OPINIONI

CYBERSECURITY

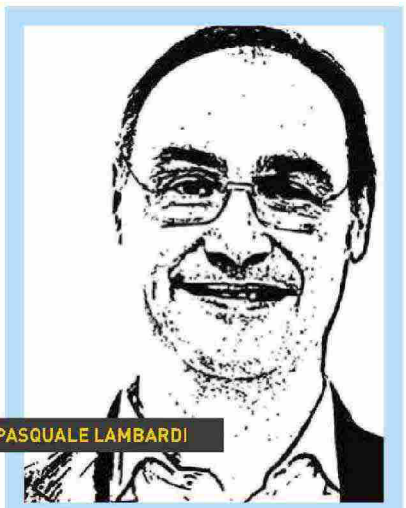
Quantum Computing, IoT Security. L'Intelligenza Artificiale (AI) ha rivoluzionato varie industrie, tra cui la cybersecurity. I grandi benefici introdotti dall'AI, o GenAI, hanno permesso anche ai cybercriminali di fare leva sulle potenzialità offerte dall'Intelligenza Artificiale per lanciare attacchi più mirati, che possono evadere le misure di sicurezza tradizionali rendendo più impegnativo il rilevamento e la mitigazione.
Le organizzazioni devono investire in soluzioni di sicurezza avanzate AI driven per rilevare e rispondere in modo efficace alle minacce emergenti.
Mentre Quantum Computing detiene la promessa di risolvere problemi complessi, pone anche una notevole minaccia agli attuali algoritmi di crittografia. I computer quantistici possono potenzialmente infrangere schemi di crittografia utilizzati per garantire dati sensibili, compromettendo la riservatezza e l'integrità.
Per mitigare questo rischio, alcune normative sono state rilasciate o in fase di rilascio; i termini per prepararsi all'eventuale passaggio ad algoritmi post-quantistici si stanno avvicinando.
L'Internet of Things (IoT) continua a espandersi e rappresenta un asse portante di molti programmi di trasformazione digitale, automazione industriale e consumer. Tuttavia, la proliferazione dei dispositivi IoT introduce nuove sfide di sicurezza, tra cui vulnerabilità del dispositivo, protocolli insicuri e mancanza di gestione centralizzata. Le organizzazioni devono investire nella sicurezza IoT per prevenire potenziali violazioni di una superficie di attacco potenzialmente "infinita" e salvaguardare i dati sensibili.
In un'epoca di minacce informatiche evolute e di trasformazione digitale, la cybersecurity propone uno scenario estremamente dinamico e in continua evoluzione.
Indirizzando i rischi introdotti dalle tendenze emergenti e adottando un approccio proattivo alla sicurezza, le organizzazioni possono efficacemente attenuare le incognite e proteggere i loro dati sensibili implementando un programma Zero Trust, e mettendo un particolare focus su programmi di sensibilizzazione e formazione.

> "UNA STRATEGIA EFFICACE È QUELLA BASATA SULL'APPROCCIO RISK-BASED, CHE CONSISTE NEL RIUSCIRE A MISURARE IL RISCHIO CYBER CONSIDERANDO TUTTI GLI ELEMENTI COINVOLTI E, IN TAL MODO, CREANDO UNA STRATEGIA ALLINEATA CON IL BUSINESS."

PL **Pasquale Lambardi,** Presidente e CEO di Relatech

VISIONE OLISTICA

In un mondo sempre più digitale e connesso, nessuna realtà è al sicuro e le aziende devono essere pronte a proteggersi implementando un adeguato piano di sicurezza. È assolutamente necessario che le aziende comprendano come la cybersecurity sia un tassello indispensabile della strategia di digitalizzazione e, quindi, del loro business.
Una strategia efficace è quella basata sull'approccio risk-based, che consiste nel riuscire a misurare il rischio cyber considerando tutti gli elementi coinvolti e, in tal modo, creando una strategia allineata con il business. Non è conveniente guardare ai servizi e ai prodotti in modo tra loro indipendente: l'integrazione è la strada migliore da percorrere.
Questo è l'approccio di Relatech - che offre una visione olistica per creare insieme ai clienti la strategia giusta -, in linea con ciò che viene maggiormente richiesto dal mercato. Del resto, si tratta di una visione d'insieme che si espleta anche nella convergenza tra IT e OT: per questo Relatech, grazie anche ad altre aziende del Gruppo, come Mediatech ed EFA Automazione, integra in un'unica piattaforma di monitoraggio e gestione degli incidenti cyber entrambi i mondi dell'Information Technology e dell'Operation Technology.
I servizi che eroghiamo con il nostro Security Operation Center ReSOC assicurano i più elevati livelli di efficienza per monitorare costantemente le reti aziendali, gestire le minacce, risolvere gli incidenti provocati da attacchi malevoli in modo rapido ed efficace. Tutto all'insegna di un approccio che, per essere vincente, non può fare a meno di essere allineato e, anzi, integrato con il business.


PASQUALE LAMBARDI

AC **Angelo Candian,** Country Business Segment Manager - Digital Connectivity and Power di Siemens Italy

DIFESA IN PROFONDITÀ

La digitalizzazione rappresenta un elemento ormai imprescindibile di competitività per le imprese industriali, ma, al tempo stesso, aumenta drasticamente il rischio di minacce informatiche.
Gli attaccanti, infatti, stanno im-