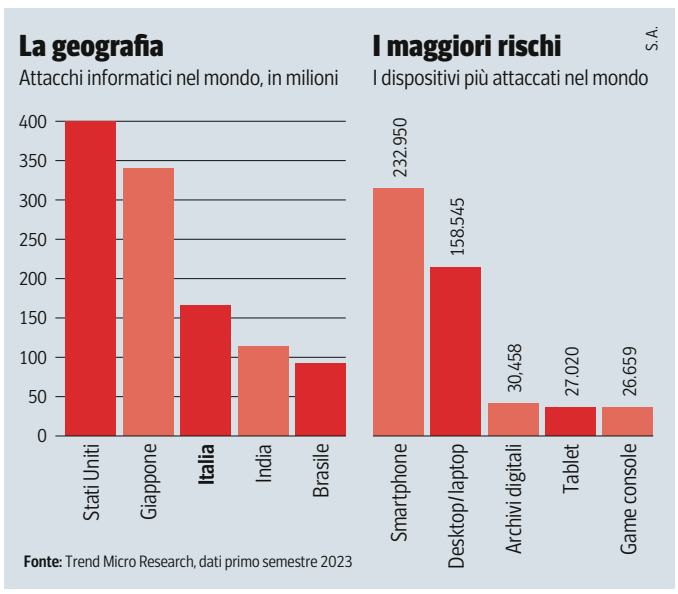
PIANI DI CYBER SICUREZZA LE PMI PRONTE? POCHE

Sono solo il 14%, stando al primo rapporto sulla preparazione informatica delle piccole imprese. Una su cinque è ancora «principiante» nel contrastare gli attacchi pirata

di UMBERTO TORELLI

L'Italia si posiziona terzo paese al mondo e primo in Europa per attacchi informatici. I *malware* che includono virus informatici e *ransomware*, le temibili aggressioni che prima crittografano i nostri dati e poi chiedono un riscatto per restituire le informazioni rubate. Il dato emerge da *Stepping ahead of risk*, il report di Trend Micro Research sulle minacce informatiche che hanno colpito il mondo nel corso del primo semestre 2023. Lo studio della società giapponese conferma ancora una volta che l'Italia è tra i Paesi più presi di mira dai cybercriminali. Il report ha individuato in totale 174 milioni di attacchi da gennaio a fine giugno. Al primo posto si posizionano Stati Uniti con 418 milioni e al secondo il Giappone (355 milioni).



I dati

A scattare un'istantanea sulla situazione della sicurezza informatica nelle aziende del Belpaese è il primo rapporto Cyber Index Pmi 2023, presentato a Roma lo scorso 19 ottobre, realizzato da Generali e Confindustria, con il supporto scientifico dell'Osservatorio Cybersecurity e data protection della School of Management del Polimi e la partecipazione dell'Agenzia per la cybersicurezza nazionale. Per la prima volta vengono definiti parametri di misura sullo stato di consapevolezza delle Pmi sul tema. In particolare lo studio monitora il livello di conoscenza dei cyber rischi, nonché i rimedi adottati per gestirli.

I numeri indicano come la protezione dati diventi un asset aziendale di primaria importanza. Nel nostro Paese dal 2018 al 2022 gli attacchi informatici sono aumentati del 60%. E nel corso del 2022, abbiamo registrato un incremento del 169% rispetto all'anno precedente. E del 191,7% addirittura nel settore manifatturiero, il più colpito vista anche la struttura della nostra economia. «La spesa in cybersecurity in Italia ha raggiunto 1.590 milioni di euro nel 2022, in costante crescita — dice Agostino Santoni, vice presidente di Confindustria per il digitale — a dimostrazione dell'aumento di consapevolezza dei pericoli legati alla sicurezza informatica, considerata dagli imprenditori fattore strategico di competitività».

Le 708 aziende coinvolte nell'indagine raggiungono un cyber index medio di 51 su 100, ma il livello di sufficienza è a 60

La statistica

Le 708 Pmi coinvolte nell'indagine raggiungono un cyber index medio di 51 su 100, con livello di sufficienza 60. Tre i criteri di valutazione adottati. Approccio strategico, identificazione, cioè la capacità di comprendere il fenomeno e le minacce. E infine l'attuazione, che riguarda il livello delle contromisure messe in atto. Emerge come in Italia manchi un approccio strategico con la definizione degli investimenti e della gestione di responsabilità da parte delle società. Qui raggiungiamo un punteggio medio di 54 su 100. Sebbene le leve di attuazione siano maggiormente sviluppate, con un 56 su 100, le Pmi hanno ancora difficoltà nello stabilire priorità d'azione. «Come primo assicuratore nazionale siamo consapevoli della nostra responsabilità e vogliamo contribuire in maniera concreta a diffondere tra le imprese la cultura della cyber sicurezza e consapevolezza dei pericoli informatici — dice Giancarlo Fancel country manager ceo di Generali Italia — per questo ci impegniamo perché nel tempo le Pmi siano più consapevoli su un tema cruciale per il Paese».

