RISCHI & CYBERSICUREZZA
PMI PIÙ CONSAPEVOLI

Il 78% dichiara fiducia nelle proprie capacità di affrontare gli attacchi informatici che arriveranno nel 2025. Ma il 38% fa fatica a trovare esperti certificati da assumere

di **UMBERTO TORELLI**

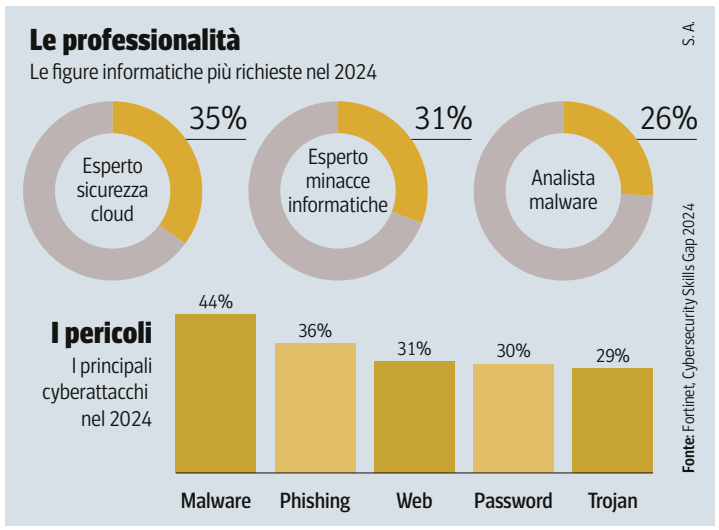
Cresce il rischio cybersecurity per le aziende italiane. Specie per le Pmi, più esposte. Con un dato preoccupante: tre su quattro si aspettano un attacco informatico nel corso del 2025. Il risultato emerge dalla recente ricerca di Qbe Insurance condotta nel mese di settembre da Research Dogma. A essere coinvolto un campione di responsabili di 400 aziende fino a 249 dipendenti, equamente distribuite sul territorio nazionale.

Lo studio precisa che il 68% delle Pmi italiane prevede di subire un attacco informatico nel prossimo anno. Il valore tocca il 74% considerando altre criticità informatiche come truffe, hackeraggi, ransomware e blocco delle attività. Guardando gli ultimi dodici mesi, metà delle piccole imprese (51%) ha purtroppo sperimentato un evento informatico critico. Il dato sale al 63% tra le aziende con ecommerce maggiormente esposte. Non solo. Dopo il caso CrowdStrike Microsoft dello scorso luglio sui bug di aggiornamento del sistema operativo Windows, il 37% dei manager intervistati ha deciso di potenziare le misure di cyberprotezione in azienda.

Secondo gli esperti Qbe Insurance le Pmi italiane adottano un atteggiamento pragmatico e strategia «no panic» nei confronti della security. Il 78% si dichiara infatti fiducioso rispetto alla capacità di affrontare i rischi informatici, mentre il restante 22% ammette la necessità di migliorare le difese.

A mettere in luce le sfide legate alla carenza di competenze in materia di cybersecurity è Fortinet, azienda californiana specializzata in soluzioni di networking e security. Nell'ultimo report Cybersecurity Skills Gap 2024 emerge che la principale carenza delle aziende riguarda le competenze informatiche, che sono inadeguate. Per combattere i pirati informatici è necessario contrastarli con professionisti formati e certificati sulle tematiche della protezione informatica.

L'indagine ha coinvolto 1.850 responsabili aziendali in ambito security provenienti da 29 paesi del mondo tra cui l'Italia. Il dato più significativo e che l'87% ha dichiarato di aver subito nell'ultimo anno una violazione dovuta alla mancanza di competenze interne. Per quanto riguarda l'Italia, i numeri parlano di una situazione da tenere sotto stretto controllo. L'86% degli intervistati ha infatti dichiarato come negli ultimi 12 mesi le loro organizzazioni abbiano subito attacchi. In buona parte possono essere attribuiti alla mancanza di competenze di cybersecurity nei team che si occupano di rete e sicurezza. Un impatto considerevole, tenendo conto che il 58% dei partecipanti ha dichiarato di attribuire tali attacchi alla mancanza di consapevolezza sul tema della sicurezza da parte di organizzazioni e dipendenti.



Fortinet
Massimo Palermo, country manager Italia

Non da ultimo, il 44% ha evidenziato come siano stati necessari da uno a tre mesi per recuperare i danni derivanti dagli attacchi subiti. Con conseguenti perdite economiche e d'immagine.

«Il report mette in luce l'urgenza di colmare quanto prima il gap esistente – spiega a proposito Massimo Palermo, country manager Italia di Fortinet -. Il primo baluardo conto la criminalità informatica è infatti la formazione», che è fondamentale non solo all'interno delle aziende, ma necessaria per stimolare a tutti i livelli un apprendimento continuo della materia.

Le competenze

Il 38% degli intervistati afferma che la propria organizzazione fatica a reclutare e assumere figure professionali nel campo della security. Emerge inoltre che l'area dove risulta più difficile coprire ruoli tecnici riguarda la sicurezza delle reti. Le tattiche dei pirati informatici diventano sempre più sofisticate e stanno rapidamente individuando i modi per eludere i controlli sicurezza. Tuttavia, molti dirigenti aziendali non dispongono del personale necessario per proteggere in modo adeguato le reti della propria organizzazione. Con una carenza di risorse sempre più evidente nel settore cybersecurity. Ecco perché in fase di assunzione i candidati in possesso di certificazioni si distinguono dagli altri. Oltre il 90% dei responsabili delle risorse umane ha dichiarato di prediligere l'assunzione di candidati in possesso di attestati. «Dunque la formazione non è solo una necessità — conclude Palermo – ma diventa un'occasione per ripensare all'intero ecosistema della sicurezza aziendale».

