Cyber Security, Fastweb fotografa la situazione italiana per il Rapporto Clusit 2020

Aumentano gli attacchi informatici ma le contromisure adottate hanno contribuito a rendere le reti più sicure

Milano, 5 marzo 2020 - Anche quest'anno Fastweb contribuisce a fotografare la situazione del cyber crime in Italia fornendo un'analisi dei fenomeni più rilevanti elaborata del proprio **Security Operations Center (SOC).** L'analisi inserita all'interno del **Rapporto Clusit 2020** presentato oggi alla stampa, il rapporto dell'Associazione Italiana per la Sicurezza Informatica sulla sicurezza ICT, si basa sugli oltre **43 milioni di attacchi informatici** (in aumento dell'1% rispetto al numero degli eventi rilevati per il Report dell'anno precedente) transitati sull'infrastruttura di Fastweb costituita da più di 6,5 milioni di indirizzi IP pubblici su ognuno dei quali possono comunicare fino a centinaia di dispositivi e server attivi presso le reti dei clienti.

L'analisi effettuata da Fastweb mette in luce **alcuni fenomeni in controtendenza** rispetto agli anni precedenti.

In particolare, accanto alla significativa e costante crescita dei cosiddetti malware, che coinvolgono per la maggior parte le utenze domestiche si evidenzia, rispetto agli anni scorsi, una importante e positiva **riduzione, dal 30% al 7%, degli attacchi di natura DDoS (Distributed Denial of Service) verso la Pubblica Amministrazione,** che nel 2018 occupava il secondo posto nella classifica dei settori più attaccati (per il 2019 si colloca invece al sesto posto). Verosimilmente si tratta di un effetto derivante dalla progressiva introduzione di strumenti di difesa da parte dagli enti pubblici attraverso l'adesione alla convenzione SPC per i servizi di cybersecurity che hanno contribuito a rendere il settore meno remunerativo, e di conseguenza meno attrattivo, per il cyber crime.

A fronte dell'aumento generale degli attacchi DDoS, soprattutto **verso il mondo del Gaming e dei settori Finance/Insurance verso i quali si indirizza il 40% degli attacchi** (seguiti dai settori Servizi, Media&Entertainment, Service Provider) si registra però un effetto positivo sulla durata degli eventi stessi che si è progressivamente ridotta in relazione al progressivo consolidamento delle tecniche di difesa e dei metodi di mitigazione all'interno delle aziende così come delle pubbliche amministrazioni. La **diminuzione della durata a meno di 3 ore per il 95% degli attacchi** costituisce un chiaro indicatore dell'efficacia delle misure adottate dai centri di competenza per il contrasto al cyber crime.

Dall'analisi sulla situazione italiana appare inoltre evidente un **cambiamento nella "geografia" degli attacchi.** Attraverso l'utilizzo di proxy "ponte" che si appoggiano a Paesi (al primo posto gli Usa, seguiti dalla Germania) che generano grandi volumi di traffico legittimo diventa sempre più difficile adottare contromisure basate sulla provenienza geografica dell'attacco: un fenomeno sempre più diffuso e globale che richiede l'adozione di strumenti di difesa sempre più sofisticati e di personale specializzato.

Il Security Operations Center (SOC) di Fastweb che ha effettuato l'analisi è un polo di eccellenza nel quale confluiscono le competenze e le tecnologie più avanzate con l'obiettivo di fornire i più elevati livelli di protezione informatica alle migliaia di piattaforme e collegamenti telematici che la società fornisce a istituzioni e aziende clienti. Il Centro di sicurezza è inoltre dedicato esclusivamente alla gestione dei servizi di sicurezza per le amministrazioni pubbliche e le aziende, attivo 24 ore su 24 per respingere attacchi e prevenire minacce.

Per informazioni:
Ufficio Stampa Fastweb spa

Roberta Dellavedova
Tel. 02 4545 4365
roberta.dellavedova@fastweb.it