

PMI italiane: abbracciare la security convergence per ottenere un vantaggio competitivo

Le piccole e medie imprese di oggi si trovano di fronte a sfide di sicurezza sempre più complesse, che vanno oltre i tradizionali confini della cybersecurity. Nonostante piccoli progressi nella loro postura di sicurezza, l'ultimo Rapporto Cyber Index posiziona l'indice sintetico di sicurezza delle nostre PMI a 52 su 100, segno che stiamo ancora navigando a vista.

In un sistema sempre più interconnesso, dove quasi la metà delle PMI (48%) fa parte di filiere strategiche, la vulnerabilità di un singolo anello può innescare un effetto domino devastante, compromettendo non solo la singola realtà, ma l'intera catena del valore e, in ultima analisi, la stabilità stessa del nostro tessuto produttivo.

La sicurezza non riguarda più solo la protezione dei dati digitali dagli attacchi informatici, ma la salvaguardia dell'intera operatività aziendale in un ecosistema sempre più interconnesso, dove il confine tra fisico e digitale è diventato sempre più labile, fino a dissolversi. È in questo scenario che emerge con forza un nuovo paradigma: la **security convergence**, l'integrazione strategica tra sicurezza fisica e digitale, a garanzia di una resilienza aziendale solida e una continuità operativa sostenibile.



Perché la sicurezza delle PMI non può più vivere a compartimenti stagni

Per troppo tempo, abbiamo concepito la sicurezza come un insieme di compartimenti stagni, con la cybersecurity che si occupava del mondo digitale, mentre la sicurezza fisica di accessi, beni materiali e persone. Questa visione frammentata, purtroppo, è ormai obsoleta e pericolosa.

Un esempio concreto di come la convergenza sia cruciale riguarda un'**utenza ausiliaria in uno stabilimento produttivo** – come un sistema di ventilazione o raffreddamento – che smette improvvisamente di funzionare a causa di un attacco informatico. In assenza di un sistema integrato, il guasto potrebbe, non solo essere rilevato in ritardo, ma anche interpretato come un semplice problema tecnico. Invece, un approccio convergente consente di correlare l'anomalia con eventi digitali sospetti, attivare allarmi mirati e intervenire tempestivamente, **evitando l'interruzione della produzione e salvaguardando la continuità del business**.

La Direttiva NIS2 è un segnale inequivocabile di quanto questa evoluzione sia considerata critica. Ampliando il perimetro di applicazione e introducendo requisiti più stringenti, la normativa ci spinge a ripensare la sicurezza in modo olistico, rendendo la sicurezza un pilastro fondamentale della strategia aziendale.



Trasformare la sicurezza da costo a vantaggio competitivo

È qui che la **Security convergence** si rivela non solo una

risposta, ma una vera e propria opportunità. Integrando sistemi di videosorveglianza, controllo accessi, allarmi e sensoristica con le piattaforme di cybersecurity, si crea un **ecosistema di protezione unificato**. Questo approccio olistico, basato sui dati, ci permette di:

- **Garantire la continuità operativa:** proteggere ogni aspetto del business significa assicurare che l'azienda possa continuare a operare anche di fronte a eventi avversi. Un approccio convergente abilita il monitoraggio e la protezione in tempo reale dei processi e delle attività critiche, permettendo reazioni tempestive a qualsiasi evento che impatti il business – dai sistemi IT alla safety e all'operatività quotidiana.
- **Ottenere una visione completa e in tempo reale:** niente più angoli ciechi. Monitorare simultaneamente eventi fisici e digitali significa identificare correlazioni e anomalie che sfuggirebbero a un'analisi separata per identificare e bloccare minacce ibride, come un attacco informatico veicolato da un'intrusione fisica, o viceversa.
- **Reagire proattivamente e in modo coordinato:** la capacità di analizzare dati provenienti da fonti diverse consente di anticipare gli attacchi, attivare risposte automatiche e coordinare l'intervento di team di sicurezza fisica e digitale. Questo riduce drasticamente i tempi di reazione e minimizza i danni, trasformando la reazione in prevenzione.
- **Ottimizzare costi e risorse:** la gestione unificata delle infrastrutture di sicurezza (ad esempio, un'unica piattaforma per monitorare allarmi, videosorveglianza e eventi cyber) riduce la complessità operativa, i costi di manutenzione e la necessità di personale dedicato. Si passa da una logica di "costo" a una di "efficienza e valore aggiunto".



Perché la security convergence è indispensabile ora

Il tempo, come spesso accade, è un fattore critico. Il divario tra la capacità offensiva dei cybercriminali e la capacità difensiva delle organizzazioni continua ad ampliarsi. Le PMI non possono più permettersi di “sperare” che non accada nulla, ma devono prepararsi a ogni evenienza: adottare un approccio **data-driven** è cruciale. Analizzando i dati provenienti da tutti i sistemi di sicurezza, la Security convergence permette di identificare pattern, prevedere rischi e prendere decisioni informate.

In questo modo, la sicurezza diventa in una leva strategica per la crescita e la competitività, garantendo la sostenibilità e la **Business Continuity** di ogni impresa in un mondo sempre più digitale e interconnesso.

Di Marco Bavazzano, CEO di Axitea

Profilo Autore



Marco Bavazzano, è Amministratore Delegato di Axitea. Dal settembre 2014 ha avviato un percorso di rinnovamento dell'azienda posizionando Axitea nel mercato italiano come il Global Security Provider in grado di assicurare la protezione fisica e cyber delle PMI e delle grandi aziende.

Past President di Asis International Italy e opinion leader nel campo della cybersicurezza, è da più di 20 anni nei settori ICT e sicurezza delle informazioni.

È stato inoltre Vice President di Intellium LTD e Director Security Strategist EMEA in Symantec.

Vanta un'esperienza decennale in Telecom Italia, come Chief Information Security Office e Director Global IT.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/notizie/pmi-security-convergence/>