Cyber Security, Fastweb fotografa le principali evoluzioni nel panorama della sicurezza italiana per il Rapporto Clusit 2022

Avanza il cybercrime ma aumenta progressivamente la consapevolezza dei rischi informatici da parte di imprese e PA spinta dalla forte adozione di strumenti digitali a seguito della pandemia.

Milano, 7 marzo 2022 – Anche quest'anno Fastweb contribuisce a fotografare la situazione del cyber crime in Italia fornendo un'analisi dei fenomeni più rilevanti elaborata dal proprio **Security Operations Center (SOC)**. In linea con la nuova strategia "Tu sei Futuro" che oltre a sostenere la digitalizzazione, l'attenzione per l'ambiente e la più ampia diffusione delle competenze digitali nel nostro Paese Fastweb concorre a fornire un ulteriore strumento di conoscenza dei macro trend in corso.

L'analisi inserita all'interno del **Rapporto Clusit 2022**, il report sulla sicurezza ICT dell'Associazione Italiana per la Sicurezza Informatica, ha evidenziato un'ulteriore crescita degli attacchi cyber, che nel 2021 sfiora il 10% a livello globale, contestualmente all'incremento del livello di impatto dei singoli incidenti: il 32% di essi è stato infatti caratterizzato da una severity "critica" e il 47% "alta". In generale, secondo gli esperti Clusit, i cyber attacchi nel 2021 sono stati più mirati e meglio tarati per colpire bersagli specifici, dimostrando che è sempre più forte la mano della criminalità organizzata sul cybercrime.

Dall'analisi sull'infrastruttura di rete di Fastweb, costituita da oltre 6,5 milioni di indirizzi IP pubblici su ognuno dei quali possono comunicare centinaia di dispositivi e server attivi presso le reti dei clienti, si sono registrati oltre **42 milioni di eventi di sicurezza**, con un **aumento del 16%** rispetto agli eventi rilevati nel Report 2021. Al tempo stesso, però, cala in un anno del 16% il numero dei **server e device privi dei livelli minimi di protezione che si attestano a 46.000 in totale.** Negli ultimi anni il numero dei server e dei device esposti è in costante calo a dimostrazione che le aziende stanno progressivamente aumentando le proprie linee difensive.

In Italia tra i macro trend rilevati da Fastweb si osserva la continua crescita dei cosiddetti **malware e botnet,** infezioni che coinvolgono per la maggior parte dei casi le utenze domestiche ma che iniziano ad essere sempre più rilevanti anche nei dispositivi mobili, attraverso link di phishing condivisi grazie a SMS o app di messaggistica. La penetrazione di questa tipologia di attacchi fa segnare infatti un netto **+58%**. Riguardo alla distribuzione geografica dei malware, in Italia nel 2021 si rileva un **aumento del numero di attacchi da server ospitati in Europa** rispetto agli Stati Uniti.

Dopo l'aumento che si era manifestato nel 2020, con un raddoppio degli eventi in alcuni periodi dell'anno a seguito dei forti cambiamenti nel mondo del digitale introdotti dalla pandemia, nel 2021 gli attacchi **DDoS** (Distributed Denial of Service), ovvero quelle minacce che consistono nel tempestare di richieste un sito fino a metterlo ko e renderlo irraggiungibile, sono tornati a crescere in maniera lineare, con 2.500 eventi e circa 18.000 anomalie registrate. I settori più colpiti si confermano il **Finance/Insurance** e la **Pubblica Amministrazione**, obiettivi che insieme costituiscono circa il **50%** dei casi. A questi si aggiunge quello dell'**Industria** che ha presentato l'**aumento più significativo, dal 7% del 2020 al 18% del 2021.**

Per quanto riguarda i tentativi di attacco "applicativo", rivolto cioè ai software dei dispositivi, la maggior parte delle tecniche utilizzate dal cybercrime sono correlate alla raccolta di informazioni e all'accesso ai dati, sfruttando le debolezze del linguaggio di programmazione per la gestione dei database. Dalla rilevazione risulta che la sorgente di questa tipologia di attacchi provenga in gran parte dagli Stati Uniti, seguiti dai Paesi Bassi e dall'**Italia, che si posiziona al terzo posto con una percentuale dell'11%** sul totale.

Il Report di quest'anno si arricchisce anche delle rilevazioni effettuate da Fastweb sui tentativi di intrusione tramite **servizi Mail dove il principale vettore d'attacco, in crescita dell'11%, è l'utilizzo di URL malevoli che vengono impiegati nell'87% degli attacchi.**

Si osserva, in generale, un incremento di tecniche organizzate in più fasi, che variano dall'installazione di **software malevolo al furto dei dati personali degli utenti.** Tra queste il **Credential Phishing** che, nonostante presenti un trend in lieve decrescita, rappresenta sempre la modalità di attacco più utilizzata con un peso del **60%** sul totale.

Da anni partner di riferimento per aziende e pubbliche amministrazioni per i servizi di cyber security, Fastweb ha recentemente inaugurato a Bari un **nuovo Security Operation Center.** e Gestito da un team di specialisti e operativo 24 ore su 24 il nuovo centro si affianca al SOC di Milano per offrire ai clienti accesso alle professionalità e alle soluzioni più avanzate di protezione informatica. Inoltre, Fastweb che nel 2019 2019 ha acquisito per il 70% la società leader nei servizi per la sicurezza informatica **7Layers,** contribuisce attivamente alla diffusione di programmi strutturati di formazione e awareness nel panorama italiano con i corsi in Cybersecurity Analyst e Network Security Architects erogati della **Fastweb Digital Academy** (FDA).

Per informazioni:
Ufficio Stampa Fastweb spa

Roberta Dellavedova
Cel. +39 348 14 71 722
roberta.dellavedova@fastweb.it

Oscar Daniel Berardi
oscardaniele.berardi@fastweb.it