Consulenza trasversale
Non basta il metodo: serve il controllo continuo

Cloud e cybersecurity sono i componenti portanti dello sviluppo aziendale: il primo garantisce flessibilità, velocità ed efficienza, la seconda protezione». Non ha dubbi sull'importanza di avere partner tecnologici solidi per affrontare un panorama digitale in continua evoluzione Roberto Fassina, Sales & Customer Solutions Director di Deda Tech: nuovo nome di Deda Cloud, controllata di Dedagroup (Deda), tra i principali operatori tecnologici a capitale interamente italiano. «Oggi — osserva Fassina — le aziende richiedono soluzioni tecnologiche non solo per affrontare le sfide immediate e per gestire la crescente complessità normativa, ma anche per costruire una resilienza di lungo periodo. In questa direzione, Deda Tech ha scelto di ampliare il proprio raggio d'azione con consulenze specializzate e servizi di governance e compliance, ma anche con un'attenzione particolare all'innovazione tecnologica e alla gestione strategica del rischio». L'evoluzione tecnologica, con l'imminente diffusione della generative AI e l'entrata in vigore delle normative NIS2 e DORA, d'altro canto, richiede cambiamenti significativi nella gestione della sicurezza e della resilienza operativa, aumentando la complessità e gli obblighi di compliance per le aziende. «Dal punto di vista della sicurezza — illustra Fassina — il rapporto CLUSIT 2024 rivela che la media mensile di attacchi gravi nel mondo è salita da 139 a 232, con un aumento dell'11% a livello globale e del 65% in Italia. Anche il mercato ICT italiano, come confermato dal Rapporto Assintel 2024, cresce oltre l'economia nazionale (+4,1% per il settore ICT business), dimostrando l'esigenza tecnologica profonda delle aziende. Per questa ragione, in futuro, si affermeranno gli operatori in grado di distinguersi per capacità di visione e consulenza trasversale abbinata a una capacità di governo delle tecnologie fondata su 3 cardini principali: metodologia, competenza e strumenti di Continuous control monitoring (non a caso, la specializzazione di Quod Orbis, azienda UK recentemente entrata a far parte del gruppo)». L'approccio si rispecchia nei risultati aziendali: la previsione è chiudere il 2024 con una crescita a doppia cifra, dopo aver archiviato un 2023 con un giro d'affari di 68 milioni di euro. Non mancano i piani di sviluppo : «Puntiamo — conclude Fassina — all'espansione internazionale, con un'attenzione particolare agli Stati Uniti».

Deda Tech
Roberto Fassina, Sales & Customer Solutions Director

Carlotta Clerici

Caccia grossa ai pirati? Anche sul «mobile»

Anticipare le esigenze della cybersecurity mobile, branca della cybersecurity la cui importanza viene spesso sottovalutata, è quanto mai attuale. Ci è riuscita Mobisec, azienda fondata a Treviso nel 2015: «Dall'inizio — racconta il ceo Simone Rebeschini — abbiamo puntato su un settore specifico, Vulnerability Assessment e Penetration Testing per le applicazioni smartphone, intuendo una tendenza che oggi è diventata una necessità. Inoltre, negli anni abbiamo sviluppato altre competenze, come ad esempio il servizio di consulenza per la configurazione e la gestione sicura dei dispositivi aziendali e promuoviamo la formazione di Security by Design, che consente a chi sviluppa applicazioni di scrivere un codice sicuro fin dall'inizio, grazie alle competenze acquisite durante il percorso formativo». Su queste basi Mobisec ha chiuso il 2023 con fatturato vicino al milione di euro, prevedendo una crescita del 30% per il 2024. Ma sarà nel 2025, secondo le previsioni di Rebeschini, che si assisterà a una vera svolta dell'azienda: «Stimiamo — anticipa il ceo — di raddoppiare il fatturato grazie agli investimenti che puntano a rafforzare il brand, ampliare la nostra rete commerciale e a sviluppare i nostri prodotti core». Il futuro della cybersecurity, in primis la sicurezza mobile, del resto, mostra un crescente interesse da parte delle aziende. «Le nuove regolamentazioni europee, come NIS2, DORA e il Cyber Resilience Act — osserva il ceo — stabiliscono standard di sicurezza più elevati, spingendo le imprese a integrare la protezione dei dati nei loro processi. Anche gli utenti finali sono più attenti alla sicurezza delle app, richiedendo soluzioni che mettano al primo posto la protezione dei dati sensibili». Nei prossimi tre anni, Mobisec, ha tracciato una rotta che punta a consolidare la presenza in Italia e in Europa: già in cantiere investimenti strategici su settori come domotica, OT (Operational Technology) e automotive. Conclude Rebeschini: «Vogliamo diventare partner di riferimento per le aziende. L'obiettivo va oltre la previsione dei rischi: creare un ecosistema digitale sicuro e resiliente per i nostri clienti».

Mobisec
Simone Rebeschini, ceo dell' azienda fondata a Treviso nel 2015

Ca. Cle.