21-LUG-2023
da pag. 1-2 / foglio 1 / 2

24 ORE NORDEST
Settimanale - Dir. Resp.: Fabio Tamburini
Tiratura: N.D. Diffusione: N.D. Lettori: 66000 (0001948)

DATA STAMPA
www.datastampa.it

Cyberattacchi e violazioni crescono Le Pmi affinano le contromisure

Il fenomeno. Aumentano le incursioni sui dati sensibili: le minacce non sono più dirette solo alle grandi imprese, anche le piccole sono entrate nel mirino. Parte dal Veneto l'iniziativa Cyber Index per diffondere la cultura della sicurezza e formare professionisti

Subire un attacco informatico è un rischio sempre più concreto per qualunque azienda che usi strumenti digitali.

Le minacce non sono dirette solo alle large corporate, ma anche alle Pmi. Lo dimostrano i dati contenuti nel Rapporto Cyber Index Pmi realizzato da Confindustria e Generali, con il supporto scientifico dell'Osservatorio Cybersecurity & Data Protection della School of Management del Politecnico di Milano e la partecipazione dell'Agenzia per la Cybersicurezza Nazionale. L'86% delle 158 Pmi con sede in Veneto che hanno partecipato al sondaggio utilizza strumenti digitali per supportare la propria attività produttiva: di queste, il 14% ha subito violazioni (ossia attacchi informatici andati a segno) negli ultimi 4 anni.

Un fattore chiave è la diffusione di una cultura della cybersicurezza tra le piccole e medie imprese con l'obiettivo di coinvolgere il maggior numero possibile di imprenditori.

Altrettanto cruciale è formare professionisti in grado di proteggere la normale operatività e il patrimonio digitale delle aziende dalle minacce provenienti dal web, che oltre a essere crescenti sono in costante evoluzione. In questo le università giocano un ruolo di primo piano, con corsi di laurea come quello in Cybersecurity inaugurato nel 2020 all'Università di Padova, che ha già sfornato una cinquantina di laureati e dovrebbe raggiungere il centinaio entro la fine dell'anno accademico. I primi laureati sono di luglio 2022 e il tasso di occupazione è sostanzialmente del 100%: qualcuno continua a fare ricerca, molti vengono assunti da aziende di tutte le dimensioni, compresi Pmi ed enti pubblici.

E poi ci sono le imprese in prima linea, attive nei servizi per i diversi settori e nel monitoraggio 24 ore su 24 delle minacce.

Ganz e **Saini** —*a pag. 2 e 3*

Cyberattacchi, le aziende affinano le contromisure

Il fenomeno. Sono in aumento le incursioni sui dati sensibili e le violazioni. Parte dal Veneto l'iniziativa Cyber Index per diffondere la cultura della sicurezza

14%

OSSERVATORIO
Oltre una azienda veneta su 10 fra quelle intervistate nel Rapporto Cyber Index Pmi di Confindustria e Generali ha subito violazioni

IN TRENTINO
Quasi giornalmente le aziende associate a Confindustria Trento segnalano attacchi: nei primi quattro mesi del 2023 i tentativi stati più di 500

Pagine a cura di
Barbara Ganz
Valentina Saini

Subire un attacco informatico è un rischio sempre più concreto per qualunque azienda che usi strumenti digitali. Le minacce non sono dirette solo alle large corporate, ma anche alle Pmi. Lo dimostrano i dati contenuti nel Rapporto Cyber Index Pmi realizzato da Confindustria e Generali, con il supporto scientifico dell'Osservatorio Cybersecurity & Data Protection della School of Management del Politecnico di Milano e la partecipazione dell'Agenzia per la Cybersicurezza Nazionale. L'86% delle 158 Pmi con sede in Veneto che hanno partecipato al sondaggio utilizza strumenti digitali per supportare la propria attività produttiva: di queste, il 14% ha subito violazioni (ossia attacchi informatici andati a segno) negli ultimi 4 anni.

Quando si tratta di cybersecurity, la consapevolezza è un primo passo, ma fondamentale. Non a caso, Cyber Index Pmi prevede una serie di incontri che, dopo la prima tappa svoltasi a Marghera, proseguirà durante il resto dell'anno a Torino, Genova, Milano,

24 ORE NORDEST
Settimanale - Dir. Resp.: Fabio Tamburini
Tiratura: N.D. Diffusione: N.D. Lettori: 66000 (0001948)

Perugia e Bologna per diffondere la cultura della cybersicurezza tra le piccole e medie imprese con l'obiettivo di coinvolgere il maggior numero possibile di imprenditori.

