Cyber Security, Fastweb fotografa le principali evoluzioni nel panorama della sicurezza italiana per il Rapporto Clusit 2025

In forte aumento (+23%) gli attacchi cyber che crescono per volumi e complessità con oltre 69 milioni di eventi di sicurezza rilevati nel 2024

L'AI sempre più elemento chiave nelle tecniche di attacco e di difesa

Milano, 25 febbraio 2025 – Anche per l'anno 2024 Fastweb, oggi Fastweb + Vodafone, ha contribuito a fotografare la situazione del cyber crime in Italia attraverso il proprio Security Operations Center (SOC), attivo 24/7, e i propri centri di competenza di sicurezza informatica.

L'analisi inserita all'interno del Rapporto Clusit 2025, il report sulla sicurezza ICT dell'Associazione Italiana per la Sicurezza Informatica, ha evidenziato nel 2024 una crescita significativa degli attacchi cyber, segnando una netta inversione di tendenza rispetto alle rilevazione dell'anno precedente e confermando il ruolo sempre più determinante dell'AI nel plasmare il panorama della cybersecurity globale.

Dall'analisi sull'infrastruttura di rete di Fastweb, costituita da oltre 7 milioni di indirizzi IP pubblici e su ognuno dei quali possono comunicare centinaia di dispositivi e server, sono stati registrati nel 2024 oltre 69 milioni di eventi di sicurezza, in aumento del 23% rispetto agli eventi rilevati nel precedente report.

Dopo un 2023 in cui il numero degli attacchi è rimasto sostanzialmente stabile, nel 2024 si registra un'escalation delle attività cyber criminali in termini di volumi, complessità e diversificazione. Torna a crescere, infatti, il numero di infezioni da malware (+131%) e botnet (+41%) rilevate in Italia e cresce anche il numero delle famiglie di software malevoli in circolazione (+7%). Anche in ambito DDoS (Distributed Denial of Service), ovvero quelle minacce che consistono nel tempestare di richieste un sito internet fino a renderlo irraggiungibile, si osserva un aumento del numero e della gravità degli attacchi rispetto al 2023, con una crescita del 100% nel volume degli attacchi e un incremento marcato anche degli eventi ad alto impatto con oltre 100 Gbps di banda impiegata.

In linea con i trend rilevati negli anni precedenti i settori più colpiti si confermano la Pubblica Amministrazione ed il Finance&Insurance che insieme costituiscono quasi il 50% dei casi. In particolare, la Pubblica Amministrazione sale al primo posto passando da 560 attacchi nel 2023 a ben 1430 nel 2024 mentre il Finance&Insurance pur rimanendo il secondo settore più colpito, dimostra una maggiore resilienza agli attacchi

registrando un aumento contenuto del 36% grazie all'efficacia delle misure adottate per mitigare le minacce cyber rispetto alla media degli altri settori che supera il 100%. L'aumento più significativo è invece quello del settore Servizi che registra un aumento del +250% rispetto al report precedente.

A fronte di questi fenomeni, la crescente pervasività delle nuove tecnologie come l'Intelligenza Artificiale, sempre più integrata all'interno strategie di attacco ma anche di difesa delle organizzazioni, oltre alla crescente consapevolezza dei rischi informatici, hanno contribuito ad arginare l'incremento degli eventi malevoli. In calo costante dal 2019, infatti, il numero dei server che espongono su internet servizi critici (-11% nel 2024) e diminuisce anche il numero di malware sconosciuti che passa dallo 0,18% nel 2023 allo 0,12% nel 2024, a testimonianza del miglioramento degli strumenti di detection e prevention delle minacce zero-day grazie anche all'impiego dell'AI.

Anche nel 2024 l'integrazione dell'AI nelle infrastrutture di cybersicurezza di Fastweb ha contribuito all'identificazione di anomalie ed eventi malevoli con sempre più efficacia, riducendo la rilevazione di falsi positivi fino al 70% in linea con i trend di settore. Grazie alle capacità dell'AI di raccogliere un maggior numero di informazioni sui *threat actor*, distinguere con maggiore precisione le minacce e riconoscere in anticipo i segni caratteristici degli attacchi cyber, si osserva nel 2024 una riduzione degli eventi malevoli legati al social engineering che sfruttano il fattore umano e le abitudini di navigazione degli utenti, invertendo la tendenza al rialzo osservata nel 2023. Tra questi, gli attacchi legati al "credential phishing" hanno registrato una riduzione del 17%, nonostante questa tipologia di attacco rimanga stabile al primo posto tra le minacce veicolate via email che diventano sempre più credibili, attraverso l'uso dell'AI.

Grazie alla collaborazione con 7Layers, azienda acquisita da Fastweb nel 2020 e specializzata in soluzioni avanzate di cybersecurity, il report include anche il monitoraggio relativo alle minacce informatiche più sofisticate rilevate e contrastate tramite il servizio di Managed Detection and Response (MDR) che ha permesso di identificare i macro trend delle tecniche di attacco più comunemente utilizzate dai criminali informatici. Al primo posto con il 38% del totale si posizionano gli attacchi "Execution" che consentono agli attori malevoli di eseguire codice dannoso all'interno dei dispositivi delle vittime, seguiti dagli attacchi "Initial Access" con il 12% realizzati per individuare potenziali vulnerabilità, mentre gli attacchi di tipo "Exfiltration" che puntano alla sottrazione di dati sensibili rappresentano il 9% degli attacchi.

Per informazioni:
Fastweb + Vodafone Ufficio Stampa

Roberta Dellavedova
Tel. + 348 14 71 722
roberta.dellavedova@fastweb.it