Bimestrale
04-2026
Pagina 108/09
Foglio 1 / 2

EUREKA!
CRONACA DELL'INNOVAZIONE

UN PARTNER DI FIDUCIA PER ESSERE PROTETTI

Quello del cybercrime è un mondo troppo complesso e richiede competenze troppo specifiche per essere gestito in modo autonomo dalle aziende manifatturiere. Per questo serve trovare un partner tecnologico di fiducia per la sicurezza informatica. Relatech, con le sue competenze ramificate e un approccio che unisce consulenza, selezione accurata delle tecnologie e servizi su misura, è l'interlocutore ideale.

DI GIOVANNI INVERNIZZI

Nell'industria la sicurezza informatica non si compra, ma si costruisce lavorando fianco a fianco con un partner fidato. È questo il presupposto su cui Relatech ha costruito la proposta della Business Unit Cybersecurity. A spiegare come si articola questo approccio è Andrea Ferrazzi, Cybersecurity Business Unit Director di Relatech. "Non è facile stabilire un rapporto di fiducia con un cliente del settore industriale se non si dimostra di capire le sue esigenze e di parlare il suo linguaggio", dice. "Se non si riesce a stabilire un filo diretto con i responsabili di produzione e i tecnici è complicato perfino avviare un dialogo". Il vantaggio di Relatech, sotto questo aspetto, è di essere una realtà articolata, con "una fortissima competenza nel contesto industriale", osserva Ferrazzi, "rappresentata dalla nostra Business Unit Industrial Automation. Quotidianamente noi abbiamo esperti che si occupano di tecnologie abilitanti e di system integration nel mondo industriale e questa è la chiave che ci permette di strutturare un rapporto di fiducia con le imprese del manifatturiero quando parliamo con loro di cybersecurity".

Non è un dettaglio. In un impianto produttivo sicurezza e continuità operativa sono strettamente connessi. Relatech ha quindi sviluppato le sue profonde competenze sulla OT Security, la sicurezza informatica delle "operations", in stretta connessione con tutte le sue anime, che si esprimono in quattro business unit (Advisory, Digital e AI, Cloud e Cybersecurity, Automazione Industriale), in cui confluiscono le esperienze native dell'azienda e quelle delle molte imprese acquisite negli ultimi anni di grande crescita.

Andrea Ferrazzi, Cybersecurity Business Unit Director di Relatech.

TRE LINEE DI INTERVENTO

Il risultato è un modello organizzativo che si esprime lungo tre linee di intervento: advisory (consulenza), soluzioni e servizi. Ferrazzi entra nel dettaglio. "In ambito advisory", dice, "lavoriamo soprattutto per spiegare ai clienti i contenuti di standard e normative in tema di cybersecurity e ciò che comportano in termini concreti per la loro attività, accompagnandoli in un percorso sartoriale di adozione dei processi. Il legislatore è stato

EUREKA!
CRONACA DELL'INNOVAZIONE

Relatech mette al servizio dei propri clienti strumenti per la sicurezza informatica come il Security Operation Center e l'Experience Center di Genova, dove vengono simulati scenari di attacco e difesa in ambito industriale.

particolarmente prolifico negli ultimi anni. La direttiva NIS2, il Nuovo Regolamento Macchine e il Cyber Resilience Act creano un nuovo scenario in cui le imprese non soltanto devono adeguarsi per rispettare la compliance, ma anche capire che cosa cambia davvero rispetto al passato perché gli scenari di rischio sono molteplici quanto concreti". I tempi sono stringenti, con scadenze rigorose entro il 2027, che incidono non solo sulle aziende manifatturiere ma anche su produttori di macchine, system integrator, sviluppatori di linee automatizzate.
Dal piano della compliance si sviluppano poi esigenze concrete. Qui entra in gioco il secondo stream di azione di Relatech, che riguarda l'offerta di tecnologie. "Abbiamo sviluppato un portfolio di soluzioni indirizzato ad aree specifiche: supply chain security, controllo accessi, microsegmentazione, analisi del traffico per monitorare anomalie, monitoraggi evoluti in ambito IoT e automazione industriale". Relatech non produce tecnologia proprietaria, ma seleziona e integra le migliori soluzioni sul mercato. "Dialoghiamo con tutti i principali vendor, sulla base di un grande lavoro di selezione di tecnologie", racconta Ferrazzi. "Siamo particolarmente impegnati a valorizzare le imprese italiane ed europee, specialmente in un momento in cui c'è incertezza nell'affidare la sicurezza delle infrastrutture a tecnologie sviluppate altrove. Sono molte le piattaforme italiane interessanti che abbiamo individuato e con cui lavoriamo".

