DOSSIER Il Sole 24 Ore 29 SETTEMBRE 2022

Dagli hacker più attacchi alle Pmi

Sicurezza informatica. L'Italia figura al primo posto in Europa per gli assalti subiti: per non essere individuati i pirati portano a termine l'operazione nel modo più rapido possibile chiedendo un riscatto per non diffondere i dati sottratti

a cura di Giancarlo Calzetta

1 di 2

AFP In evoluzione. Il numero di cyber attacchi globali è in crescita, ma il panorama delle tecniche utilizzate si sta trasformando: i pirati sfruttano sempre di più le vulnerabilità in software e sistemi operativi

Il fenor

Ransomware, furto di dati, spionaggio informatico, truffe, impersonificazioni, accessi non autorizzati: tutte attività criminali che le aziende devono fronteggiare ogni giorno, camuffate sotto mille forme e in ogni angolo del globo. Dagli ultimi report rilasciati da aziende specializzate e associazioni di categoria, però, sembra che i cyber-pirati amino particolarmente rubare i dati delle aziende del nostro territorio per poi chiedere dei riscatti.

Secondo Trend Micro, infatti, l'Italia figura al primo posto in Europa per numero di attacchi ransomware subiti e ci posizioniamo al settimo posto nella classifica mondiale, dove davanti abbiamo nazioni come gli Stati Uniti (19,69%), Giappone (il cui dato del 10,18% è un po' sfalsato dalla grande diffusione di prodotti Trend Micro nel Paese del Sol Levante), Turchia (7,97%), India (5,11%), Taiwan (4,29%) e Messico (4,00%). L'Italia, con il 3,56% è seguita da Olanda (3,26%), Francia (3,08%) e infine Germania (2,96%) che chiude la top 10.

Secondo Pierluigi Iezzi di Swascan, l'Italia è particolarmente interessata dal fenomeno del Ransomware perché sono molte le aziende disposte a pagare per recuperare i dati criptati dopo l'attacco. C'è da dire che diversi report indicano il numero totale di attacchi ransomware in leggera frenata rispetto al passato proprio grazie al fatto che sono migliorati gli strumenti di resilienza informatica nelle grandi e medie aziende, portando sempre meno aziende a pagare i riscatti richiesti. Purtroppo, a questo rallentamento si contrappone un aumento molto rapido degli attacchi tramite malware condotti nel nostro Paese. Sempre secondo Trend micro, infatti, nella prima metà del 2021 erano stati poco più di 28 milioni, mentre nella prima metà di quest'anno hanno sfiorato gli 83 milioni. In Europa, solo il Regno Unito ne ha subiti di più.

Ma quali sono i bersagli preferiti da questi attacchi? Secondo uno studio del Clusit, l'associazione Italiana per la sicurezza informatica, al primo posto si trovano bersagli legati al settore della Pubblica Amministrazione e Difesa, seguiti da quelli del settore Ict. Al terzo posto dei settori più attaccati si trova la sanità, seguita da istruzione e settore finanziario/assicurativo.

In termini complessivi, quindi, il numero di attacchi globali è in crescita, ma il panorama delle tecniche utilizzate si sta trasformando. I malware restano sempre gli strumenti più comuni per portare a termine le intrusioni informatiche, ma i metodi per farli arrivare sui computer da colpire sono in evoluzione. Fino al 2020, phishing e altre forme di social engineering la facevano da padrone, affiancando il furto di credenziali, ma nel 2021 si è assistito a un balzo in avanti dello sfruttamento delle vulnerabilità in software e sistemi operativi.

Questa tendenza trova la sua spiegazione nella necessità dei pirati di portare a termine gli attacchi nel modo più rapido possibile. Mentre in passato erano disposti a investire anche mesi in una operazione criminale, il fatto che adesso le difese delle aziende sono organizzate meglio rende difficile restare nascosti per lunghi periodi. Questo li porta ad azioni rapide, con infiltrazioni, esplorazioni delle reti aziendali fino a trovare dove vengono tenuti i dati e poi furto dei file. In questo modo si arriva molto velocemente al momento della richiesta di riscatto che è, sempre più spesso, giustificata solo dalla minaccia di divulgare i dati rubati e non dalla criptazione degli stessi.

Ma se questo sembra un miglioramento nel panorama della sicurezza informatica, l'abbondanza di attacchi che va a segno mette a nudo una situazione drammatica per quello che riguarda le fondamenta delle infrastrutture di difesa. I criminali, infatti, ricorrono sempre più spesso allo sfruttamento di vulnerabilità in software e sistemi operativi per infiltrarsi nelle aziende e questo è possibile perché in pochi hanno un sistema davvero efficace di manutenzione dei sistemi. La stragrande maggioranza delle intrusioni, infatti, avviene sfruttando bug conosciuti da mesi, se non da anni, che nessuno si preoccupa di sistemare, nonostante di solito basti solo scaricare un programmino dal sito del produttore del software per chiudere la porta in faccia ai

pirati. La carenza di personale e di organizzazione, però, rende complicatissime queste operazioni banali.

Un altro problema risiede nella scarsa organizzazione che caratterizza i reparti di sicurezza informatica nelle medie e grandi aziende. Anche se spesso i budget a disposizione sono piuttosto consistenti, all'interno mancano le persone con le competenze necessarie a organizzare una difesa ben strutturata oppure sono troppo poche in relazione alla mole di lavoro da svolgere. Di conseguenza, sempre più spesso ci si trova davanti ad aziende che hanno molti prodotti di sicurezza installati sulle proprie macchine, ma nessuno che riesca a gestirli e configurarli in modo da ottenere il risultato sperato. Per questo molti esperti consigliano alle aziende di delegare buona parte della sicurezza informatica a un partner esterno, che possa garantire il funzionamento delle contromisure e la corretta configurazione delle risorse interne in modo da rendere molto difficile il compito dei potenziali aggressori.