Lo spettro umano dietro la cybersecurity

Cristiano Daolio (Cfo, Altea Federation) e Alessandro Manfredini (Direttore Group Security e Cyber Defence, A2A) dialogano sui punti deboli della sicurezza informatica aziendale. Non solo quelli legati alla tecnologia, ma soprattutto quelli connessi all'elemento umano, lo stesso che, se ben formato, resta il fattore decisivo.

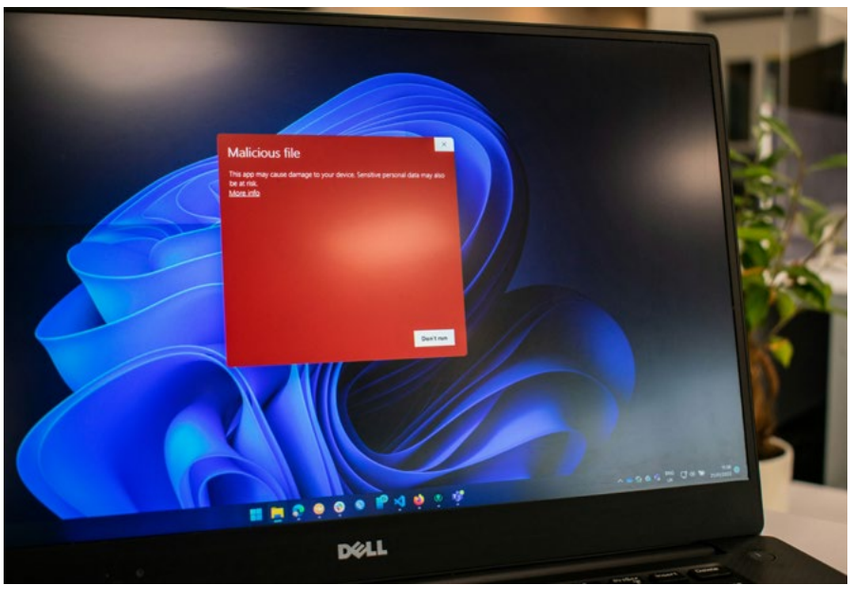
di Riccardo Russo

Nel lessico della sicurezza informatica si parla spesso di firewall, protocolli e intelligenza artificiale, più raramente di persone. Eppure dietro ogni sistema di difesa c'è sempre un comportamento, una scelta presa da un decisore umano che, nello svolgere la propria mansione, può attuare accorgimenti per proteggere i propri dati e quelli aziendali o, per una qualsiasi défaillance, può invece comprometterli. La tecnologia evolve a ritmi vertiginosi, ma resta un dato costante: l'errore umano è ancora la principale vulnerabilità e, se gestito con consapevolezza, anche la migliore risorsa.

Per il ruolo di Manfredini, monitorare lo sviluppo tecnologico è cruciale: «*Ma non si risolve solo con la tecnologia* – sostiene – *il fattore umano è determinante. È importantissimo avere persone formate e che mantengono comportamenti consapevoli*». Daolio, dal canto suo, allarga il campo. L'espansione informatica è arrivata a tal punto che, pur con i dovuti accorgimenti, possiamo definire alcune tecnologie quasi delle commodities. Dunque, in un'era iper-digitale, paradossalmente ciò che fa la differenza resta la condotta degli operatori.

Certamente questi utenti hanno bisogno di un ampliamento delle proprie competenze, insieme a un mutamento negli approcci e nei valori. Tra questi valori, una posizione speciale occupa l'empatia, ritenuta una soft skill, uno di quegli attributi che fanno parte degli "accessori" del lavoratore, subordinati alle competenze tecniche. Saper fare il proprio mestiere resta fondamentale, ma secondo Daolio, più elevato è il grado raggiunto in azienda, maggiore è il peso delle qualità umane. Un Cfo può essere percepito all'esterno come una figura grigia e apatica, allora l'empatia può entrare in gioco e aiutare a sbloccare i rapporti con i colleghi, a creare fiducia nel team di lavoro, a comprendere le posizioni di tutti.