La formazione

Altrettanto cruciale è formare professionisti in grado di proteggere la normale operatività e il patrimonio digitale delle aziende dalle minacce provenienti dal web, che oltre a essere crescenti sono in costante evoluzione. In questo le università giocano un ruolo di primo piano, con corsi di laurea come quello in Cybersecurity inaugurato nel 2020 all'Università di Padova, che ha già sfornato una cinquantina di laureati e dovrebbe raggiungere il centinaio entro la fine dell'anno accademico.

I primi laureati sono di luglio 2022 e il tasso di occupazione è sostanzialmente del 100%: qualcuno continua a fare ricerca (a Padova, ma anche alla Sorbona), molti vengono assunti da aziende di tutte le dimensioni, compresi Pmi ed enti pubblici.

Impartito interamente in inglese, il corso di laurea magistrale - diretto da Mauro Conti, astro nascente della cybersicurezza italiana (attualmente Editor-in-Chief di IEEE TIFS, la rivista scientifica internazionale di riferimento nell'area della Cybersecurity) - è gestito congiuntamente dai Dipartimenti di Matematica e Ingegneria dell'informazione dell'ateneo padovano. Tra gli insegnamenti, principi di sicurezza delle informazioni, principi e protocolli crittografici, sicurezza software, reti e sistemi cyber-fisici, e strumenti di machine learning.

Trovare lavoro per i laureati in cybersecurity è impresa ben meno ardua che per quelli di altre discipline, in primis umanistiche.

La richiesta di queste figure è altissima, basti pensare che secondo l'Enisa (l'agenzia di Bruxelles per la cybersecurity) nell'Unione Europea mancano all'appello tra i 260mila e i 500mila professionisti del settore. Chi non resta in accademia per fare ricerca viene assunto da enti pubblici e imprese.

In prima linea

Sul campo operano realtà come come Corvallis, azienda padovana con oltre 600 dipendenti, leader in Italia nel settore dell'Information Technology grazie a una esperienza di oltre 40 anni e a un'offerta ampia rivolta al settore bancario, assicurativo, industriale e al mondo della Pubblica amministrazione. Nel 2020 è entrata a far parte del Polo Cyber di Tinexta Group (un gruppo da 357 milioni di fatturato), ampliando così la sua offerta ai servizi.

«Abbiamo seguito i grandi gruppi bancari e assicurativi nazionali - ha affermato il ceo Enrico Del Sole commentando l'entrata in Tinexta Cyber -. Puntiamo a essere il system integrator nel nuovo polo della cybersecurity tutto italiano del quale si sentiva l'esigenza, sia per competere sul mercato e soprattutto per proteggere il know-how nazionale».

A Montebelluna, Treviso, il team del Cognitive security operation center di Yarix - società pioniera del settore fondata nel 2001, oggi a capo della divisione Digital Security di Var Group - segue su un grande schermo quello che può sembrare un wargame, archi che viaggiano veloci da un continente all'altro: si tratta di attacchi che vanno da un server all'altro, minacce informatiche, monitorate in tempo reale, 24 ore su 24, da squadre composte da analisti di sicurezza informatica. Il 2001 era l'anno del worm "Red Code" che infettò 359mila server, quasi una anteprima di quello che sarebbe avvenuto negli anni successivi. Il team Cyber Threat Intelligence di Yarix (YCTI) ha seguito e monitorato fin dalla sua fondazione, tra gli altri, le attività del gruppo hacktivista filorusso NoName057(16) che lo scorso marzo ha messo sotto scacco siti del settore governativo e trasporti (fra cui governo.it, difesa.it, Atm, Atac e aeroporto di Bologna).

«Le compromissioni causate dai moderni ransomware hanno enorme risonanza mediatica, oltre a causare danni considerevoli. Le violazioni, tuttavia, possono causare l'interruzione dei servizi offerti, magari solo temporaneamente, arrecando comunque un danno all'utente finale e di immagine», spiega il ceo e founder Mirko Gatto. Tra i casi più eclatanti gestiti dal CTI di Yarix, lo smantellamento di una rete mondiale di 13mila fake shop in collaborazione con la Polizia Postale: 1.200 in totale i siti fraudolenti associati a 48 marchi italiani, di cui 9 erano famosi brand veneti, il cui nome era sfruttato dalla rete per indurre gli utenti a fare acquisti.

Un attacco informatico è un rischio sempre più concreto per qualunque azienda che usi strumenti digitali

Il fenomeno riguarda le grandi imprese e le Pmi, che a torto credono di non essere un obiettivo appetibile