CEO Fraud

Beim sogenannten «CEO Fraud» handelt es sich um eine perfide Betrugsmasche. Hierbei werden Mitarbeitende eines Unternehmens mit direkter Zahlungsermächtigung, per E-Mail von einer vorgesetzten Person angewiesen, eine Zahlung an eine bestimmte Adresse sofort auszulösen. In Wahrheit ist der Absender jedoch vorgetäuscht – dahinter verbirgt sich ein Betrüger.

Wichtigste Merkpunkte für Mitarbeitende:

- Geben Sie bei ungewöhnlichen oder zweifelhaften Kontaktaufnahmen keine Information preis und befolgen Sie keine Anweisungen, auch wenn Sie unter Druck gesetzt werden.
- Lassen Sie sich solche Zahlungsaufforderungen vor der Ausführung von der vorgesetzten Person über einen anderen Kanal direkt bestätigen (persönlich oder per Telefon).
- Achten Sie auf allenfalls fehlende oder nicht korrekte Sicherheitselemente wie E-Mail-Signaturen (https://www.ebas.ch/e-mail-signatur-outlook/) .

Wichtigste Merkpunkte für Unternehmen:

- Sensibilisieren Sie Ihre Mitarbeitenden bezüglich dieser Betrugsart.
- Kontrollieren Sie, welche Informationen über Ihr Unternehmen online zugänglich sind und schränken Sie diese wo möglich und sinnvoll ein.
- Definieren und implementieren Sie einen Zahlungsfreigabeprozess mittels Vieraugenprinzip mit Kollektivunterschrift.
- Melden Sie solche Betrugsversuche umgehend der Polizei.
- Prüfen Sie die Verwendung von erweiterten Sicherheitselementen wie E-Mail-Signaturen in kritischen Geschäftsprozessen (Zahlungsprozess).

Sicheres Verhalten der Mitarbeitenden

Wenn eine vorgesetzte Person Sie per E-Mail zur Auslösung einer sofortigen Zahlung auffordert, die nicht angekündigt beziehungsweise vorher nicht bekannt war, ist erhöhte Vorsicht angebracht. In solchen ungewöhnlichen Fällen ist es ratsam, die Legitimität des Auftrags genauer abzuklären, z. B. indem Sie allfällig vorhandene Sicherheitselemente wie E-Mail-Signaturen (digitale Unterschrift) prüfen. **In jedem Fall sollten Sie die vorgesetzte Person direkt (persönlich oder zumindest per Telefon) kontaktieren und abklären, ob die Zahlung tatsächlich ausgeführt werden soll.**

Treffen Sie als Unternehmen Vorkehrungen

Mitarbeitenden-Sensibilisierung

Der Versand solcher betrügerischen E-Mails lässt sich mit technischen Massnahmen etwas eindämmen, jedoch nie ganz verhindern. Die Betrüger wechseln ständig ihre Adresse und verschleiern damit ihre Identität und Herkunft. Zudem gelingt es ihnen mitunter auch, das echte E-Mail-Konto der vorgesetzten Person für ihre Zwecke zu missbrauchen.

Die wichtigste Massnahme zur Vorbeugung ist deshalb die Sensibilisierung der Mitarbeitenden in den von diesem Betrug am stärksten betroffenen Abteilungen, wie z.B. der Finanzbuchhaltung.

Online-Informationen
Zum Starten eines «CEO Frauds» benötigt der Angreifer als Erstes entsprechende Auskünfte über die Firma und deren Mitarbeitenden. Oft geben die Firmenwebsite oder das Handelsregister bereits genügend Informationen preis. Ausserdem sind soziale Netzwerke (wie z.B. LinkedIn (https://www.ebas.ch/linkedin-einstellungen/) oder Xing) für Betrüger interessant, weil dort Informationen über geschäftliche Beziehungen oder die Identität und Funktion von Mitarbeitenden zu finden sind. Kontrollieren Sie deshalb, welche Informationen über Ihre Firma und Ihre Mitarbeitenden online zugänglich sind und schränken Sie diese soweit möglich ein.

Zahlungsfreigabeprozess
Der eigentliche Betrug passiert durch die Überweisung der Zahlung. In der Regel erfolgt diese auf ein ausländisches Bankkonto, von welchem das Geld dann schnell auf andere Konten weitergeleitet wird. Um solche fälschlichen Zahlungen zu verhindern, empfiehlt es sich, einen strikten Zahlungsfreigabeprozess mit Kontrollpunkten zu etablieren – am besten mittels des Vieraugenprinzips mit Kollektivunterschrift. So ist die Chance wesentlich grösser, dass mindestens eine der beiden freigebenden Personen den Betrug erkennt und dadurch verhindern kann.

Verwendung von E-Mail-Signaturen
Der «CEO Fraud» manipuliert den Zahlungprozess, indem er den legitimen Absender des Zahlungsauftrags vortäuscht (sogenanntes E-Mail-Spoofing).

Die einfachste Variante davon ist das Fälschen der E-Mail-Absenderadresse. Davor bietet eine E-Mail-Signatur (digitale Unterschrift), welche nur vom echten Absender korrekt angebracht werden kann, einen guten Schutz. Allerdings ist dieses Verfahren relativ aufwändig zu implementieren und bedingt zudem, dass die Signatur beim Empfänger entsprechend überprüft wird.

Gravierender ist der Missbrauch des echten (gehackten) E-Mail-Kontos des Absenders, z.B. infolge eines vorgängig erfolgreich durchgeführten Phishing-Angriffs. Hierbei kann sogar die E-Mail-Signatur missbraucht werden. In diesem Fall helfen ein strikter Zahlungsfreigabeprozess und die Sensibilisierung aller involvierten Personen.

Bei der Betrugsmasche «CEO Fraud» (auch CEO Betrug oder Chef Betrug genannt) geben sich Angreifer als CEO (Chef) eines Unternehmens aus und weisen Mitarbeitende mit Zahlungsermächtigung an, kurzfristig die Überweisung einer grösseren Geldsumme auszulösen.

«CEO» steht für Chief Executive Officer und bedeutet sinngemäss Geschäftsführer, «Fraud» ist das englische Wort für Betrug.