Il canto della segretaria

Il crimine informatico si nutre delle distrazioni emotive dei collaboratori aziendali. Stress, impreparazione e sollecitazioni esterne dai social aumentano i casi di phishing.

Martina lavora come segretaria presso un rinomato studio medico del Canton Ticino. Per lei è tempo di vacanze estive, dopo la lunga maratona professionale primaverile. Gli ultimi giorni di lavoro sono parecchio impegnativi, oltre ad aver accolto nuove richieste di visite mediche, ha dovuto fare ordine nel database centrale dei dati per assicurarsi che non vi fossero fatture scoperte o dimenticate prima delle meritate vacanze. Naturalmente le cose non arrivano mai sole. Come se non bastasse, nella sua casella di posta elettronica continuano a giungere messaggi che segnalano un imminente aggiornamento del software, che proprio Martina utilizza in ufficio per la gestione dei pazienti. Ma presa da mille faccende, non pone particolare attenzione ai dettagli dei loro contenuti, consapevole che in genere le questioni tecniche sono di competenza degli informatici specializzati, che il titolare dello studio incarica per gestire l'intera infrastruttura informatica e la relativa sicurezza delle informazioni.

I giorni scorrono veloci e sempre con maggiore intensità, anche perché l'imminente fine dell'estate significa per Martina concedersi le tanto sognate ferie. È ormai una tradizione per lei e la sua famiglia trasferirsi per tre settimane nella vicina Sardegna, un posto idilliaco molto apprezzato sia dal marito che dai figli in piena adolescenza. Per lei le vacanze in famiglia sono sacre, per questo con l'avvicinarsi della partenza esprime molto entusiasmo ma anche forte stress, perché al lavoro non trascura nulla, è molto meticolosa nella gestione di tutti i potenziali dettagli che potrebbero comprometterle. Lavora per quello studio medico da molti anni, e in passato è sempre filato tutto liscio, mai nessun imprevisto che non avesse messo a preventivo. Quest'anno però, a rendere la situazione particolare, sono i continui messaggi e-mail che riceve più volte durante il giorno, per segnalare con sempre maggiore enfasi che in breve tempo sarebbe stata contattata dell'azienda che ha sviluppato il software che lo studio usa per la gestione della contabilità e dei suoi clienti. È programmato così bene che Martina non potrebbe più farne a meno. Ma qualcosa non torna, i messaggi aumentano con il passare del tempo, soprattutto con il sopraggiungere della chiusura dello studio, una strana coincidenza. Non era mai accaduto prima. Martina non ne ha parlato con il titolare, il timore che potesse saltar fuori qualche problema dell'ultimo minuto la preoccupava, e il solo pensiero che le sue vacanze fossero a rischio la rendeva nervosa. Una condotta sicuramente inopportuna e poco professionale, ma molto frequente in molte realtà aziendali dove stress, pressione, stanchezza e voglia di andare in ferie alimentano uno strato pericoloso di superficialità operativa, inutile negarlo. Mancano solo ventiquattro ore alla fine della settimana e alla chiusura dell'ufficio, e Martina si accorge che i fatidici messaggi hanno cessato improvvisamente di bussare alla sua casella di posta elettronica. Per lei è un sollievo e un forse segnale rassicurante. Così nella sua mente trova spazio l'idea che i tecnici informatici abbiano finalmente preso a carico il problema dell'aggiornamento del software. Tutto falso. Il silenzio era voluto e magistralmente generato per l'occasione, affinché abbassasse la guardia emotiva e credesse che tutto fosse risolto. Come volevasi dimostrare, la telefonata arrivò puntuale a pochissimi minuti dalla chiusura dell'ufficio, proprio quando la segretaria era convinta di aver concluso tutte le pratiche ancora in sospeso. Il telefono squillò con la certezza che qualcuno avrebbe presto risposto con la fretta di sbrigare velocemente la questione.

