

La cybersecurity per le PMI italiane: una sfida di risorse e priorità

La cybersecurity per le PMI italiane rappresenta oggi un paradosso: tutti ne riconoscono l'importanza, pochi la traducono in azioni concrete. Non per negligenza, ma per una combinazione di fattori che vanno dalla scarsità di budget alla difficoltà di orientarsi in un panorama tecnologico in costante evoluzione. Eppure, proprio le realtà più piccole sono quelle che rischiano di più: un singolo attacco può compromettere anni di lavoro e relazioni commerciali. Ecco perché serve un cambio di prospettiva.

Cybersecurity per le PMI: la minaccia corre, i budget restano fermi

Aperto un telegiornale, sfogliando un quotidiano o navigando su una rivista di settore, non passa giorno senza leggere di un attacco informatico ai danni di una grande azienda o di un'istituzione pubblica. Ciò che un tempo era considerato un evento eccezionale, oggi è diventato la norma: la cosiddetta *CyberWar* è ormai un fronte stabile delle tensioni internazionali. Non serve guardare lontano: lo abbiamo visto con il conflitto russo-ucraino, in cui i cyber attacchi hanno affiancato le azioni militari tradizionali, ma anche in attacchi sempre più sofisticati a infrastrutture critiche in Europa, Italia compresa.

Eppure, nonostante questa costante esposizione mediatica e il bombardamento di notizie su ransomware, data breach e furti di identità digitali, quando si parla di **investimenti in**

sicurezza informatica, i budget restano sorprendentemente limitati.

Allora la domanda sorge spontanea: **il problema non esiste o semplicemente non è percepito?**

La risposta è più semplice di quanto sembri: le aziende provano a restare aggiornate, ma l'evoluzione tecnologica alimentata oggi dall'intelligenza artificiale, che viene ormai impiegata anche per ottimizzare e automatizzare gli attacchi, corre molto più veloce della capacità di adattamento di sistemi e persone.

Per misurare questa crescita basta uno sguardo ai numeri: secondo i dati del NIST National Vulnerability Database (NVD), nel 2023 sono state pubblicate 28.818 nuove Common Vulnerabilities and Exposures (CVE), salite a oltre 40.000 nel 2024 – un incremento del 38%. Le proiezioni per il 2025, basate sul trend del primo semestre, indicano un possibile superamento delle 50.000 vulnerabilità annue.

Non sono semplici statistiche: rappresentano la misura del ritmo con cui vengono riscontrate nuove vulnerabilità, ogni giorno, su sistemi vecchi e nuovi. Un trend che racconta, da solo, quanto la superficie d'attacco digitale si stia espandendo. Non sono semplici statistiche: rappresentano la misura del ritmo con cui vengono riscontrate nuove vulnerabilità, ogni giorno, su sistemi vecchi e nuovi. Un trend che racconta, da solo, quanto la superficie d'attacco digitale si stia espandendo.

I tre pilastri della difesa

Come affrontare un'evoluzione così rapida e complessa? Le fondamenta della sicurezza digitale possono essere riassunte in tre pilastri, apparentemente semplici ma spesso trascurati:

1. **Fattore umano** – Formare costantemente il personale sulle tematiche di cybersecurity.

2. **Asset Management** – Mappare e prioritizzare i beni aziendali, digitali e fisici.
3. **Aggiornamento continuo** – Mantenere sistemi, software e infrastrutture sempre allineati alle ultime versioni e patch di sicurezza.

Formazione cybersecurity: il fattore umano e il social engineering

Il primo pilastro è, da sempre, il più fragile. Il *fattore umano* resta il vero motore di ogni organizzazione, ma anche il suo anello debole.

Chi lavora sotto pressione, tra scadenze e obiettivi, è più esposto a truffe informatiche e tecniche di *social engineering*.

L'espressione "abbiamo sempre fatto così" spesso è il segnale d'allarme più evidente: indica un'abitudine cristallizzata, una barriera mentale al cambiamento e, soprattutto, una **sottovalutazione del rischio**.

