Cyber Security, Fastweb fotografa le principali evoluzioni nel panorama della sicurezza italiana per il Rapporto Clusit 2021

Con la «rete» al centro del nuovo modo di lavorare e vivere, il cybercrime si è adattato, cercando nuove forme di vulnerabilità da sfruttare. Nel 2020 si è registrato un aumento del 50% degli attacchi indirizzati ai PC personali e del 37% degli eventi DDoS.

Milano, 2 marzo 2021 – 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 2021** presentato oggi alla stampa, il report dell'Associazione Italiana per la Sicurezza Informatica sulla sicurezza ICT, ha evidenziato alcuni fenomeni in controtendenza rispetto al 2019, diretta conseguenza della pandemia di COVID-19 e del mutamento degli stili di vita che hanno impattato in modo rilevante sulle dinamiche del 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 **36 milioni di eventi di sicurezza**, in netta flessione rispetto agli eventi rilevati per il Report 2020 (- 16%).

La flessione è iniziata principalmente **dopo il primo trimestre del 2020**, in corrispondenza con il lockdown e la remotizzazione del lavoro di molte imprese. L'esposizione di alcune tipologie di servizi (SMB Server Message Block, RDP Remote Desktop Protocol, Telnet,...) si sono ridotti del 18% rispetto al 2019. Analizzando il solo mese di marzo 2020 è stata registrata addirittura una diminuzione di questo indicatore del 63%.

La maggior consapevolezza dei rischi legati agli attacchi informatici in periodo di pandemia ha spinto dunque le aziende ad innalzare i propri livelli di protezione dotandosi di strumenti tecnologici, come ad esempio firewall o VPN per garantire la continuità operativa. Tali strumenti da un lato hanno consentito ai dipendenti l'accesso da remoto alle reti virtuali aziendali, dall'altra ad avere una maggiore protezione perimetrale e una conseguente riduzione della superficie di attacco.

Una novità che, sebbene sia sicuramente positiva, ha spinto i criminali informatici a spostare la loro attenzione verso un punto più debole della catena ovvero verso l'endpoint, il pc del dipendente. Si è infatti notata una **crescita del numero di attacchi indirizzati ai PC personali** (85.000), che sono raddoppiati rispetto allo stesso periodo del 2019, dove si registravano 45.000 infezioni. Questo fenomeno è spiegabile considerando che, durante il periodo di emergenza, molte aziende non sono riuscite a dotare i propri dipendenti di laptop aziendali con conseguente utilizzo di dispositivi personali, solitamente maggiormente vulnerabili a malware e virus.

Un'ulteriore evidenza, del fatto che il cybercrime è in qualche modo evoluto verso tipologie di attacchi più efficaci durante questo periodo di lavoro da remoto, è anche data dal trend degli eventi **DDoS (Distributed Denial of Service)** registrati dal Security Operations Center (SOC) di Fastweb. Il volume degli attacchi DDoS infatti ha toccato i **7 Tbps**, in fortissima crescita anche rispetto al mese peggiore dello scorso anno dove si attestava al massimo a 1.8 Tbps.

In particolare, si è notato un forte innalzamento dei volumi nei mesi del primo e secondo lockdown (marzo 2.2 Tbps, aprile 3.3 Tbps, maggio 5 Tbps, ottobre e novembre circa 6.5Tbps) per poi tornare negli altri mesi a valori in media con l'anno precedente.

Il fenomeno riguarda senza esclusione un esteso numero di settori, tra i quali i più esposti risultano essere il **Finance/Insurance e il mondo dei servizi che sono obiettivo nel 54% dei casi**, seguiti dai settori PA, Service Provider e Media&Entertainment.

Nel "new normal", che ha visto la rete diventare asset irrinunciabile del modo di lavorare e di vivere la società e il cybercrime adattarsi, attraverso nuove forme di vulnerabilità da sfruttare, la sicurezza informatica diventa sempre di più, insieme alla virtualizzazione dei processi abilitata dal cloud, uno dei cardini della trasformazione digitale delle imprese. Un settore in cui **Fastweb opera già dal 2011**, offrendo ad aziende e alla pubblica amministrazione servizi di protezione, analisi delle minacce e gestione preventiva, che aiutano i clienti a individuare le vulnerabilità, e a prevenire e difendersi dagli attacchi informatici.

Nell'ottica della strategia di costante rafforzamento dell'offerta di Cybersecurity, Fastweb ha acquisito all'inizio dello scorso ottobre il 70% di **7Layers**, società leader nei servizi per la sicurezza informatica, fondata nel 2012 a Firenze. La società è stata inserita per quattro anni consecutivi, dal 2017 al 2020, dal Financial Times nella classifica delle mille compagnie che crescono più in fretta in Europa. E recentemente ha ricevuto da Palo Alto Networks, leader mondiale per la cyber security, il riconoscimento di **Next Wave Managed Security Service Provider** (MSSP) per la fornitura a livello globale di servizi gestiti, diventando dunque un partner per l'erogazione di soluzioni di tipo Managed Detection and Response (MDR) per la gestione e mitigazione degli attacchi più evoluti.

Ai servizi principalmente legati alla protezione delle infrastrutture di rete monitorate costantemente dal Security Operation Center (SOC), polo di eccellenza per la fornitura di servizi di sicurezza per le amministrazioni pubbliche e le aziende, attivo 24 ore su 24 e 7 giorni su 7, si aggiungono quindi soluzioni avanzate di Threat Management e di Threat Intelligence, l'area della Security di cui 7Layers è leader, che permettono di aumentare sensibilmente il livello di protezione dell'IT aziendale grazie ad un approccio preventivo e alla capacità di gestione e di mitigazione degli attacchi più evoluti (Managed Detection and Response).

L'integrazione dei servizi offerti da 7Layers consentirà a Fastweb di rispondere a tutte le esigenze di protezione dei propri clienti grazie a un portafoglio strutturato e completo di strumenti di Cyber Security, con la possibilità di avere un controllo diretto end-to-end dell'intero ciclo di vita dei servizi erogati e di rispondere ancora più velocemente alle esigenze del mondo business.

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