Dati rilevati dagli Enti certificatori o autocertificati
Tiratura 12/2016: 158.319
Diffusione 12/2016: 194.405
Lettori Ed. II 2016: 843.000
Quotidiano - Ed. nazionale

Il Sole 24 ORE
Dir. Resp.: Guido Gentili

30-MAG-2017
da pag. 5
foglio 1 / 2
www.datastampa.it

IMPRESE E ATTACCHI INFORMATICI

Pmi e cybersecurity: investimenti all'anno zero

Andrea Biondi e Matteo Meneghello ▸ pagina 5

Cybersecurity, Pmi all'anno zero

Nel 2016 investiti solo 250 milioni di euro per proteggere gli impianti e i dati

I pericoli

Industria 4.0 ha aumentato le connessioni con l'esterno e i rischi di attacchi informatici

Lo stato dell'arte

Il 93% degli investimenti poco consapevoli Il 9% dei piccoli ha piani di formazione

SUL CAMPO

Molte realtà non hanno mai fatto un backup La denuncia: sono frequenti i casi di imprese che pagano riscatti dopo attacchi pirata

Andrea Biondi
Matteo Meneghello

«Conosco molti imprenditori che hanno pagato il riscatto ai pirati. Se non hai fatto almeno un backup non hai scampo». È l'esperienza vissuta sul campo che porta a questa considerazione amara Giancarlo Turati, past president della Piccola Industria dell'Aib e titolare di Fasternet, azienda che fornisce servizi informatici a largo raggio. Quasi una dichiarazione di impotenza, soprattutto se letta alla luce dell'attacco informatico dei giorni scorsi attraverso il ransomware WannaCry.

Il campanello d'allarme è risuonato forte. Anche perché la situazione rischia di precipitare all'interno delle fabbriche, dove i macchinari oggi sono sempre più connessi e dipendenti dalla capacità di raccolta, trasmissione e analisi di dati. Proprio per questo motivo il Governo sta cercando di intervenire con il piano Industria 4.0, che ha tra i suoi pilastri anche l'agevolazione degli investimenti delle imprese in cybersicurezza. «Il Piano è fondamentale per l'evoluzione del sistema industriale italiano. Sarebbe però altrettanto importante, come peraltro già evidenziato, trovare le modalità con cui gestire anche servizi continuativi, come l'ingaggio di esperti di sicurezza, che sono particolarmente importanti e non sono coperti dalle modalità di incentivazione introdotte da Industria 4.0», spiega Giorgio Mosca, presidente Steering Committee Cybersecurity di Confindustria Digitale, associazione che sta lavorando alla creazione di un framework di passaggi necessari per mettere in cybersicurezza un'azienda.

«Eventi come WannaCry paradossalmente aiutano. Anche se ora il problema è più di alfabetizzazione che di mancata consapevolezza che il rischio esista», dice dal canto suo Marco De Bellis, di Exage: digital technology integrator, e quindi società che coniuga consulenza strategica e sviluppo di tecnologie. Adesso occorrerà vedere la reazione delle piccole e medie imprese dopo l'attacco cyber di WannaCry. Finora però «andavamo noi dalle aziende. E in meno di un caso su 10 iniziavamo a lavorare con le aziende. In genere poi le soluzioni per la cybersecurity si vendono solo se accompagnate ad altro».

Alla fine quindi, che ci sia o meno la consapevolezza del problema l'altro scoglio da superare è quello della volontà di investire in maniera strutturata. Una recente indagine dell'Osservatorio Information Security&Privacy del Politecnico di Milano ha evidenziato che il mercato delle soluzioni di information security ha raggiunto in Italia nel 2016 un giro d'affari di 972 milioni: +5% rispetto al 2015. Peccato che a spendere siano per il 74% le grandi imprese. Il che però vuol dire che alle Pmi resta solo un 26%: poco più di 250 milioni.

Onestamente non granché in un Paese che, stando all'indice sintetico creato da Accenture, vede l'Italia nelle retrovie con aziende con buone performance nel 29% degli ambiti analizzati (10 su 33): meglio di Germania e Spagna, ma molto peggio rispetto a Uk e Francia. A essere analizzato dalla multinazionale Usa è tutto l'universo delle imprese, ma la consapevolezza ormai acquisita tra le realtà di maggiore dimensione non è ugualmente diffusa nelle realtà più piccole, dove anche l'intrusione attraverso mail pirata e la mancanza di adeguate difese sono quotidianamente il primo fattore di rischio. Proprio sulle Pmi poi, un altro dato dello studio del Politecnico di Milano risulta particolarmente impietoso: il 93% delle Pmi ha dedicato un budget alle soluzioni di information security nel 2016, ma senza un utilizzo maturo e consapevole. A pesare è soprattutto l'adeguamento normativo (48%) con solo il 9% delle piccole aziende (fra i 10 e i 49 addetti) che ha specifici programmi di formazione. «Negli ultimi tempi – spiega Luca Beltramino, managing director di Supernap Italia, che ha un maxi datacenter in provincia di Pavia – qualcosa si sta comunque muovendo. Registriamo un crescente interesse delle piccole imprese per l'affidamento all'ester-

