Come tutelarsi da una delle truffe più dannose: CybergON indica i segnali da valutare

Cyber-frode del ceo, è allerta

In tempi di smartworking aumentano i rischi di attacchi

Pagina a cura
DI ROXY TOMASICCHIO

Il ricorso a smartworking e telelavoro impone di alzare la guardia verso i possibili attacchi informatici. In particolare quelli che sfruttano false e-mail. In tal caso cosa fare? Gli imprenditori devono ribaltare il punto di vista e il rapporto di fiducia e devono pensare che ogni comunicazione o richiesta di dati sia anomala. Così **Marco Lucchina**, cybersecurity manager di CybergON Security, business unit di Elmec Informatica, spiega a *ItaliaOggi Sette* come evitare la cosiddetta «frode del ceo». Prende il nome dal chief executive officer, cioè l'amministratore delegato di una società, in quanto appunto il cybercriminale si finge il ceo, o un'altra figura manageriale, di un'azienda e si inserisce in conversazioni via e-mail già esistenti o inizia trattative con utenti che abitualmente hanno una corrispondenza con la persona a cui ha rubato l'identità virtuale o si occupano di contabilità aziendale. Tecnicamente, infatti, questi attacchi ricadono sotto la tipologia delle frodi Bec, business email compromise, che prevedono la compromissione di account aziendali. «È uno degli attacchi più sofisticati, servono competenze tecniche e di ingegneria sociale, è predisposto solo dopo una lunga e approfondita preparazione da parte del cybercriminale che deve far propri contenuti e modalità di comunicazione di chi andrà a fingersi, per questo molto spesso è molto difficile riconoscerli. L'obiettivo sono i soldi, mi permetto di aggiungere come sempre. In questo modo si arriva direttamente all'obiettivo, quando rubano le informazioni arrivano all'obiettivo solo dopo averle rivendute», dice ancora Lucchina. Secondo un'analisi di Symantec, l'Italia, con circa 400 aziende colpite al giorno, è al secondo posto dopo gli Stati Uniti per numero di attacchi di questo tipo. Ma lo scenario potrebbe anche essere più grave, visto che la maggior parte delle vittime preferisce non dichiarare l'attacco. Infatti, aggiunge Lucchina, «ci sono i dati della polizia postale, che però si riferiscono a qualcosa di più esteso, ossia le truffe che portano a fare bonifici extra-Ue: sono stati quantificati in denunce per 35 milioni di euro per il 2018. Secondo noi è solo la punta dell'iceberg, dato che pochi denunciano».

In questo periodo, in cui, per l'emergenza sanitaria causata dalla diffusione del Coronavirus, le aziende stanno incentivando il lavoro da remoto dei propri dipendenti, limitando quanto più possibile i contatti personali, aumentano le possibilità di essere colpiti da attacchi di questo tipo. Soprattutto a essere nel mirino dei cybercriminali sono le aziende che fanno affidamento solo sulle e-mail per i processi interni. «Se i bonifici fossero fattibili solo da Erp (*Enterprise resource planning, ovvero software gestionali, nda*) e con l'autorizzazione esplicita di più persone la riuscita sarebbe più complessa. Come altre truffe, colpiscono persone non consapevoli del rischio o superficiali rispetto ai processi interni», riferisce il cyber security manager di CybergON, nuova business unit dedicata alla sicurezza informatica di Elmec, società che a sua volta offre servizi e soluzioni It. «Le conseguenze di questi attacchi possono essere estremamente critiche. Oltre alla perdita di denaro, infatti, entra in gioco il tema reputazionale della società e naturalmente dei dirigenti che vengono coinvolti».

Per evitare di cadere in questa frode un buon punto di partenza è la consapevolezza che queste dinamiche esistono e che ognuno di noi può diventarne vittima. A questo scopo è fondamentale la formazione: «noi mettiamo a disposizione due moduli gratuiti che mostrano le tipologie di attacco e alcuni esempi», dice Lucchina. «Dobbiamo fare in modo che le persone invertano la relazione di fiducia soprattutto se stanno lavorando da casa: devono pensare che ogni comunicazione sia potenzialmente malevola e chiedersi se rientra nella classificazione di anomalia: "mi sarei aspettato questo o è strano"? Se nessuno ti ha mai chiamato per chiederti la password, non lo farà neanche ora».