L'IMPORTANZA DEI SERVIZI

Il terzo livello d'azione è quello dei servizi. "Parliamo di progettazione, implementazione di piattaforme e servizi gestiti integrati nel nostro Security Operation Center", dice ancora Ferrazzi. Non solo tecnologia quindi, ma gestione continua, active probing per testare l'efficacia delle difese e monitoraggio evoluto. E poi ci sono scenari per consentire ai clienti di toccare con mano l'efficacia della tecnologia e quindi rendersi conto delle logiche e degli impatti che un attacco cyber potrebbe avere sulla loro organizzazione. È quanto succede nell'Experience Center che Relatech ha attivato a Genova, dove vengono simulati scenari di attacco e difesa in ambiente industriale. "I nostri clienti possono vedere cosa accade durante un attacco e come le tecnologie e i servizi vanno a contenere gli effetti della minaccia. Non è una demo commerciale, ma un laboratorio dove si riproducono condizioni reali, si analizzano comportamenti anomali dei diversi dispositivi in campo, si osservano gli effetti di un accesso compromesso. Insomma, un luogo dove la sicurezza informatica diventa esperienza concreta.

DIGITAL TWIN E SECURITY

Ma i servizi possono coprire molti campi. Un altro problema delicato per l'implementazione di soluzioni di cybersecurity nell'OT è, per esempio, quello di testare senza interferire con la produzione. "Un contesto operativo è molto delicato", dice ancora il Cybersecurity Business Unit Director di Relatech. "Safety e continuità del business devono andare di pari passo. Per questo stiamo lavorando con una start-up allo sviluppo di una piattaforma di Digital Twin che permette di replicare ambienti produttivi in modo fedele. In questo modo si possono testare vulnerabilità e debolezze in un contesto non operativo virtuale, senza interessare l'impianto reale e fermare la produzione".
In un mondo fatto di fitti intrecci con fornitori e clienti, un ulteriore aspetto da non trascurare è il governo degli accessi. Anche in questo caso Relatech ha diverse soluzioni in portafoglio. "Dalla supply chain spesso arrivano i rischi più rilevanti", avverte Ferrazzi. "Se un fornitore esterno si porta dietro un computer infetto, tutto quello che si è fatto per proteggere la rete interna serve a poco. Occorre quindi un approccio 'zero trust', con soluzioni in grado di disinnescare il rischio portato da device esterni. Ci sono diversi vendor che propongono soluzioni di questo tipo sul mercato. La nostra scelta è proporle 'as a service', sotto forma di servizi anche perché c'è un tema di competenze: molte aziende non hanno le persone per governare queste tecnologie, per noi è materia quotidiana.".

IMPROVVISARSI NON È UN'OPZIONE

Insomma, in un contesto dove "le vulnerabilità aumentano molto anche in funzione del comportamento umano" e dove "l'economia del cybercrime è complessa e altamente specializzata", l'improvvisazione non è un'opzione.
"Nel mondo della cybersecurity le nostre aziende, sia quelle che utilizzano le tecnologie sia i produttori di macchine e system integrator, hanno la necessità di sviluppare partnership", conclude Ferrazzi. "Affidarsi a qualcuno che possa dare garanzie e che sia un interlocutore con una competenza e una visione ampia, dall'advisory fino al servizio gestito, in grado di dialogare con i diversi attori in campo o di coprire esso stesso la maggior parte dei contesti operativi in modo efficace e concreto.".
È questa la proposta di Relatech per l'industria: una struttura integrata, competenze che parlano il linguaggio della fabbrica, selezione rigorosa delle tecnologie, simulazione realistica degli scenari e servizi continuativi. Perché nella manifattura connessa la sicurezza informatica non è un accessorio. È parte del progetto industriale.