Dati rilevati dagli Enti certificatori o autocertificati
Tiratura 12/2016: 158.319
Diffusione 12/2016: 194.405
Lettori Ed. II 2016: 843.000
Quotidiano - Ed. nazionale

Il Sole 24 ORE
Dir. Resp.: Guido Gentili

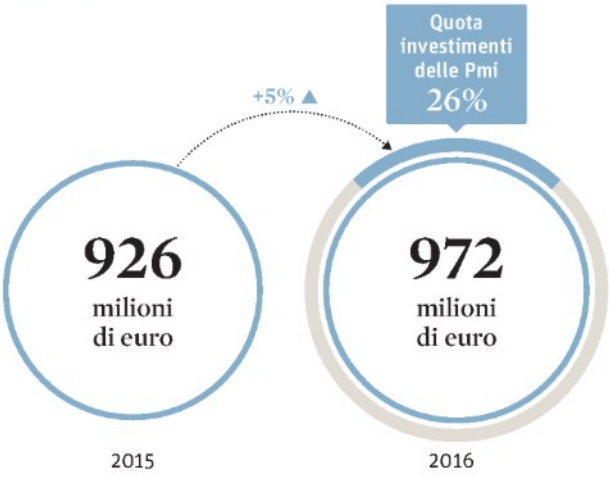
30-MAG-2017
da pag. 5
foglio 2 / 2
www.datastampa.it

no della gestione dei data center». Una spinta che vedono anche i "vendor": «I problemi iniziano a essere più presenti agli imprenditori e il mercato, negli ultimi 12 mesi è diventato sempre più effervescente» dice Francesco Teodonno (Security leader Ibm Italia).

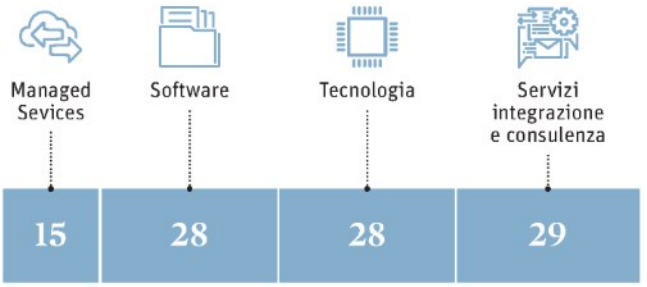
La strada da fare è ancora lunga, nonostante tra i produttori di macchine utensili la consapevolezza dei rischi stia crescendo (Ucimu ha in calendario per fine giugno un seminario sul tema). «Nel mondo della metallurgia - spiega ancora Giancarlo Turati, past president Aib - si sono già registrati, per esempio, episodi di hackeraggio di colate, attraverso l'alterazione dei parametri di temperatura richiesti. In casi meno estremi, si rischia il furto di informazioni sui propri processi produttivi». In tutto questo c'è anche un risvolto paradossale: il tema della concorrenza «oggi preoccupa più di un cyberattacco» spiega Stefano Linari, ceo di Alleantia, azienda che fornisce soluzioni cloud. Cedendo i dati in rete, i potenziali clienti temono di essere esposti a un furto di know how da parte dei competitor. Ma, anche in questo caso, è sufficiente seguire pochi accorgimenti. «È come installare Facebook sul proprio telefonino: bisogna privilegiare soluzioni - sintetizza il manager - che consentono una cessione graduale delle informazioni».

Gli investimenti

IL VALORE DEL MERCATO



IN QUALI AMBITI SI INVESTE
Quota %



Fonte: Politecnico di Milano

Il prontuario

Le sei mosse per tutelare dati e linee dell'impresa

1 Fissare i criteri per una strategia di successo sulla cybersecurity

Stabilire delle linee guida chiare in materia di cybersecurity allineandole alle priorità del business e focalizzandole sulla capacità di rilevare e contrastare gli attacchi più avanzati

2 Effettuare pressure-test sul livello di protezione

Sottoporre l'azienda a simulazioni di attacco, per avere una valutazione delle proprie capacità di difesa e individuare i punti di debolezza

3 Proteggere dall'interno verso l'esterno

È necessario individuare e dare priorità agli asset critici dell'azienda e a focalizzare gli sforzi sulle violazioni che possono avere impatto

4 Proseguire nelle azioni mirate all'innovazione

Investire in soluzioni innovative e all'avanguardia piuttosto che aumentare la spesa in programmi esistenti che si sono rivelati inefficaci

5 Rendere la sicurezza una priorità per tutti nell'azienda

I dipendenti hanno un ruolo critico nell'individuare e prevenire le violazioni. Va garantito un adeguato livello di formazione e di investimento culturale

6 Pensare ad azioni per sensibilizzare il top management

I Ciso (Chief information security officer) devono sensibilizzare la leadership sulla priorità della cybersecurity e sull'impatto che una cattiva gestione può avere sull'immagine e sul valore dell'azienda