Pensiamo a una truffa sempre più diffusa: un'azienda riceve una mail apparentemente autentica da un fornitore o cliente storico, con la richiesta di modificare l'IBAN per futuri pagamenti. La comunicazione è perfetta, la firma digitale ricorda quella genuina, l'indirizzo email differisce solo di un carattere o peggio ancora, è proprio inviata dall'email del mittente originale. Bastano pochi secondi di distrazione e un pagamento importante finisce su un conto estero non recuperabile.

Eppure, con una formazione adeguata e una semplice *procedura di verifica interna*, basterebbe una telefonata di conferma per evitare centinaia di migliaia di euro di danni.

Proprio per questo, gli esperti sottolineano che **la cultura della sicurezza** deve diventare parte integrante del DNA aziendale, al pari della qualità o della sicurezza sul lavoro. Investire in formazione continua – anche con *simulazioni di phishing* e scenari realistici – è spesso più efficace di

qualsiasi firewall di ultima generazione.

Asset management IT: mappare l'infrastruttura per difenderla

Secondo pilastro: conoscere ciò che si ha.

Può sembrare scontato, ma in molte aziende l'elenco dei dispositivi esiste solo nei libri contabili, aggiornati dal reparto amministrativo, e non in un inventario digitale dinamico. Senza una mappa precisa dell'infrastruttura, dai server ai dispositivi mobili passando dai software installati è impossibile difendersi in modo consapevole o riconoscere per tempo i rischi.

Un efficace **Asset Management** consente di individuare gli apparati obsoleti, valutarne l'età e programmare la sostituzione. Non dimentichiamo che in ambito aziendale un dispositivo comincia a considerarsi "usurato" dopo due o tre anni di utilizzo continuativo e più diventa vecchio, più le vulnerabilità aumentano e con loro i rischi di rottura.

Un esempio concreto: in molte piccole e medie imprese italiane ancora oggi sono presenti switch o sistemi NAS acquistati oltre cinque anni fa e mai aggiornati. I test S.M.A.R.T. dei dischi segnalano errori critici da mesi, ma "finché funziona..." resta la filosofia dominante.

Eppure, è proprio in quei supporti che risiedono i dati più sensibili: listini, contabilità, progetti, informazioni commerciali.

Un buon asset management, inoltre, non serve solo alla sicurezza: aiuta a **ottimizzare gli investimenti IT**, evitare sprechi e stimare con precisione i costi di manutenzione nel tempo.

Patch management e aggiornamenti: il pilastro più sottovalutato

Il terzo fondamento della sicurezza è anche quello più

trascurato. Ogni sistema, software o dispositivo richiede un ciclo costante di verifiche e aggiornamenti. In un panorama in cui le vulnerabilità crescono del 38% anno su anno, l'inerzia tecnologica equivale a lasciare la porta aperta.

Un dispositivo non aggiornato è come una porta blindata lasciata socchiusa.

Negli audit sulle infrastrutture aziendali, capita spesso di scoprire sistemi di backup mal configurati, antivirus scaduti o firewall privi di patch da mesi. Quando lo si fa notare, la risposta è spesso la stessa: “funzionava correttamente, perché toccarlo?”.

L'esperienza dimostra invece che l'inerzia tecnologica è una delle principali cause di vulnerabilità. I dati dei principali CERT (Computer Emergency Response Team) europei lo confermano: una larga parte degli incidenti informatici degli ultimi anni è derivata da sistemi non aggiornati, configurazioni errate o credenziali deboli.

Software open source in azienda: TCO e costi nascosti

All'interno di questa logica di aggiornamento continuo, merita attenzione il tema del software open source. La filosofia open è un pilastro della ricerca informatica e ha offerto al mondo strumenti straordinari, ma nel contesto aziendale “senza costi di licenza” non sempre equivale a “costo zero”.

Oltre ai vantaggi – assenza di licenze, trasparenza del codice, maggiore flessibilità – esistono costi nascosti: formazione del personale, installazione, test di sicurezza, integrazione con sistemi preesistenti. Una migrazione mal pianificata verso soluzioni open può generare costi indiretti più alti delle licenze commerciali originarie.

Un approccio professionale richiede una Total Cost of

Ownership Analysis su un arco temporale realistico, ad esempio cinque anni. Solo così si può paragonare in modo oggettivo il costo di licenze, supporto tecnico, formazione e manutenzione, valutando il reale impatto sull'azienda.

