CEO Fraud

La cosiddetta «truffa del CEO» è uno stratagemma subdolo. I collaboratori di un'azienda autorizzati a effettuare pagamenti direttamente ricevono via e-mail da un loro superiore l'ordine di avviare immediatamente un pagamento a un indirizzo specifico. In realtà, però, il mittente è falsificato – è tutto opera di un truffatore.

Punti principali per i collaboratori:

- Se venite contattati in circostanze inconsuete o sospette, non divulgate nessun tipo di informazioni e non seguite nessuna istruzione, nemmeno se vi viene fatta pressione.
- Prima di eseguirle, chiedete conferma di tali richieste di pagamento al superiore contattandolo attraverso un canale differente (di persona o al telefono).
- Prestate attenzione a eventuali elementi di sicurezza mancanti o errati, come le firme delle e-mail (https://www.ebas.ch/it/firma-email-outlook/) .

Punti principali per le aziende:

- Sensibilizzate i vostri collaboratori su questo tipo di truffa.
- Controllate quali informazioni sulla vostra impresa sono disponibili online e, ove possibile e utile, ridimensionatele.
- Definite e applicate una procedura di autorizzazione dei pagamenti mediante controllo incrociato con firma collettiva.
- Segnalate immediatamente alla polizia tali tentativi di truffa.
- Verificate l'utilizzo di elementi di sicurezza avanzati come le firme delle e-mail nei processi aziendali critici (procedura di pagamento).

Condotta sicura dei collaboratori

Se un superiore vi chiede via e-mail di effettuare un pagamento immediato senza averlo prima annunciato o senza che voi ne foste già a conoscenza, occorre prestare particolare attenzione. In questi casi fuori della norma raccomandiamo di verificare più a fondo la legittimità dell'ordine, p. es. controllando la presenza di eventuali elementi di sicurezza come le firme dell'e-mail (firma digitale). **In ogni caso, dovreste contattare direttamente il vostro superiore (di persona o almeno al telefono) e accertare se il pagamento va veramente effettuato.**

Come azienda, adottate misure precauzionali

Sensibilizzazione del personale

La ricezione di questo tipo di e-mail fraudolente può essere in qualche modo limitata con provvedimenti tecnici, ma è impossibile prevenirla del tutto. I truffatori cambiano continuamente indirizzo mascherando così la loro identità e la loro provenienza. Inoltre, a volte riescono persino a impadronirsi del vero account e-mail del superiore e a sfruttarlo per i loro scopi.

La principale forma di prevenzione consiste quindi nel sensibilizzare il personale degli uffici più interessati da

questo genere di truffa, come la contabilità finanziaria.

Informazioni online

Per sferrare una «truffa CEO», l'hacker ha bisogno innanzitutto di informazioni congrue sull'azienda e i suoi collaboratori. Spesso, il sito Internet della società o il registro di commercio contengono già informazioni sufficienti. Inoltre, i siti di social networking (come LinkedIn (https://www.ebas.ch/it/impostazioni-di-linkedin/) o Xing) sono particolarmente interessanti per i truffatori, perché contengono informazioni sulle relazioni commerciali o sull'identità e la funzione dei collaboratori. Controllate quindi quali informazioni sulla vostra impresa e i vostri collaboratori sono pubblicamente accessibili online e, per quanto possibile, ridimensionatele.

Procedura di autorizzazione dei pagamenti

La truffa vera e propria si concretizza con il trasferimento della somma richiesta. Di norma, la destinazione è un conto bancario estero, dal quale il denaro viene poi rapidamente spostato su altri conti. Per evitare tali pagamenti erronei è consigliabile stabilire una rigorosa procedura di autorizzazione dei pagamenti con punti di controllo – preferibilmente adottando il principio del controllo incrociato con firma collettiva. Ciò aumenta in misura significativa la probabilità che almeno una delle due persone che autorizzano la transazione si accorga che è una truffa e blocchi l'operazione.

Utilizzo di firme nelle e-mail

La «CEO Fraud» manipola il processo di pagamento falsificando il legittimo mittente dell'ordine (c.d. e-mail spoofing).

La variante più semplice consiste nella falsificazione dell'indirizzo del mittente. Una firma dell'e-mail (firma digitale), che può essere apposta correttamente solo dal mittente reale, rappresenta una buona soluzione. Tuttavia, si tratta di una procedura relativamente complicata da implementare ed è indispensabile anche che la firma venga controllata dal destinatario.

Più grave è l'uso illecito dell'account e-mail reale (compromesso) del mittente, p. es. a seguito di un preliminare attacco di phishing riuscito. In questo caso, anche la firma dell'e-mail può essere utilizzata in modo improprio. L'unica soluzione consiste allora in una rigorosa procedura di autorizzazione dei pagamenti e nella sensibilizzazione di tutte le persone coinvolte.

Nello schema di truffa «CEO Fraud» (noto anche come «truffa del CEO» o «truffa del capo»), i malintenzionati si spacciano per il CEO (il capo) di un'azienda e impartiscono ai collaboratori autorizzati a effettuare pagamenti l'ordine di eseguire immediatamente il versamento di una somma consistente.

«CEO» è l'abbreviazione di Chief Executive Officer e significa generalmente «amministratore delegato»; «fraud» è la traduzione in inglese di «truffa».