Leitblatt

CEO-Fraud

Bundesverband

Eine absolut authentische E-Mail erreicht den Mitarbeiter aus der Geschäftsführung. Der große Deal in China, von dem seit einiger Zeit in der Firma gesprochen wird, steht bevor. Dazu müssen 750 000 $ schnell auf eine Bank in Shanghai überwiesen werden. Hierüber sei jedoch Stillschweigen zu bewahren. Der Mitarbeiter weiß, der Absender der E-Mail befindet sich in China und ist schwer erreichbar. Die Summe wird angewiesen – und ist verloren.

Der wahre Absender ist ein Krimineller, der sich im Vorfeld gut über das Unternehmen informiert hat. Ein solcher, so genannter CEO-Fraud ist nur schwer zu erkennen, aber einfach zu bekämpfen – durch Nachfragen!

Charakteristika von CEO-Fraud

- Absender oftmals aus den Reihen von Vorstand / Geschäftsführung
- Absender kann unbekannt sein oder auch bekannt
- Bestehende Geldflüsse sollen umgeleitet werden
- Neue Gelder sollen auf ein bis dato unbekanntes Konto fließen
- Beträge müssen nicht hoch sein
- Verschwiegenheit wird gefordert
- Häufig Drang zu großer Eile

Ein einfaches Gegenmittel: Identitätscheck!

- Schauen Sie sich die E-Mail-Adresse genau an! Oftmals lässt sich anhand der E-Mail-Adresse erkennen, dass es sich bei dem Absender zwar augenscheinlich um eine hohe Führungskraft des Unternehmens handelt, bei genauerem Hinsehen ist jedoch die „Fake-Adresse“ feststellbar.
- Vergewissern Sie sich der Identität des Absenders: Suchen Sie nach den Kontaktdaten im Intranet und rufen Sie über diese bekannten Kontaktdaten zurück!
- Lassen Sie sich nicht unter Druck setzen, binden Sie in Verdachtsfällen Ihren Vorgesetzten und die in Ihrem Unternehmen zuständigen Ansprechpartner für Sicherheit ein!
- Informieren Sie sich bei den zuständigen Sicherheitsbehörden. Dort sind in der Regel entsprechende weitere Warnhinweise vorhanden.
- Teilen Sie diese Warnhinweise in Ihrem Unternehmen, z. B. über das firmeninterne Intranet
- Sensibilisieren Sie gezielt die Bereiche im Unternehmen, die solche Zahlungen veranlassen können (z. B. Finanzbereich, CFO)

Beispiele

Fall 1

Es erreicht Sie ein Anruf oder eine E-Mail von jemandem, den Sie nicht kennen, vermeintlich aus der Geschäftsführung oder dem Vorstand, und weist Sie an, Gelder zu überweisen oder Informationen zu teilen.

Empfehlung

Rufen Sie zurück! Suchen Sie die Kontaktdaten der entsprechenden Person aus dem Intranet (nicht aus der E-Mail-Signatur!) und vergewissern Sie sich in einem Anruf, dass die Anweisung tatsächlich von dieser Person stammt. Nehmen Sie im Zweifel Kontakt zu der Person aus Geschäftsführung/Vorstand auf, die für gewöhnlich Zahlungsanweisungen gibt.

Fall 2

Jemand aus der Geschäftsleitung, der Ihnen persönlich bekannt ist, fordert in einer E-Mail eine dringende Überweisung auf ein bestimmtes Konto an oder bittet um eine Änderung eines Überweisungsziels.

Empfehlung

Fragen Sie telefonisch nach! Vergewissern Sie sich, dass die E-Mail auch tatsächlich von der angegebenen Person stammt.

Fall 3

In der Aufforderung zur Geldüberweisung wird um Stillschweigen gebeten, ein telefonisches Nachfragen sei nur schwer möglich, wenn dann unter einer anderen Telefonnummer.

Empfehlung

Rufen Sie dennoch an – unter der Ihnen bekannten Telefonnummer! Sollten Sie die Ihnen bekannte Person nicht erreichen, informieren Sie Ihren Vorgesetzten oder jemand anderen in der Geschäftsleitung.

Fall 4

Eine neue Geldüberweisung soll sehr kurzfristig durchgeführt werden, so dass Rückfragen praktisch unmöglich sind.

Empfehlung

Gerade dann fragen Sie nach! Vergewissern Sie sich, dass die Überweisung wirklich so wie angegeben stattfinden soll.

ASW Bundesverband

Herausgeber: ASW Bundesverband – Allianz für Sicherheit in der Wirtschaft e. V. | **Stand:** März 2016 | **Kontakt:** info@asw-bundesverband.de