

L'ANALISI. Presentati i risultati dell'indagine condotta da Csm, Kaspersky, Fasternet e Zerouno

Cybersecurity: il «made in Bs» è consapevole, ma in ritardo

Le minacce informatiche sono considerate un rischio non indifferente dalle Pmi del territorio: formazione e rimedi, però, sono sottovalutati

Più consapevoli, ma non ancora attrezzate contro gli attacchi informatici alle reti industriali e molto in ritardo nella formazione. È la fotografia delle aziende bresciane scattata dall'indagine, realizzata da Csm, Kaspersky, Fasternet e Zerouno Informatica negli ultimi mesi in alcune realtà del territorio. Anche se non ha un valore statistico, il risultato è interessante e mette in luce come, nonostante le cyberminacce siano considerate un rischio non indifferente per le Pmi del territorio, la cybersecurity è ancora un aspetto sottovalutato anche nelle realtà dove il 4.0 è una realtà consolidata.

LA RICERCA, presentata durante un incontro alla Officine Meccaniche Rezzatesi (gruppo OMR di Rezzato), ha coinvolto realtà industriali (i cui nomi non sono stati resi noti per motivi di riservatezza e di sicurezza) con un numero di dipendenti compreso tra 150 a 2.500 e un fatturato tra i 30 e i 350 milioni di euro. I risultati dello studio, condotto sotto forma di intervista guidata, sono stati analizzati da un team specializzato in sicurezza informatica, che ha suddiviso le risposte in cinque macroaree basandosi su standard ricono-

I risultati			
RISULTATI (0-10)	VALORE MINIMO	VALORE MASSIMO	VALORE MEDIO
MACROAREA «PERSONE E PROCEDURE»			
FIGURE	2,67	10	5,08
PROCEDURE	1,85	4,44	2,78
FORMAZIONE	0,48	1,9	1,31
DOCUMENTAZIONE	0	2,5	1,46
MACROAREA «ARCHITETTURA E TOPOLOGIA»			
PROGETTAZIONE E CERTIFICAZIONE	3,15	6,85	5,09
SEGMENTAZIONE E CONTROLLO	1,25	6,67	3,44
BUS DI CAMPO	0	2,78	1,67
MACROAREA «SICUREZZA FISICA»			
CONTROLLO ACCESSI FISICI	3,81	7,62	5,6
CONNESSIONI DI APPARATI E DEVICE	0	5	2,5
MACROAREA «ACCESSO E IDENTIFICAZIONE»			
IDENTIFICAZIONE	2,78	6,11	4,17
POLICIES	0,67	5,67	3,08
ACCESSO REMOTO SOGGETTI TERZI	5,56	7,78	6,67
MACROAREA «GESTIONE E MANTENIMENTO»			
ASSET MANAGEMENT	0,91	5,15	3,9
MONITORAGGIO	3,33	4,44	4,17
SOLUZIONI DI CYBERSECURITY	0	3,33	1,94

sciuti a livello internazionale: «Persone e procedure», «Architettura e topologia», «Sicurezza fisica», «Accesso e identificazione» e «Gestione e mantenimento». Per giungere a un risultato misurabile si è scelto di assegnare un punteggio alle domande e alle risposte così che, relativizzando quanto emerso con i riscontri di un'ipotetica azienda «ideale», si potesse avere un ritorno immediato sulla situazione della rete industriale analizzata e capire

le aree su cui intervenire.

I RISULTATI mostrano «una situazione drammatica», come l'ha definita Alberto Zanetti di Zerouno Informatica: «La formazione è praticamente assente, nonostante i responsabili della cybersecurity siano la prima figura che deve intervenire in caso di attacco - ha spiegato -. Anche nella progettazione e nella realizzazione delle reti non c'è la necessaria cura». I valori medi rilevati dalla ricerca

sono tutti molto bassi, quasi tutti inferiori a sei (non da intendere come soglia della sufficienza, che varia in base alle esigenze delle aziende): fatto «dieci» il valore ideale, la formazione ha totalizzato 1,31, la documentazione 1,46, la progettazione delle reti 5,09, le soluzioni di cybersecurity 1,94. «Spesso si adottano le soluzioni utilizzate nel mondo dell'ufficio, ma non è assolutamente sufficiente: c'è ancora molta strada da fare», ha concluso Zanetti. •