

I risultati dell'indagine realizzata da Zerouno Informatica & Fasternet, Iobo, Csmc e Kaspersky SICUREZZA, UN PILASTRO DELL'INDUSTRIA 4.0

Anita Loriana Ronchi

È ancora lungo il percorso della messa in sicurezza delle reti industriali. Se le attività di hackeraggio diventano sempre più sofisticate, e di conseguenza i rischi più elevati ed estesi ad aree ritenute finora inattaccabili, d'altra parte le aziende dedicano tuttora poca attenzione a questa voce fondamentale del processo di digitalizzazione.

La cybersecurity fa parte dei nove pilastri dell'Industria 4.0. Ma, mentre i sistemi attinenti a robotica, IoT, big data sono stati negli ultimi anni significativamente implementati, lo stesso non può dirsi per la protezione delle reti aziendali. Eppure i rischi non sono più legati soltanto al fermo impianti o alla perdita di dati: cosa succederebbe se esistesse la possibilità di modificare i parametri di produzione, inviandoli da un Plc a un nodo utilizzatore, senza che nessuno se ne possa accorgere? Non è uno scenario da fantascienza, e ad essere

maggiormente vulnerabili sono le piccole-medio imprese.

Vero che, in generale, sta avanzando una presa di coscienza della pericolosità del cyber crime (reato che ha superato nel mondo il narcotraffico, producendo un giro di 76 miliardi di dollari) e sono allo studio soluzioni tecnologiche evolute per far fronte al problema. Tuttavia siamo ancora agli inizi di un cammino virtuoso. Dato da cui muovono le conclusioni dell'indagine realizzata da Zerouno Informatica Spa & Fasternet, Iobo members - Csmc - Kaspersky su un campione di aziende manifatturiere bresciane di diversi settori merceologici, il cui fatturato rientra in un range dai 30 ai 150 milioni di euro e che impiegano dai 150 ai 2.000 dipendenti. La survey segue a un primo evento in materia, svoltosi a febbraio, ed è stata presentata nella sede di Omr, con i responsabili delle società organizzatrici, il supporto di Alvise Biffi, delegato di Confindustria e i manager

Raffaele De Benedetto (Omr Automotive Group), Andrea Ferrari (Streparava), Alessandro Sala (Ferrari Spa), Fabio Sammartino (Kaspersky), moderati dall'esperto Primo Bonacina.

Cinque le macroaree in cui è articolata l'inchiesta, comprendenti persone e procedure, architettura e topologia, sicurezza fisica, accesso e identificazione, gestione e mantenimento. I punteggi ottenuti tramite le «interviste assistite», disposti in una scala da 1 a 10, rimandano una sostanziale mediocrità per tutte le voci, dove migliore è il risultato riguardante la sicurezza fisica, ma appaiono limitate le competenze specifiche (la figura del Ciso), la documentazione non viene aggiornata sistematicamente e le reti Ot non segmentate e separate da It. Altri elementi di debolezza concernono la propagazione delle reti wifi all'esterno, le scarse policies sui device, le soluzioni di monitoraggio poco evolute e l'uso di utenze generiche e non nominali.