ISO 27001 e audit interni: la sicurezza come processo continuo

La norma **ISO/IEC 27001**, riferimento internazionale per la gestione della sicurezza delle informazioni, stabilisce che ogni organizzazione debba definire controlli periodici (*audit interni*) per verificare l'integrità dei propri sistemi. Non è una formalità burocratica: significa valutare se quello che si crede sicuro lo sia davvero.

Un audit efficace consente di individuare falle logiche, credenziali condivise, dispositivi dimenticati in rete o processi mai testati.

È anche un modo per **educare alla trasparenza interna**, coinvolgendo ogni reparto nel tema della protezione dei dati. La sicurezza, infatti, non è competenza esclusiva dell'area IT, ma una responsabilità condivisa tra direzione, amministrazione e personale operativo.

Investimenti in cybersecurity: una strategia multilivello per PMI

Arriviamo così alla domanda più frequente: *“In cosa dovrei investire per rendere sicura la mia azienda?”*

La risposta non sta in un singolo prodotto miracoloso, ma in una **strategia multilivello**.

Ecco alcuni principi basilari ma ancora troppo spesso ignorati:

- Mantieni **antivirus e firewall aggiornati** in modo costante.

- Assicurati che il personale tecnico e consulenti esterni siano **formati** e certificati.
- **Limita gli accessi esterni** alla rete aziendale ai soli casi indispensabili.
- Implementa una **segmentazione della rete** per isolare le aree più critiche.
- Adotta politiche di **backup e disaster recovery** testate periodicamente.
- Monitora il traffico anomalo e applica sistemi di *threat intelligence*.
- Mantieni tutti, dal vertice all'ultimo dipendente, **informati e consapevoli** dei principali rischi.

La sicurezza non è un *progetto da completare*, ma un **processo continuo**. Ogni giorno emergono nuove tecniche di attacco: non esistono soluzioni eterne, solo strategie dinamiche.

AI e deepfake: le nuove minacce alla sicurezza aziendale

Il panorama delle minacce digitali sta cambiando velocemente. L'intelligenza artificiale, se da un lato potenzia le difese (con sistemi di rilevamento comportamentale e analisi predittiva), dall'altro rende più sofisticati gli attacchi.

Oggi è possibile generare, in pochi minuti, video o audio di dirigenti aziendali tramite *deepfake* capaci di convincere un dipendente ad autorizzare pagamenti o divulgare dati riservati.

La linea tra realtà e falsificazione digitale diventa sempre più sottile, e la **fiducia** – un tempo basata sul riconoscimento visivo o vocale -perde significato.

Cultura della sicurezza: il miglior

investimento a costo zero

In un contesto dove tutto è connesso – dalle fabbriche automatizzate ai sensori IoT – la sicurezza informatica non può più essere considerata un costo, ma un investimento strategico.

Le aziende che sopravvivono agli incidenti informatici non sono necessariamente quelle più ricche, ma quelle più **preparate**.

Come ricordava Kevin Mitnick, uno dei più noti hacker della storia, “non esiste patch di sicurezza per la stupidità umana”.

In altre parole, la tecnologia è solo metà della difesa.

L'altra metà è la **consapevolezza**, fatta di formazione, cultura e responsabilità condivisa. Ed è l'unico antivirus che non può essere disinstallato.

Profilo Autore



L'Ing. Lorenzo Giustiniani è un ethical hacker e consulente ICT con oltre 20 anni di esperienza in progettazione, sviluppo e gestione di infrastrutture e applicazioni complesse, con un forte focus su cybersecurity, DevOps e processi di digitalizzazione.

Ha ricoperto ruoli di responsabilità come CTO, CISO, project manager e responsabile sviluppo per realtà pubbliche e private, occupandosi di piattaforme a microservizi, integrazione di sistemi, gestione di database e sicurezza delle informazioni, anche in ambito cloud (AWS, Azure) e PNRR. Parallelamente svolge attività di docenza su cybersecurity, networking e trasformazione digitale per enti di formazione e aziende, affiancando alla competenza tecnica una consolidata esperienza di coordinamento team e supporto strategico ai processi di innovazione.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/articoli/cybersecurity-per>

-le-pmi/