Per dare indicazioni concrete alle imprese, inoltre, CybergON ha individuato i campanelli d'allarme utili per riconoscere un attacco di questo tipo prima che sia troppo tardi (*si veda la tabella in pagina*). Ovviamente la richiesta di denaro deve insospettire, soprattutto se si chiede di far riferimento a un conto corrente diverso da quello normalmente utilizzato. In genere i cybercriminali preferiscono che le conversazioni avvengano solo via e-mail, motivando la sua richiesta con ragioni di urgenza e confidenzialità. In sintesi è bene prestare attenzione a qualsiasi episodio che non rientra nel normale funzionamento delle cose. «Dopo aver riconosciuto uno dei campanelli d'allarme», conclude Lucchina, «occorre segnalare al proprio supporto tecnico la cosa e verificare sempre il mittente con un canale di comunicazione differente». Mentre a livello preventivo si può agire su due fronti: formare gli utenti e configurare i sistemi di posta con capacità crittografiche e reputazionali. Le buone abitudini legate alle truffe online sono sempre valide per evitare brecce negli account di posta: password efficaci e autenticazioni multi-fattore mitigano il rischio», prosegue, «avere un processo interno di gestione e controllo delle e-mail fornisce inoltre un ulteriore livello di protezione da eventuali tentativi di attacco Man in The Middle (*tradotto uomo nel mezzo, l'attaccante si inserisce in una comunicazione tra due utenti con lo scopo di spiare, registrare e rubare informazioni, nda*) o frode del Ceo. Procedure anti-frode, l'analisi delle mail, dei domini e di altri indizi sono alcune modalità di intervento che la specialità di Cyber Intelligence può farsi carico per garantire una strategia di difesa efficace. Ciò che individualmente possiamo fare è rimanere vigili, fare controlli incrociati su richieste inconsuete chiamando il diretto interessato, verificare sempre l'indirizzo del mittente e agire solo ed esclusivamente quando si è sicuri della legittimità della richiesta e della fonte».

I campanelli d'allarme

1. Richieste di denaro su un nuovo conto corrente

Tipicamente le richieste che giungono dal «falso ceo» sono di versare denaro, spesso in modo rateale, su un conto corrente diverso da quello normalmente utilizzato

2. Una comunicazione esclusivamente via e-mail

Il cybercriminale chiede di proseguire la conversazione esclusivamente via mail motivando la sua richiesta con ragioni di urgenza e confidenzialità, che possono suonare anche molto credibili e familiari

3. Destinatari a contatto con la contabilità aziendale

Le vittime prescelte sono spesso dipendenti che ricoprono ruoli con la possibilità di intervenire nella contabilità di un'azienda e abituati quindi a gestire trasferimenti di denaro

4. Attenzione a qualunque anomalia

Una anomalia è qualcosa che non rientra nel normale funzionamento delle cose. Se, per esempio, un a.d. chiede ai propri collaboratori di compilare un form, senza averlo mai fatto prima, è buona norma sospettare del link che ha allegato e chiedere conferma attraverso un altro canale di comunicazione

La finanza è tra i settori più esposti. Il phishing accelera

Il cybercrime finanziario è in aumento, in un contesto generale di crescita esponenziale di attacchi (1.670 gravi, lo scorso anno, a livello mondiale): le statistiche del 2019 fanno registrare 6.854 casi a livello nazionale, come segnalato dalla Polizia postale e delle comunicazioni nel rapporto Clusit sulla sicurezza Ict in Italia, giunto alla quindicesima edizione (considerando gli aggiornamenti semestrali), presentato in diretta streaming lo scorso 17 marzo (si veda l'anticipazione su *ItaliaOggi Sette* del 9/3/2020).

I dati descrivono uno scenario in cui il fenomeno del phishing (le truffe via e-mail, con lo scopo di rubare codici personali e dati sensibili) è in notevole aumento. Così come in aumento sono anche i casi riguardanti il cosiddetto «Vishing» (phishing vocale) e «Smishing» (phishing attraverso messaggi ed sms).

Anche dal rapporto Clusit, Associazione italiana per la sicurezza informatica, emerge che il tessuto economico-produttivo italiano continua a essere oggetto degli attacchi noti a livello mondiale con le espressioni Bec e Ceo Fraud (Business e-mail compromise e froe del ceo, *si veda l'articolo principale*). Obiettivo delle organizzazioni criminali è intromettersi nei rapporti commerciali tra aziende dirottando ingenti somme verso propri conti correnti. Malgrado la difficoltà operativa di bloccare e recuperare le somme provento di frode informatica, soprattutto perché inviate verso paesi extraeuropei (Cina, Taiwan, Hong Kong), la Polizia postale spiega come, nel 2019, grazie alla versatilità della piattaforma OF2CEN (On line Fraud Cyber Centre and Expert Network) sono stati bloccati e recuperati 18 milioni di euro. La piattaforma in questione, frutto di convenzioni con l'Abi con gran parte del mondo bancario, consente di intervenire in tempo quasi reale sulla segnalazione, bloccando la somma prima che venga polverizzata in vari prestanome.

Tornando al rapporto, che analizza su base semestrale i più gravi cyberattacchi noti avvenuti nel mondo, le tecniche di phishing e social engineering segnano un +81,9% rispetto al 2018, arrivando a rappresentare il 17% del totale. Una quota crescente di questi attacchi basati su phishing si riferisce, confermano gli esperti Clusit, a Bec scams. In merito alle altre tecniche di attacco, i cybercriminali nel 2019 hanno utilizzato malware nel 44% dei casi (+24,8%). Al secondo posto, a rappresentare il 19% del totale, ci sono varie tecniche sconosciute, ma in decrescita (-22,3%).