

Sicurezza informatica PMI: perché sei un bersaglio

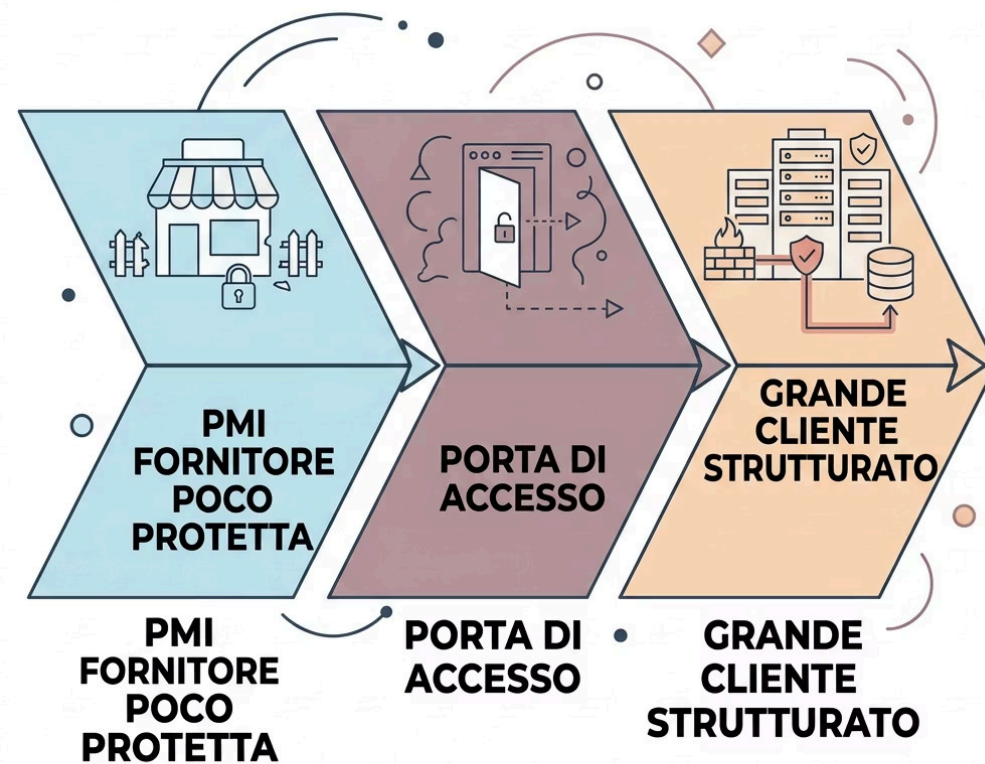
Molti titolari di PMI pensano di essere troppo piccoli per interessare a un hacker. **È proprio questo pensiero a renderli un bersaglio.**



