DATA STAMPA
www.datastampa.it
ItaliaOggi Sette
Dir. Resp.: Pierluigi Magnaschi
Tiratura: N.D. Diffusione: N.D. Lettori: 85000 (0000118)
10-GEN-2022
da pag. 5 /
foglio 1 / 3
Superficie: 100 %

Cyber attacchi, Pmi nel mirino

Imprese medio-piccole sempre più esposte ai ransomware

Le previsioni Trend Micro nello studio Project 2030 scenari per il futuro della cybersecurity

Pagina a cura
DI ANTONIO LONGO

La connettività tra dispositivi, la condivisione di dati e l'intelligenza artificiale stanno cambiando la società e l'economia ma anche la quotidianità di milioni di cittadini. La sicurezza informatica è, però, sempre più a rischio, soprattutto nei prossimi anni. A confermarlo è lo studio «Project 2030: Scenari per il futuro della cybersecurity» curato da Trend Micro che mostra come potrà essere il mondo all'inizio del prossimo decennio e come il settore della cybersecurity risponderà all'evoluzione del crimine informatico. «Speriamo che il possibile futuro delineato susciti un dibattito nel settore della cybersecurity e nella società in generale, solo anticipando attentamente gli scenari futuri possiamo offrire a governi, aziende e individui un modo per prepararsi alle sfide informatiche del prossimo decennio» osserva Lisa Dolcini, head of marketing di Trend Micro Italia. In particolare, gli analisti evidenziano che gli strumenti di intelligenza artificiale permettono anche agli individui senza competenze tecniche di compiere attacchi cybercriminali su larga scala mentre ingegneria sociale e disinformazione diverranno più radicate e difficili da ignorare. Sono soprattutto gli ambienti caratterizzati da un grande numero di dispositivi connessi che attraggono azioni di sabotaggio ed estorsione, soprattutto nei settori manifatturiero, della logistica, dei trasporti, della sanità, dell'istruzione, della vendita al dettaglio.

A fronte di tali scenari, come rileva il Security Leaders Research Report di Vectra, l'89% dei manager che si occupano di sicurezza sostiene che gli approcci tradizionali non siano più in grado di proteggere le infrastrutture dalle nuove minacce e che vadano cambiate le regole del gioco. Peraltro, il 76% del campione ha acquistato strumenti che non si sono rivelati all'altezza delle promesse mentre il 69% pensa che la propria organizzazione potrebbe aver subito una violazione senza che il team di sicurezza se ne sia accorto. «Con l'attuale evoluzione del panorama di minacce informatiche, le difese tradizionali stanno diventando progressivamente inefficaci, le organizzazioni hanno bisogno di strumenti moderni» commenta Massimiliano Galvagna, country manager per l'Italia di Vectra AI.

Pericolo «estorsione» per le medio-piccole aziende europee. Il ransomware, ossia il furto di dati o il blocco di un sistema da parte dei criminali informatici per ottenere in cambio un riscatto, colpirà sempre più l'Europa, considerato che il governo degli Stati Uniti sta stringendo la morsa attorno alle organizzazioni responsabili degli attacchi. E, in particolare, saranno prese di mira anche realtà più piccole. A lanciare l'allarme è Edgard Capdevielle, ceo di Nozomi Networks: «I cybercriminali si sposteranno su obiettivi più facilmente attaccabili ed in paesi dove è meno presente la minaccia di ritorsione da parte dei governi. E mentre si continueranno a vedere richieste di riscatto multimilionarie, allo stesso tempo cresceranno gli attacchi di dimensioni più ridotte».

Lo spettro del dark web. I criminali informatici non si limitano a crittografare i dati e bloccarne il recupero ma procedono alla cosiddetta «data exfiltration», minacciano, cioè, di pubblicare i dati sul dark web o metterli all'asta su internet. «Quest'ultima minaccia è quella che desta le maggiori preoccupazioni, dal momento che nessuna azienda opera più da sola, le attività economiche richiedono ampie relazioni con fornitori, clienti e partner e nessun brand può permettersi il danno reputazionale e l'umiliazione pubblica a cui la esporrebbero i cyber criminali» sottolinea Manlio De Benedetto, director system engineering di Cohesity, «la cyber-resilienza è diventata un bisogno prioritario».