Cfo e direttore della sicurezza collaborano strettamente quando in azienda si fa la valutazione del rischio, un momento fondamentale per il direttore, perché dopo aver ricevuto tutti i dati con le priorità sulle aree di intervento, deve avviare una larga comunicazione interdisciplinare. Tutti i settori aziendali sono toccati dalla sicurezza e il direttore deve trovare il modo di comunicare con tutti, far capire le proprie esigenze, ricevere feedback, a metà tra la figura del tecnico e quella del mediatore empatico.



Tuttavia l'empatia, nella sfera della cybersecurity, non è solamente una skill utile ai lavoratori, ma potenzialmente, anche ai criminali. Infatti, ancora oggi il phishing e i suoi derivati sono causa della maggioranza degli attacchi informatici e non solo: anche gli attacchi informatici più tecnici possono comunque partire da credenziali rubate tramite lo stesso meccanismo. Oggi molti crimini informatici sono perpetrabili anche da una sfera di persone che non possiede competenze tecniche elevate, aiutate da IA e piattaforme automatizzate che consentono di comprare online template di email-truffa o interfacce fake di banche o aziende. Se il criminale è in grado di sfruttare la debolezza cognitiva o emotiva della persona, il direttore della sicurezza deve essere altrettanto in grado di prevedere e proteggere quelle vulnerabilità, cercando di guidare gli utenti a comportamenti più responsabili.

Manfredini ha dunque lanciato un programma molto serrato di formazione e addestramento interno ad A2A. Il fulcro operativo sono campagne di phishing settimanali a tutti i dipendenti: la popolazione aziendale è segmentata in gruppi in base alle competenze dimostrate nell'anno precedente e le campagne successive vengono targettizzate di conseguenza. A

questo tipo di formazione si affianca l'insegnamento "classico": corsi in aula e pillole digitali, video e registrazioni. Per aumentare la fiducia e la capacità di ascolto, alcuni contenuti sono realizzati da colleghi non appartenenti alla security che si sono distinti in positivo: volti familiari e credibili che aumentano l'efficacia del messaggio.

Dietro queste pratiche di addestramento c'è un'idea semplice, ma non scontata: la sicurezza nasce dal confronto. Nessun team può essere impermeabile, e spesso la soluzione arriva da chi guarda le cose da un'altra angolazione. *«Al 99%, la soluzione a uno dei problemi aziendali è già stata trovata all'esterno in casi simili e può essere facilmente riapplicata, senza doversi inventare la ruota»*, osserva Manfredini. Oggi più che mai è fondamentale alzare la testa per non perdere il contatto con la realtà, che sia all'interno di diversi dipartimenti della stessa azienda, o dalla struttura verso l'esterno.

«Jack Welch diceva che se lui fosse ancora l'amministratore delegato di un'azienda, il primo indice che guarderebbe tutte le mattine entrando in ufficio sarebbe l'indice di trasformazione», ricorda Daolio. La trasformazione di un'impresa non è un compito che può essere affidato a una sola persona, ma richiede sguardi molteplici: un amministratore delegato oggi potrebbe affidarsi a presidi organizzativi interni per mantenere la rotta e destinare sempre più tempo a osservare il mondo fuori, per non limitarsi a inseguire l'oggi, ma studiare e anticipare ciò che accadrà domani.

Come nei processi di trasformazione aziendale, anche nella cybersecurity l'uomo resta al centro del processo. Lo "spettro umano" è proprio questo: la componente imprevedibile che può generare vulnerabilità o difesa, errore o intuizione. È sufficiente una semplice distrazione per produrre danni incalcolabili, così come un gesto consapevole può generare miglioramenti. Accettare questo aspetto significa riconoscere che la sicurezza digitale non si costruisce nonostante le persone, ma investendo su di esse.