# Cyber security per le fabbriche italiane

di Alessia Cotroneo

DA MEAD INFORMATICA, SYSTEM INTEGRATOR ICT CON PIÙ DI 1500 CLIENTI IN TUTTI I SEGMENTI DI MERCATO, L'ALLARME: IL PERICOLO LEGATO ALLE FALLE NELLA SICUREZZA INFORMATICA DELLE AZIENDE È SOTTOVALUTATO, SOPRATTUTTO NELLA SUPPLY CHAIN

Fioccano ogni settimana, se non ogni giorno, le segnalazioni di attacchi informatici all'interno di aziende e pubbliche amministrazioni. Ma se nell'occhio del ciclone, nei mesi scorsi, sono finiti i siti e i dataset di ministeri e controllate pubbliche per motivi di ordine geopolitico, le ragioni degli attacchi, mirati o casuali, che mietono vittime tra grandi e piccole imprese del tessuto produttivo nostrano sono molto meno notiziabili e più banali: è la concorrenza, bellezza, per parafrasare una celebre citazione cinematografica, con tutto ciò che si porta dietro in termini di segreti industriali, lotta tra competitor e guerre intestine.

Ne sanno qualcosa i professionisti di Mead Informatica Srl, system integrator Ict nato nel 1994 con un organico di 5 risorse, arrivato oggi a oltre 180 addetti distribuiti tra le sedi di Reggio Emilia, Marghera (Ve), Agrate Brianza (MB), Roma. Con più di 1500 clienti in tutti i segmenti di mercato, un fatturato che si aggira intorno ai 25 milioni di euro e oltre 300 certificazioni, Mead risponde alle esigenze di business del mercato enterprise e della pubblica amministrazione, soprattutto in tema di gestione dei cambiamenti e progetti complessi che prevedono integrazione tra tecnologie multicanale. «Ormai gli attacchi informatici alle imprese anche italiane non sono più un'eccezione – sottolineano dalla direzione commerciale – e di esempi ce ne sono moltissimi. Qualche anno fa, un'azienda del distretto ceramico di Sassuolo è stata costretta a fermare la produzione per alcuni giorni, due settimane fa in una nota azienda emiliana un attacco informatico ha bloccato il magazzino verticale. A volte questi attacchi sono dovuti anche a una cattiva progettazione e implementazione dell'impianto di rete. Una banalità, appunto, ma solo apparentemente, dato che è uno scivolone che può provocare danni seri anche solo a causa di una mail con virus annesso, che si propaga velocemente dal settore amministrativo dell'azienda a quello industriale, se non correttamente separati».


Mead Informatica si trova a Reggio Emilia
**www.meadinformatica.it**

Stando ai dati forniti da Mead, nell'ultimo anno, il comparto che ha subito più attacchi informatici è stato quello manufatturiero che ha registrato il +191 per cento rispetto all'anno precedente. Questo aumento è sicuramente dovuto all'incremento esponenziale dei dispositivi IoT e OT che, oggi, richiedono una connessione a Internet. Se Industria 4.0 puntava principalmente alla sostenibilità e alla resilienza dell'impianto produttivo mentre, con il passaggio a Industria 5.0 si andrà verso un approccio human centric, con l'uomo e l'intelligenza artificiale interconnessi nel processo produttivo, per un ulteriore aumento dell'esposizione al rischio cyber.

«Tanto più avanzerà la digitalizzazione e il cloud nelle fabbriche – continuano dall'impresa emiliana – quanto più crescerà l'esposizione al rischio. E il principale problema è la scarsa consapevolezza del management aziendale medio italiano. Nonostante le normative spingano, addirittura quasi obblighino a tenere alta la guardia, il pericolo connesso ai cyber attacchi è molto sottovalutato, soprattutto nella supply chain, dove il rischio è ancora più alto. I grandi gruppi industriali stanno cominciando a intervenire nei processi e nella tecnica della cyber security per mettere al sicuro la loro produzione e i loro segreti industriali ma occorre che gli imprenditori e i manager siano consapevoli del rischio, che nel migliore dei casi è il fermo macchine, considerando che al momento quasi tutta la parte prettamente industriale delle fabbriche italiane è attaccabile, avendo un'età media e un ciclo di vita nettamente più lungo rispetto a qualunque minaccia che viaggia sulla rete. Bisogna migliorare i processi esistenti – concludono da Mead – e integrare i piani relativi alla business continuity con i rischi derivanti dagli attacchi cyber, considerando l'aspetto umano, legale, culturale, procedurale e per ultimo quello tecnologico». •

## UN PERICOLO SOTTOVALUTATO

**Tanto più avanzerà la digitalizzazione e il cloud nelle fabbriche quanto più crescerà l'esposizione al rischio che, nel migliore dei casi, è il fermo produzione**

### *INDUSTRIAL SOC, UNA CONTROL ROOM PER LE LINEE INDUSTRIALI*

Mead ha ingegnerizzato il servizio Industrial SOC con un duplice scopo: garantire la business continuity dell'impianto produttivo in modalità 24 ore su 24; guidare e accompagnare le aziende nel percorso di compliance verso gli standard e le normative (Iec 62443, Dora, direttiva Nis2 e Iso 27001). Industrial SOC è un servizio di cybersecurity che esegue attività di analisi del rischio, progetta e realizza soluzioni di protezione per gli impianti industriali. Si avvale della competenza, in materia di processi e tecnologia, di Lead Auditor (ISO 27001 e 22301) in grado di monitorare, proteggere e rispondere tempestivamente alle minacce. «Con Industrial Soc – spiegano da Mead – è come avere guardie giurate che controllano continuamente anziché il monitor di una banca, quello che succede all'interno della linea di produzione industriale. Il servizio offre un security operation center, una sorta di control room, in cui analisti e ingegneri specializzati in sicurezza industriale controllano tutto in tempo reale. L'obiettivo non è produrre carta o installare nuove tecnologie ma perfezionare la formazione, i processi e le tecnologie già in uso in azienda per garantire il livello di sicurezza necessario».