29-MAG-2023
da pag. 39 / foglio 1 / 2

L'Economia del Corriere della Sera
Settimanale - Dir. Resp.: Luciano Fontana
Tiratura: N.D. Diffusione: N.D. Lettori: 1749000 (0005725)

DATA STAMPA
www.datastampa.it

CYBERSICUREZZA DUE MILIARDI NON BASTANO

Il valore degli investimenti nella protezione informatica, la metà di Francia e Germania. Si può fare di più: solo il 7% delle imprese è in grado di difendersi, contro il 15% della media mondiale. Il 7,6% è già stato preso di mira, con perdite di 500.000 dollari...

Palermo (Fortinet): «In Italia, 3 organizzazioni su 4 riconoscono gli attacchi, ma metà ne rimane vittima»

di **UMBERTO TORELLI**

La battaglia tra aziende e pirati informatici continua senza sosta. Soltanto il 7% delle imprese italiane ritiene di essere in grado di difendersi da un cyberattacco. A livello globale la percentuale raddoppia, il 15%.

È questo il dato saliente che emerge dal «Cybersecurity Readiness Index 2023» di Cisco, il rapporto realizzato dalla società americana per monitorare la preparazione e la resilienza delle aziende nei confronti dei criminali del web. Un'indagine condotta su un campione di 6.700 professionisti di 27 Paesi, tra cui l'Italia, che operano in ambito sicurezza. Al termine, le aziende sono state classificate in quattro gradi di preparazione: «principiante», «formativo», «progressivo» e «maturo».

I numeri

I risultati non sono incoraggianti, visto che nel nostro Paese meno di una impresa su dieci si posiziona nella fase matura, mentre l'8% si trova in quella principiante e il 61% nella formativa, con preparazione inferiore alla media globale. Dice a *L'Economia* del *Corriere* Gianmatteo Manghi, amministratore di Cisco Italia: «l'aumento esponenziale degli attacchi informatici preoccupa per la tipologia delle aziende coinvolte e la facilità con cui vengono portati a termine. Non a caso, la maggior parte degli intervistati si aspetta un'interruzione dell'attività entro i prossimi due anni».

Ma quanto può costare questa vulnerabilità? Dalla ricerca Cisco emerge che una società su quattro, tra quelle colpite da malware (in genere ransomware), ha speso almeno 500 mila dollari per riprendere il controllo completo delle proprie attività. Nel 2022 i gravi attacchi informatici andati a segno in Italia sono stati 188, in crescita del 169% rispetto all'anno precedente. Lo mette in luce l'ultimo rapporto Clusit, l'associazione Italiana per la sicurezza informatica. Si tratta del 7,6% degli attacchi globali. «Parliamo della punta dell'iceberg — dichiara Alessio Pennasilico, del comitato scientifico — ma i numeri sono superiori perché nel nostro Paese chi li subisce spesso non denuncia, nonostante l'esistenza di normative consolidate, come il Regolamento Gdpr e la Direttiva Nis». Il rapporto evidenzia che investiamo per la cybersecurity un miliardo e 850 milioni. Cifra all'apparenza ragguardevole, ma solo metà di quanto spendono Paesi come Francia e Germania. Rispetto al 2021, i comparti più colpiti riguardano l'industria manifatturiera con un +191%. Particolarmente prese di mira anche le organizzazioni informatiche (+100%) e governativo-militari (+65,2%). Ma è la categoria dei cosiddetti «multiple target» a subire maggiormente gli attacchi, con una crescita percentuale anno su anno del 900%. Dunque i cybercriminali tendono a colpire le aziende con obiettivi multipli, piuttosto che singoli attacchi.

Alti livelli di minaccia

La californiana Fortinet ha rilasciato in questi giorni l'edizione 2023 del Global Ransomware Report. Una ricerca condotta a livello globale tra 569 leader in ambito sicurezza informatica provenienti da 31 Paesi, tra cui l'Italia.

Diversi sono i settori interessati, inclusi quello manifatturiero, il comparto hi tech, trasporti e sanità. Ebbene, la minaccia globale degli attacchi ransomware, complice la guerra Russia-Ucraina, rimane ai massimi livelli. «Tre organizzazioni italiane su quattro individuano gli attacchi ransomware, ma metà ne rimane comunque vittima — dice Massimo Palermo, country manager Italia di Fortinet —. Ecco perché è necessario un approccio globale alla security, oltre agli investimenti hi tech, con priorità alla formazione del personale».