Nello studio vengono individuati quattro livelli di operatività aziendale. Il 14% è considerato maturo con un approccio strategico alla materia, consapevole dei rischi e capace di mettere in campo le corrette leve di attuazione. Il 31% viene definito consapevole, in grado di valutare le implicazioni dei rischi, ma capacità operativa ridotta. Il 35% risulta informato, ma non consapevole degli strumenti da mettere in atto e si approccia alla sicurezza in modo «fai da te». Ma ancora una Pmi su cinque rientra nella categoria dei principianti. Poco consapevole dei cyber rischi e con una bassa implementazione delle misure di protezione.

Al fine di aumentare la conoscenza sui rischi cyber e sugli attacchi degli hacker, sono previsti incontri di formazione e workshop su base territoriale. Gli esperti di Generali coinvolgeranno le imprese associate a Confindustria per garantire maggiore consapevolezza sulle problematiche legate a mondo digitale e crimini informatici.

Uno sviluppo dal software alla «nuvola»

Da system integrator a sviluppatore di piattaforme software sulla nuvola informatica. Questo il cammino di CoreTech, intrapreso oltre vent'anni fa per iniziativa del fondatore e attuale ceo, Roberto Beneduci. Negli anni la società milanese ha cominciato a produrre e distribuire soluzioni software. Poi nel 2009 la svolta più importante, motivata dal fatto che molti partner avevano abbracciato sistemi sul cloud computing. L'azienda si è così concentrata su due attività. La distribuzione di prodotti informatici propri e di terzi, nonché l'offerta di una piattaforma online «su misura». Con le infrastrutture per fornire servizi e software di gestione archiviati in data center europei. «La scelta di fornire un'offerta aperta consente di personalizzare le soluzioni», dice Beneduci». Oggi la rete CoreTech conta 1.030 partner attivi e dal 2018 il fatturato cresce del 20% anno su anno Non solo. L'azienda si è dedicata allo sviluppo del mercato estero, con l'obiettivo di proporsi come intermediario tra venditori e clienti. Senza sostituirsi al ruolo dei service provider, ma affiancandoli per potenziarne le soluzioni rivolte alle Pmi. CoreTech è inserita nel circuito Elite della Borsa Italiana, ed è conforme al Codice di condotta Cispe. l'associazione di categoria per i fornitori di servizi cloud. E fa anche parte di Assintel l'associazione in prima linea per lo sviluppo della cultura digital e di CompTia (Computing technology industry association) l'ente americano che rilascia certificazioni per il mercato dell'Information technology, con il compito di garantire la conformità ai requisiti del Gdpr, il regolamento europeo sulla privacy.

Innovazione
Roberto Beneduci, fondatore e ceo di CoreTech. La società fa parte del programma Elite di Borsa Italiana

U. To.

Ora scende in campo l'Ai

E con l'aiuto degli algoritmi difendersi è più facile

Per combattere i pirati informatici le aziende devono ottimizzare soluzioni e risorse interne. Non si tratta solo di contenere il budget, ma risulta necessario far lavorare insieme le diverse tecnologie acquistate negli anni dalle imprese per dotarsi di strumenti di difesa digitali.

Si parla di gestire in modo razionale, sistemi e soluzioni che assicurino la difesa delle singole postazioni (endpoint). A trecento sessanta gradi. Dalle protezioni delle applicazioni sul cloud, ai sistemi di posta elettronica e navigazione web, arrivando alla gestione delle identità e autenticazioni personali. Spiega Marco Rottigni, direttore tecnico di SentinelOne: «la principale criticità è quella di come tutte queste tecnologie possano lavorare insieme secondo flussi operativi ordinati, venendo in aiuto ai team di sicurezza nel momento in cui lo stress è più elevato, vale a dire quando scatta l'emergenza causata da un attacco informatico».

Idee
Marco Rottigni, direttore tecnico di SentinelOne

In Italia si punta ancora a contrastare il cybercrimine con l'installazione di firewall, antivirus e sistemi Edr (Endpoint detection response). Ma la risposta alle nuove esigenze di security arriva da soluzioni globali di tipo Xdr, le cosiddette Extended detection response. In grado di integrare tra loro i vari sistemi di sicurezza e automatizzare i flussi di risposta agli attacchi. Già da qualche anno i criminali informatici usano sistemi di Intelligenza artificiale per amplificare gli attacchi e renderli più efficaci, riuscendo a generare intrusioni coordinate più veloci e difficili da rilevare.

«In quest'ottica anche le aziende si stanno dotando di strumenti intelligenti — dice ancora Rottigni — per difendersi e fronteggiare gli attacchi». Il ruolo dell'Ai nella cybersecurity è fondamentale, sia nel caso dei soggetti buoni, sia per i malintenzionati.

Il principio fondante di SentinelOne è sempre stato quello di essere a favore dei buoni, con l'Ai al centro di tutte le attività. Già anni fa l'azienda ha introdotto nella propria piattaforma modelli di rilevamento statico e comportamentale basati sull'Ai. Migliorando le capacità di rilevare le minacce rispetto ai precedenti approcci troppo legati a password e identificazioni personali.

Ecco perché SentinelOne ha realizzato di recente Purple Ai, un sistema dotato di intelligenza artificiale generativa rivolta agli specialisti di cybersecurity, i cosiddetti «threat hunting».

La soluzione consente di prevenire le minacce fornendo risposte rapide e dettagliate a qualsiasi domanda, riducendo i livelli di complessità necessari per ottenere gli approfondimenti e automatizzando le capacità di agire sulle minacce online.

U. To.