Reati informatici in crescita soprattutto nel Nord-Est. Se nell'arco di 12 mesi il cybercrime ha fatto registrare un vero e proprio boom, con una crescita nel 2020 in tutta Italia del 17,2% di reati informatici rispetto al precedente anno a fronte in una generale diminuzione dei reati (-17,4%) denunciati nello stesso periodo, una vera e propria impennata si è registrata in Veneto (+35,3%), Abruzzo (+29,7%) e Puglia (+26,7%). È quanto emerge dall'analisi condotta dal Centro Studi delle Camere di commercio Tagliacarne che registra una crescita generale dei reati economici (+0,9%), tra cui spiccano i delitti informatici (+19,8%) e le truffe e frodi informatiche (+17%). È soprattutto il Nord-Est ad avere rilevato una crescita delle denunce di reati informatici (+21,3%). Ma in rapporto alla popolazione, la regione più colpita è la Liguria, con 571,7 reati informatici denunciati ogni 100 mila abitanti mentre a rischio criminalità digitale è stata soprattutto Gorizia, con il 50% in più di reati denunciati rispetto alla media italiana.

Il futuro della sicurezza informatica

L'intelligenza artificiale permette anche agli individui senza competenze tecniche di compiere attacchi cybercriminali
Gli attacchi causano il caos nelle filiere delle industrie e danni fisici agli esseri umani che utilizzano impianti cyber
L'ingegneria sociale e la disinformazione diventano più radicate e difficili da ignorare
Gli ambienti caratterizzati da un utilizzo massivo di connessioni tra dispositivi attraggono azioni di sabotaggio ed estorsione
Le tecniche di occultamento attraverso l'intelligenza artificiale rendono impossibile l'attribuzione delle identità
Il 5G e il 6G rendono gli attacchi più precisi e sofisticati
Il tecno-nazionalismo diventa uno strumento geostrategico chiave per alcune delle nazioni più potenti del mondo

Fonte: Trend Micro 2030

La geografia dei reati informatici nel 2020

Pos.	Regioni	Reati informatici *100.000 ab.	Pos.	Regioni	Variazione 2020 /2019 in %
1	Liguria	571,7	1	Veneto	35,3
2	Piemonte	569,1	2	Abruzzo	29,7
3	Friuli-Venezia Giulia	530,1	3	Puglia	26,7
4	Umbria	507,6	4	Umbria	26,4
5	Veneto	481,2	5	Sardegna	21,0
6	Lombardia	474,5	6	Toscana	18,9
7	Valle d'Aosta	473,2	7	Sicilia	18,9
8	Lazio	453,8	8	Campania	18,5
9	Campania	451,2	9	Piemonte	17,7
10	Sardegna	448,6	10	Emilia-Romagna	16,8
11	Abruzzo	431,6	11	Molise	15,9
12	Emilia-Romagna	430,7	12	Marche	14,9

13	Sicilia	428,5	13	Lazio	14,8
14	Toscana	419,1	14	Lombardia	12,1
15	Molise	390,9	15	Basilicata	11,5
16	Calabria	386,2	16	Calabria	7,3
17	Basilicata	360,3	17	Friuli-Venezia Giulia	6,3
18	Puglia	355,9	18	Liguria	4,6
19	Marche	354,1	19	Valle d'Aosta	0,9
20	Trentino Alto Adige	231,8	20	Trentino Alto Adige	-7,4
	Nord-ovest	509,3		Nord-ovest	12,8
	Nord-est	443,7		Nord-est	21,3
	Centro	434,2		Centro	16,9
	Sud	407,9		Sud	19,5
	Isole	433,5		Isole	19,4
	Italia	**450,1**		**Italia**	**17,2**

Fonte: elaborazioni Centro Studi Tagliacarne su dati Ministero dell'Interno – Istat