Sicurezza e reti aziendali Il grave ritardo di Brescia

Il convegno in Omr: mancano tecnici specializzati, soprattutto nelle Pmi

Altro che *advanced analytics*, qui c'è ancora bisogno di ripassare i fondamentali. Se il verbo di Industria 4.0 ha ormai fatto breccia nei piani aziendali del manifatturiero bresciano, con un tasso di connettività fra le linee di produzione che è salito esponenzialmente dal decreto Calenda in poi, non altrettanto si può dire per l'altra faccia della *digital transformation*, quella cioè più nascosta ma altrettanto importante che è la sicurezza informatica.

Allarmante — data la portata del fenomeno hacker che nel 2018 ha toccato i 76 miliardi di dollari di giro d'affari globale, più di quello del narcotraffico, per intendersi — il livello di impreparazione del terzo sistema economico d'Europa, almeno a scorrere i dati contenuti nella ricerca realizzata da Fasternet, Iobo, Zerouno, Csmt e Kaspersky e presentata ieri nella sede di Omr a Rezzato. «Nessun programma di formazione dedicato agli utilizzatori delle tecnologie digitali e connesse in azienda, nessuna procedura scritta in caso di emergenza, scarsa conoscenza delle tecnologie utilizzate e delle sue criticità, insufficiente consapevolezza delle vulnerabilità delle reti wi-fi, ugualmente insufficienti policy di controllo sui device utilizzati, dai protocolli di accesso alla identificazione degli utenti, e poi reti spesso e volentieri non segmentate, il che significa che ogni singola via d'accesso, dal wi-fi alle porte fisiche presenti sui macchinari, sono autostrade che possono condurre gli hacker dritti nel cuore dell'azienda» hanno sintetizzato Daniele Rovetta del Csmt e Alberto Zanetti di Zerouno Informatica.

La qualità degli attacchi, tra l'altro, è ormai oggetto di letteratura: «In un'azienda farmaceutica — ha spiegato Alvise Biffi, responsabile del gruppo tecnico cybersecurity di Confindustria — gli hacker hanno modificato la composizione di un farmaco e hanno chiesto un riscatto per permettere all'impresa di individuare quale lotto, ormai sul mercato, fosse stato alterato. Nel settore automotive sono stati hackerati dei robot addetti alla saldatura. Il risultato è stato il ritiro di un'intera commessa dopo i problemi di sicurezza riscontrati dagli automobilisti. Sono stati violati persino dei pacemaker che rilasciano insulina». Tipologie molto diverse di attacchi — dall'esfiltrazione di dati sensibili alle richieste di riscatto fino al fermo macchina per favorire i competitor — che non colpiscono solo le grandi aziende: «Il 43% degli attacchi sono rivolti a Pmi» ha proseguito Biffi.

«La cybersecurity è spesso vista come un costo e una questione per tecnici It— è stato il ragionamento di Giancarlo Gervasoni della rete Iobo — tuttavia le ripercussioni degli attacchi possono essere devastanti e per questo il tema della sicurezza informatica deve diventare centrale per le aziende, interessando dalle prime linee del management fino all'ultimo collaboratore».

Massimiliano Del Barba
mdelbarba@corriere.it

76

Miliardi di euro
È il giro d'affari raggiunto a livello globale nel 2018 dal business della cybersecurity

43%

La quota
di attacchi hacker a impianti industriali che sul totale ha interessato in Italia le Pmi