano la vostra infrastruttura IT 24 ore su 24. In questo modo, le minacce informatiche vengono rilevate, analizzate e affrontate rapidamente. Utilizzate il nostro Security Operation Center come supporto esterno per la sicurezza e alleviate il vostro reparto IT. Richiedete il vostro concetto di cybersecurity personalizzato: 800 031 031

passion for technology . Bolzano & Trento . konverto.eu KONVERTO