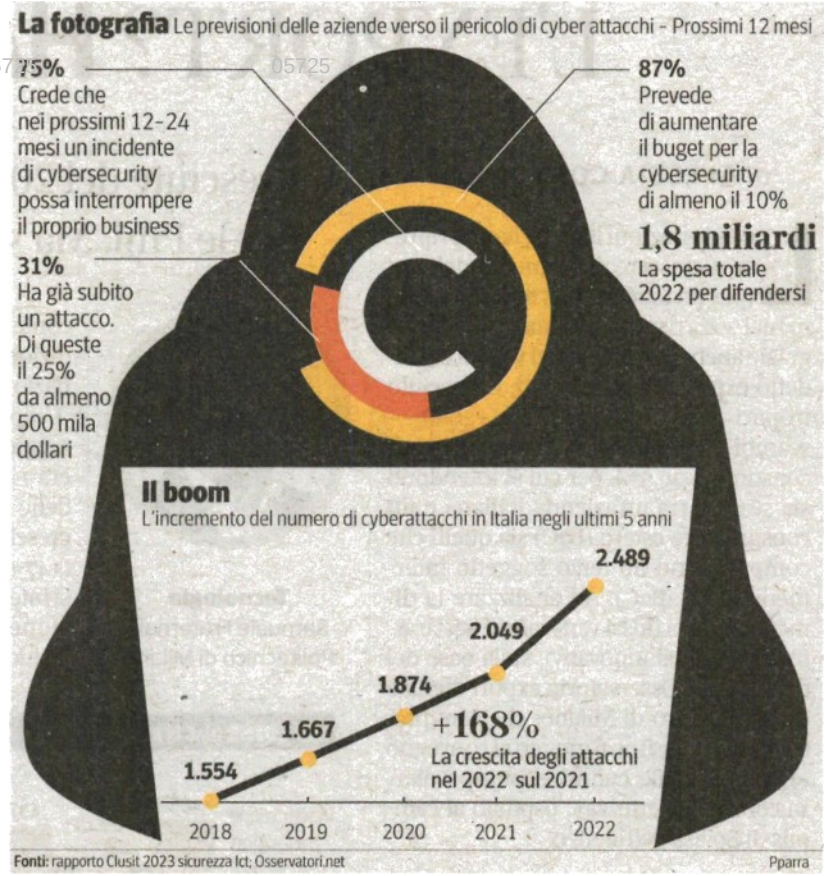
Si accorciano anche i tempi impiegati dai cybercriminali per entrare nelle strutture informatiche aziendali e rubare dati. È quello che in gergo tecnico viene chiamato «breakout time».

Secondo gli esperti della texana CrowdStrike, specializzata in sicurezza informatica, siamo passati da 98 minuti del 2021 a 84 minuti dello

L'Economia del CORRIERE DELLA SERA
Settimanale - Dir. Resp.: Luciano Fontana
Tiratura: N.D. Diffusione: N.D. Lettori: 1749000 (0005725)

scorso anno. Una dimostrazione, se mai ne avessimo avuto bisogno, del miglioramento delle tecniche di attacco.

Intanto crescono in Italia le strutture di controllo. Bip CyberSec ha inaugurato settimana scorsa a Palermo il «Re@ck Security Center». Operativo tutto il giorno per la sicurezza informatica di istituzioni e aziende. Il progetto «Bip nel Mezzogiorno» ha scelto come partenza la Sicilia, dove ha già creato un team di 250 professionisti in ambito digitale.



Il glossario

Adware Visualizza pubblicità indesiderate, compromette privacy

Botnet Una rete di computer infetti, chiamati bot, controllati da remoto

Ransomware Cripta i file, blocca l'accesso richiede un riscatto in criptovalute

Trojan Un cavallo di Troia, si nasconde all'interno di software e consente l'accesso in un secondo tempo.

Personaggi
Gianmatteo Manghi, ceo di Cisco Italy: la maggior parte delle aziende teme un attacco nei prossimi due anni