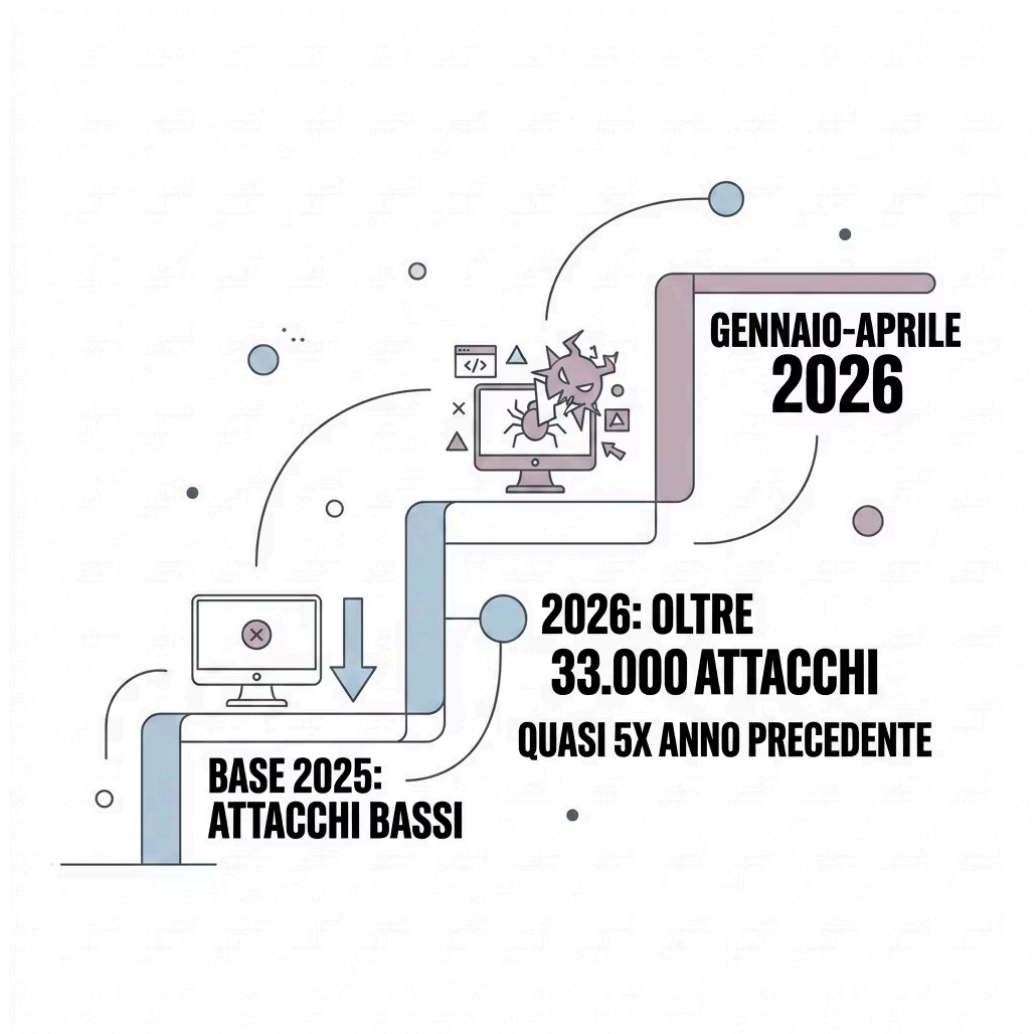
Il vero motivo per cui le PMI sono nel mirino

Le PMI non vengono colpite per quello che hanno, ma per **chi conoscono**. Gli attacchi che sfruttano una piccola impresa come ponte verso un partner più grande sono aumentati significativamente.

⚠ Dal 12,7% al 15,5% dei vettori di accesso iniziale tra il 2024 e il 2025 — la crescita degli attacchi a catena di fornitura.



La nuova esca: malware travestito da intelligenza artificiale



Come funziona la truffa

Link, estensioni e tool apparentemente ufficiali promettono accesso ai servizi AI più popolari. In realtà nascondono **trojan** capaci di scaricare ulteriori **payload** sul dispositivo della vittima.

Link fasulli

URL che imitano portali AI noti

Estensioni false

Plugin che si presentano come AI tool

Payload nascosti

Trojan che si diffondono silenziosamente

Phishing su piattaforme che usi ogni giorno

L'efficacia non sta nella sofisticazione tecnica, ma nella **familiarità**: un dipendente che usa OneDrive ogni giorno non sospetta una notifica di condivisione documento.

OneDrive fasullo

Finte notifiche di condivisione file che reindirizzano a pagine di raccolta credenziali

Facebook policy

Pagine di violazione policy costruite ad arte per rubare accessi aziendali

Zoom Docs

Esche in due fasi su pagine apparentemente legittime di Zoom Docs

Checklist difensiva per la tua PMI

1

Gestisci gli accessi

Limita e revoca tempestivamente i permessi di collaboratori e fornitori non più attivi

2

Igiene delle credenziali

Password uniche per ogni servizio e autenticazione a più fattori (MFA) ovunque possibile

3

Forma il tuo team

Simulazioni reali di phishing, non solo slide teoriche — le persone imparano dall'esperienza

4

Solo fonti ufficiali

Installa software esclusivamente da canali verificati e store ufficiali

5

Fornitori nel perimetro

Tratta ogni fornitore come parte integrante della tua strategia di sicurezza



Non eliminare il rischio: alzare il costo dell'attacco

Nessuna misura elimina del tutto il rischio. Ma ognuna **alza il costo per chi attacca** — l'obiettivo è diventare un bersaglio abbastanza scomodo da spostare l'attenzione altrove.

Vuoi sapere a che punto è la sicurezza informatica della tua azienda?
Richiedi un assessment gratuito — BitAgorà.