IL SOLE 24 ORE – 30 GIUGNO 2025

Cybersicurezza, nell’area euro investimenti verso i 75 miliardi

Il report. Nuovo approccio difensivo per le aziende. Dalla reazione alla prevenzione: la spesa passa dal 5% di oggi al 50% entro il 2030. Stop alle incursioni con i modelli linguistici di intelligenza artificiale

di Ivan Cimmarusti

Nel giro di cinque anni, la cybersecurity sarà più di una barriera digitale: sarà il metro della solidità aziendale. Lo sarà per chi deve difendere processi, reputazione, forza lavoro. E lo sarà per chi vuole sedersi al tavolo degli appalti, firmare contratti con la pubblica amministrazione, restare agganciato alle catene produttive. Perché una società sicura è anche una società appetibile.

Lo sa bene il 90% dei consiglieri d’amministrazione interpellati a livello globale: per loro la sicurezza digitale è diventata una priorità, come rivela un report di strategia industriale non divulgabile per questioni di riservatezza ma che Il Sole 24 Ore ha potuto consultare.

Il rischio cyber è così uscito dagli uffici It. È approdato nei consigli di amministrazione ed è diventato materia per figure dirigenziali come i Chief information security officer (Ciso). Perché vulnerabilità digitale significa danno reputazionale, perdita finanziaria, esclusione dal mercato. Come in Italia per Pmi, manifattura e studi professionali: bersagli perfetti, vittime eccellenti di phishing mirato, attacchi alle supply chain aziendali, furti di dati. Sono le armi di un conflitto che non fa rumore ma che frena la crescita e il Pil. E può mandare in tilt intere aziende. Come è successo a una società veneta che, a febbraio scorso, ha dovuto mettere in cassa integrazione 350 dipendenti per colpa di un attacco ransomware, un’estorsione digitale fondata sull’esfiltrazione di dati riservati.

Da questo punto di vista la direttiva Ue Nis 2 ha rinnovato e rafforzato l'impianto normativo. Pensata per i grandi comparti critici è ormai punto di riferimento trasversale per tutte le realtà produttive, vittime non solo di semplici cyber-criminali ma anche di una guerra ibrida con attacchi mirati di origine "statuale" che hanno l'obiettivo di indebolire le economie dei Paesi nemici (si veda l'articolo a destra).

Stando al report, elaborato da un'importante società internazionale di analisi del mercato, il contesto attuale sta innescando una corsa agli investimenti. Il mercato globale della cybersecurity punta dritto ai 309 miliardi di dollari nel 2029, in salita dai 201 miliardi previsti per il 2025. Una crescita spinta da normative più rigide, digitalizzazione accelerata e nuove minacce. Con un tasso annuo composto (Cagr) del 10,6 per cento.

Anche in Europa la curva è positiva. La spesa cyber nell'area euro è oggi a circa 50 miliardi, ma viaggia verso i 75,6 miliardi di dollari entro il 2029, con un Cagr stabile attorno al 10-11 per cento. Ma il 2025 potrebbe segnare una frenata, dicono le stime più aggiornate. Colpa di una crescita economica fiacca, dell'instabilità geopolitica e di tensioni commerciali che rallentano le decisioni d'investimento. A pesare sono anche le politiche statunitensi dei dazi. Le imprese europee, pur consapevoli dei rischi, si trovano così a ricalibrare i budget. E a scegliere: difendersi o rimandare. In Italia – secondo Deloitte – si calcola che il 52% delle aziende prevede un aumento degli investimenti di cybersecurity entro i prossimi due anni, in considerazione del numero di attacchi che ogni anno subiscono in particolare le realtà private (si veda il grafico) anche «a seguito delle tensioni geopolitiche che si registrano», ha detto il direttore dell'Agenzia per la cybersicurezza nazionale Bruno Frattasi.

Nel frattempo, la tecnologia corre e i metodi di attacchi cyber si evolvono. La sicurezza cerca di essere al passo. Secondo il report, entro il 2028 le aziende a livello globale muteranno il modo con cui si proteggono. Oggi le imprese gestiscono decine di strumenti di sicurezza, spesso scollegati tra loro. Un labirinto di tecnologie che rallenta i team It e apre nuove superfici d'attacco. Ma il futuro

parla di *platform consolidation*: il 45% delle aziende si affiderà a meno di 15 strumenti per l'intera difesa digitale, rispetto alla frammentazione attuale. Una svolta che punta all'efficienza.

Ma non basta ridurre. Serve anticipare. È qui che entra in scena la *preemptive cybersecurity*: sicurezza che non aspetta il danno per reagire, ma lo previene. Se oggi solo il 5% della spesa It è destinata alla prevenzione, entro il 2030 si salirà al 50%. Un ribaltamento delle priorità: dall'allarme all'anticipo, dal firewall alla previsione. Si investirà in analisi comportamentali, modelli predittivi, automazione intelligente.

A fare da motore, come sempre, l'intelligenza artificiale. Ma stavolta non quella generica. Il cuore della nuova sicurezza saranno i *Domain-specific language models* (Dslm): modelli linguistici progettati per leggere, interpretare e neutralizzare minacce digitali in tempo reale. Oggi li usa solo il 10% delle soluzioni. Nel 2028 saranno integrati nel 75% delle difese informatiche.