IMPARARE A DIFENDERSI DA CIÒ CHE NON SI VEDE

di MARIA MORO

L'ATTIVITÀ IN SMART WORKING HA AUMENTATO L'ESPERIENZA DIGITALE DEGLI UTENTI MA MOLTO MENO QUELLA DEL RISCHIO CORRELATO. LA RETE RIMANE ANCORA UNA TRAPPOLA POTENZIALE, SPECIALMENTE QUANDO SI NAVIGA FUORI DAI PIÙ PROTETTI RECINTI DELLE AZIENDE. IN QUESTO SENSO, LAVORARE E STUDIARE DA CASA HA CREATO UNA PROMISCUITÀ PERICOLOSA DI CUI HANNO BENEFICIATO LE ORGANIZZAZIONI CRIMINALI

Secondo alcuni osservatori, la consapevolezza di imprese e privati sul rischio cyber è in crescita, ma non si può dire che in parallelo sia aumentata in maniera adeguata la capacità di difendersi. Da sempre il rischio di cyber crime si affronta in rincorsa, caratterizzato com'è non da potenziali eventi prevedibili e mitigabili ma da un'attività in continua, e in gran parte imprevedibile, evoluzione. Questa tipologia di rischio è legata a un'aleatorietà non determinata dal caso ma da una forza consapevole di persone che hanno l'obiettivo di creare situazioni di minaccia a proprio vantaggio. È un rischio nell'ambito della criminalità, ma è immateriale e per questo di difficile previsione e individuazione.
Il rapporto **Clusit** ha osservato per il 2021 un aumento degli attacchi gravi del 10% rispetto al 2020 e afferma che i danni stimati lo scorso anno a livello globale siano misurabili in quattro volte il Pil italiano. Nel nostro Paese si sono verificati nel 2021 42 milioni di eventi di sicurezza, in crescita del 16%. Tra le caratteristiche del rischio cyber individuate da Clusit ci sono l'aumento dell'impatto di ogni singolo evento, la maggiore capacità delle organizzazioni di cyber criminali di selezionare i propri obiettivi, il fatto che non esistano settori più esposti di altri e la costituzione di vere e proprie organizzazioni criminali che operano in un mercato illegale.

Ma il fatto che i cyber criminali tengano nel mirino e facciano di tutto per colpire i bersagli grossi non significa che i *pesci piccoli* siano dimenticati. Con loro funziona quella che **Alessandro Curioni**, presidente di **Di.Gi. Academy**, docente e scrittore sui temi del cyber, definisce la "pesca a strascico", un modello con cui le vittime vengono adescate e poi setacciate secondo un sistema che non richiede particolari sforzi, perché è la vittima stessa che cade nella trappola seguendo gli "inviti" del pirata. Forse la percezione del rischio da parte dell'utente privato è aumentata, non si può dire altrettanto invece della consapevolezza nell'affrontarlo anche perché, annota Curioni, "i criminali sono diventati di più e sono più strutturati, una truffa su tre va a buon fine e i loro ricavi sono aumentati. Alle persone più che l'informazione manca quell'esperienza storica che permette di introiettare il rischio e di creare la *forma mentis* che fa tenere un comportamento sempre adeguato".

TROPPO INGENUI PER GLI HACKER

L'esperienza delle attività a distanza durante la chiusura per la pandemia ha avuto un'utilità relativa. "È accaduto che con lo smart working, e con la Dad, si è confuso il confine tra ambito privato e lavorativo e con esso anche i perimetri di sicurezza: abbiamo utilizzato

la rete di casa per collegarci ai sistemi dell'azienda, in contemporanea il resto della famiglia era ugualmente collegato creando un ambiente promiscuo. E se qualcosa di malevolo entra nella rete di casa, poi si trasmette ai sistemi dell'ufficio, e viceversa. Un primo passo utile (oltre a cambiare la password di fabbricazione del router) è di creare da esso due reti, una per l'attività di lavoro o studio e l'altra per il privato".
L'uomo è sempre l'anello debole della catena e carpire la sua fiducia è facile, innanzitutto perché sottovaluta il fatto di poter essere un obiettivo e in secondo luogo perché non sa riconoscere un messaggio malevolo, senza considerare che spesso le truffe sono costruite così bene che è effettivamente difficile riconoscerle. "L'hacker può creare un messaggio assolutamente credibile, ad esempio una comunicazione da parte di una banca con l'informazione di un problema e l'invito a fornire le proprie credenziali: lanciato come *phishing* o *smishing*, tra migliaia di persone ne troverà qualche decina, o centinaia, per le quali il contenuto del messaggio calza a pennello". Non solo: potremmo non essere vittime dirette ma essere usati come tramite per raggiungere un determinato scopo. Per il fatto stesso che curiamo delle relazioni, lavorative o private, possiamo detenere informazioni su un collega, un amico, un familiare, un superiore che inconsapevolmente forniamo allo spione cyber installato nel nostro *device*. È il caso dello *spear phishing*, una forma di "pesca mirata" di informazioni che vengono successivamente analizzate e ricostruite per identificare un obiettivo interessante. I gruppi specializzati in attività cyber illecite operano come in un vero mercato di domanda e offerta, con gruppi specializzati nel ransomware e altri nella raccolta di informazioni: "gli Iab (*Initial access broker*), ad esempio, sono organizzazioni specializzate nella raccolta di informazioni utili a profilare le persone. Le loro fonti sono archivi di varia natura, per esempio frutto di *databreach* che acquisiscono nel *dark web*, grazie ai quali sono in grado di ricostruire veri e propri dossier che vengono venduti. Per intendersi, le credenziali di dieci dipendenti di un obiettivo interessante possono fruttare parecchie decine di migliaia di dollari".

***Alessandro Curioni**, presidente di Di.Gi. Academy*

AGGIRARE L'OSTACOLO TRA SISTEMI DI DIFESA E NUOVI MODELLI

Per quanto riguarda banche e assicurazioni, per Curioni si tratta di settori che oggi possono fare da *benchmark* per gli altri: "Il rischio non è che colpiscano direttamente la banca quanto piuttosto i suoi clienti. Lo stesso vale per le compagnie assicurative, dove il punto debole può non essere la direzione quanto la rete agenziale: i criminali si potrebbero infiltrare nel sistema di posta elettronica dell'agenzia (in genere non quello ufficiale) e da lì osservare gli scambi di email, inserendosi con un account credibile al momento giusto per fornire i dati di un conto corrente falso. In un contesto in cui siamo tutti interconnessi, la criticità è spesso nelle *supply chain*".
Per difendersi possono certamente essere utili gli antivirus e i sistemi *antimalware*. Curioni suggerisce di ovviare al problema delle credenziali poco sicure utilizzando un tool *"password manager"*, oppure, nei siti in cui è prevista, di utilizzare l'autenticazione a due fattori, ma anche in questo campo il "rischio zero" non esiste. Una soluzione per aumentare le difese e ridurre l'esposizione, migliorando la qualità del rischio che le compagnie si assumono, è nel lavorare a monte direttamente con i produttori degli oggetti connessi: "le compagnie possono affiancare i produttori nell'individuare degli standard che migliorino la sicurezza degli oggetti connessi, così da poter vendere il prodotto con inclusa la copertura cyber realizzata su misura. Di fronte alla difficoltà di fare l'*assessment* del rischio, soprattutto per il privato, il focus assicurativo può essere spostato sull'oggetto e sul produttore".