Un fattore temporale ed emotivo voluto e atteso, che trovò in Martina un'interlocutrice pronta a tutto pur di arrivare a chiudere l'ufficio nel minor tempo possibile. Chi compose il numero era a conoscenza di tutte queste informazioni e del suo stato d'animo, perché Martina senza troppe precauzioni e con molto entusiasmo lo aveva scritto ripetutamente nel suo profilo Facebook. Anzi, senza rendersene conto, i suoi post in Facebook erano il miglior feedback che i malintenzionati potessero ottenere quando la sua casella di posta veniva presa di mira. Per lei era un semplice sfogo, ma per gli altri una conferma ad alto valore aggiunto che la trappola stesse andando proprio nella direzione desiderata. Inoltre, con superficialità, con il suo smartphone personale aveva pubblicato in Instagram selfie, video e storie della vacanza che da lì a poco avrebbe fatto in Sardegna con la famiglia, tutte informazioni personali preziose che avevano permesso a estranei di cogliere i suoi ritmi professionali, le sue pause e i suoi pensieri. Lei non lo sapeva, ma questa miriade di informazioni personali erano come oro colato per coloro in procinto di attuare una delle più semplici ed efficaci tecniche di ingegneria sociale. Non immaginava che in pochi minuti le sue vacanze sarebbero saltate e il suo posto di lavoro avrebbe accusato un grosso colpo.

Durante la breve telefonata, il finto tecnico con tono deciso e persuasivo, si presentò ricordando a Martina l'importanza di eseguire con urgenza l'aggiornamento del programma informatico ancora in sospeso, quello per cui riceveva continui messaggi e-mail. In pratica, con una raffica di termini tecnici ben allineati, spiegò alla segretaria che l'aggiornamento software doveva essere fatto all'istante, onde evitare la perdita irreversibile di tutti i dati presenti nel database centrale, backup compreso. Una potenziale catastrofe. Martina era comprensibilmente spaventata, e invitò l'imbroglione a prendere contatto con i tecnici informatici per effettuare l'operazione di aggiornamento, ma il suo interlocutore, con molta abilità, la convinse di aver già parlato con loro e di essersi messo d'accordo per eseguire l'aggiornamento direttamente con lei, in quanto il computer principale da cui operare era proprio il suo. Di fronte a questa rassicurazione, Martina cedette senza troppi problemi. Boom, il dado era tratto. Senza il benché minimo scrupolo le venne chiesta la sua password personale di accesso al database centrale, affinché si potesse procedere con l'aggiornamento del software. Naturalmente Martina era già con la mente in vacanza, quindi tutto ciò che avrebbe detto il falso tecnico al telefono lo prendeva per buono, anzi, buonissimo, a patto che facesse i fretta. Il danno era ormai fatto e in pochi secondi tutti i dati sensibili registrati dello studio medico erano stati rubati, con grande maestria e perseveranza.

> «Il fattore umano continua a essere l'elemento debole di una filiera tecnologica sempre più complessa e distribuita, che sommato alle innumerevoli distrazioni a cui sono sottoposte le persone durante il giorno, rende il crimine informatico organizzato una vera e propria macchina da soldi»

Scenari come quello appena descritto non sono il frutto di una qualsivoglia fantasia, ma una realtà ben radicata anche il Cantone Ticino. Infatti, Security Lab di Lugano, azienda leader nel campo della cybersecurity, questo lo sa bene, perché sempre più spesso viene sollecitata da aziende locali, nazionali e internazionali per svolgere corsi di sensibilizzazione alle tecniche di ingegneria sociale, atti proprio alla formazione dei collaboratori su ciò che potrebbe capitare loro durante il lavoro nei periodi di maggiore stress.

E in seguito, cosa ancor più importante, giocando il ruolo dell'attaccante verifica concretamente il grado di preparazione acquisita del personale, attraverso la simulazione reale di attacchi di ingegneria sociale diversificati. Un'alfabetizzazione importante, continua, interdisciplinare e complementare a quella tradizionale di cybersecurity, dovuta e necessaria, ma non più sufficiente. Il fattore umano continua a essere l'elemento debole di una filiera tecnologica sempre più complessa e distribuita, che sommato alle innumerevoli distrazioni a cui sono sottoposte le persone durante il giorno, rende il crimine informatico organizzato una vera e propria macchina da soldi.

Alessandro Trivilini

Informazioni di contatto
Security Lab
Alberto Redi
+41 91 922 59 41
www.sec-lab.com

Inchieste nel Deep Web

Un corso rivolto ai professionisti del settore dei media, interessati a conoscere nuovi strumenti di lavoro per le inchieste giornalistiche nel Deep Web. Censura e controllo, oltre le fakenews, invadono il mondo della comunicazione e dei media. Un cambiamento dirompente con forte impatto sulla società, sui cittadini, sulle imprese, ma anche sui media, sempre più interessati a cercare informazioni 'hot' in luoghi nascosti come il Deep Web. Il corso consente la creazione, l'apprendimento e l'utilizzo di un ambiente di lavoro personale, personalizzato, sicuro e protetto, da usare per le inchieste giornalistiche, attraverso una semplice memoria Usb.
Informazioni e iscrizioni: https://www.ated.ch