La Redazione

Sicurezza fisica e logica: le differenze tra aziende maxi e PMI

“Aziende di grandi e di piccole dimensioni affrontano il tema della sicurezza – sia fisica che logica – in modo nettamente differente: è questa una delle evidenze portate alla luce dalla ricerca Axitea condotta con NetConsulting sugli investimenti delle aziende italiane. Differenza che, in primis, riguarda proprio le figure aziendali che gestiscono la security fisica e logica.

La ricerca pone l’attenzione su un dato: in materia di cybersecurity il 74,3% delle aziende intervistate dispone al suo interno di un It Manager. Un numero molto significativo, ma che riguarda prevalentemente le realtà di grandi dimensioni. Le piccole aziende tendono invece ad affidarsi a società esterne specializzate (11,7% delle risposte). La ricerca di una figura interna, quale l’It Manager, nelle aziende di grandi dimensioni è la risposta alle continue minacce derivanti dallo smart working, modalità di lavoro molto presente in questa tipologia di impresa e che – ampliando il perimetro di attacco – richiede un livello di protezione più elevato.

Decalogo di sicurezza

1. Puntare su tecnologie adeguate, moderne, basate sul machine learning, per bloccare i tentativi di cifratura non autorizzata e per andare oltre il rilevamento basato sulle firme. Occorrono quindi anche competenze idonee.
2. Dotarsi di sistemi per operare frequenti backup cifrati e svolgere esercitazioni di ripristino da questi backup. L’adozione di soluzioni SaaS per il lavoro da remoto facilita i cyber attacchi perché molti lavoratori modificano le impostazioni di firewall e i punti di accesso per connettersi ai sistemi aziendali Software-as-a-Service (SaaS) dalle abitazioni.
3. Implementare difese di elevata qualità in ogni parte del proprio ambiente informatico. Per ogni servizio che si vuole utilizzare, usare accessi indipendenti. Si consiglia l’approccio Zero-trust per cui prima che possa concretizzarsi, ogni transazione di rete deve essere autenticata.
4. No ai server Remote Desktop Protocol esposti su Internet, nemmeno con password cd. “sicure”.
5. Verificare i controlli di sicurezza, per assicurarsi che continuino a soddisfare le esigenze. Eseguire periodicamente vulnerability assessment di tutti gli asset informatici e, ove presenti vulnerabilità medio/alte non rimediabili in tempi rapidi, eseguire un penetration test.

La sicurezza fisica

L'analisi non si sofferma soltanto sulla sicurezza informatica, ma pone l'accento anche sulla sicurezza fisica ed evidenzia come la sua gestione nelle aziende di grandi dimensioni sia in prevalenza affidata alla "Direzione Sicurezza Aziendale" guidata dal CSO (68,6%). Al contrario, le PMI tendono ad affidarsi anche in questo caso a società esterne (12,9%). Questa marcata differenza è determinata per lo più da una realtà organizzativa più articolata nelle imprese di grandi dimensioni rispetto a quelle piccole, caratterizzata da numero elevato di beni fisici da proteggere, un progressivo incremento del numero di sedi e un ampliamento delle dimensioni degli uffici.

I rischi per le PMI

Gli ultimi anni hanno registrato una vera e propria esplosione delle minacce portate alle aziende, sulla scia della crescente adozione dello smart working e della sempre più rapida digitalizzazione.
Ogni azienda ormai deve affrontare il tema in modo prioritario puntando su competenze avanzate e aggiornamento costante, qualità che le realtà più piccole trovano spesso in fornitori esterni specializzati.

Italia fanalino di coda

Secondo Trend Micro Research Navigating New Frontiers nel 2021 l'Italia è diventata il quarto paese al mondo e il primo in Europa più colpito da malware, con un numero totale di attacchi intercettati pari a 62.371.693 (il triplo rispetto al 2020). Secondo un recente sondaggio di Sophos su 5600 IT manager che lavorano in organizzazioni di medie dimensioni in 31 Paesi, gli attacchi dal 2021 al 2022 sono quasi raddoppiati, sono sempre più problematici e comportano un maggiore onere finanziario e operativo per le imprese vittime. Se poi, come si prevede, entro fine 2023 la maggioranza dei dati sarà generata da chi lavora da casa, aumenterà ancora il rischio per la cyber security delle imprese, come è emerso durante la pandemia. Nonostante questi scenari a tinte fosche, la sensibilità delle PMI sul tema cyber pare ancora deficitaria.

Decalogo di sicurezza

Per aiutare le aziende a una corretta strategia di prevenzione, specie in caso venga adottato lo smart working per i dipendenti, contro ransomware, fughe di dati o altri attacchi informatici (con conseguente fermo attività, perdita di dati e pagamento di riscatti), CWS ha rilasciato un decalogo.

6 Svolgere attività di individuazione proattiva delle minacce.

7 Dotare i dispositivi di patch e altri strumenti di remediation. Ogni giorno di ritardo nell'applicare i fix di sicurezza rilasciati dai produttori lascia una falla non solo aperta, ma anche nota (i bug di sicurezza per cui vengono rilasciate patch sono di dominio pubblico) nella sicurezza aziendale.

8 Proteggere i computer: cambiare regolarmente le password, non memorizzare elenchi di password non crittografate, mantenere aggiornato l'antivirus e tutte le applicazioni.

9 Analizzare il proprio traffico di rete per scovare minacce offuscate o al momento in fase passiva di raccolta dati. Le soluzioni di Endpoint Detection and Response (EDR) sono ideali per questo.

10 Formare dipendenti e quadri: spiegare come vengono rubati i dati, stabilire regole e rafforzare anche le soft skill.

Decalogo