CEO-Betrug

written by Christian Hafner | 23 Januar, 2023

Riskmanagement & IKS News

CEO-Betrug

Eine immer noch relativ neue Betrugsmasche mit der Unternehmen um Millionen von Franken geprellt werden (können).

Beim CEO-Betrug geben sich Täter beispielweise als Geschäftsführer (CEO) das Unternehmens aus und veranlassen einen Mitarbeiter zum Transfer eines grossen Geldbetrags ins Ausland.

Die Täter nutzen hierfür Informationen, die Unternehmen in Wirtschaftsberichten, im Handelsregister, auf ihrer Homepage oder in Werbebroschuren veröffentlichen. Die Täter legen ihr Augenmerk insbesondere auf Angaben zu Geschäftspartnern und künftigen Investments.

Das Nationale Zentrum für Cybersicherheit (NCSC) beschreibt ein typisches Vorgehen wie folgt:

«Die Betrüger reservieren eine Domäne mit einem ähnlichen Namen (z.B. Namen einer Anwaltskanzlei) und erstellen dafür eine entsprechende E-Mail-Adresse.

In einem zweiten Schritt wird eine fiktive Kommunikation zwischen einem Angestellten des gefälschten Anwaltsbüros (zumeist nehmen die Betrüger dazu den Namen einer realen Person, welche dort arbeitet) und dem CEO der angegriffenen Firma erstellt.

Alle in dieser Fake-Kommunikation verwendeten E-Mail-Adressen sind korrekt – da diese in Wirklichkeit nie stattgefunden hat, sondern sehr gut gefälscht wurden.

In der gefälschten Kommunikation erkundigt sich die «Anwältin» beim CEO wegen einer angeblich noch nicht bezahlten Rechnung. In der ebenfalls gefälschten

Antwort des CEO – welche nun auch an die Buchhaltung der Firma gehen kann – anerkennt der CEO offenbar die Rechnung und weist die Buchhaltung an, möglichst rasch die Zahlung zu prüfen und allenfalls zu bezahlen.

Die Kommunikation läuft von nun an direkt zwischen der betrügerischen «Anwältin» und der Buchhaltung, die Betrüger haben freie Hand.

Kurz darauf meldet sich die «Anwältin» per E-Mail nochmals beim Direktor, bedankt sich für die Unterstützung und bittet die Buchhaltung um die rasche Abwicklung des Geschäfts. In dieser E-Mail ist aber nun die E-Mail-Adresse des CEO geändert, sodass eine Antwort an alle nicht zum CEO sondern zu den Betrügern gehen würde.»

Ein beliebtes Thema für den Betrug ist eine (fiktive) Firmenübernahme. Da geht es immer um grosse Beträge.

Die Täter gehen sehr geschickt und mit viel Druck vor. Sie sind gut organisiert und vorbereitet. Dem Buchhalter eines Unternehmens wird durch mehrfache E-Mails und Anrufe vorgespielt, eine dringende und geheime Geldüberweisung müsse schnell und unauffällig durchgeführt werden.

Zum Beweis der leidigen Aktualität von CEO-Betrügereien, hier der Link zu einem kürzlich bekannt gewordenen Fall: Betrüger erbeuten zwei Millionen von Erfurter Firma

Praxis-Tipps:

1. Soziale Netzwerke, in denen Mitarbeiter ihre Funktion und Tätigkeit oder persönliche Details preisgeben, stellen eine wichtige Informationsquelle dar. Checken Sie z.B. wie Ihre Mitarbeiter auf LinkedIn auftreten und weisen Sie Ihre Mitarbeiter an, was Job-mässig in den sozialen Netzwerken publiziert, resp. nicht publiziert werden darf.
2. Täter versuchen die E-Mail-Erreichbarkeiten der mit Geldtransaktionen betrauten Mitarbeiter herauszufinden. Die Systematik von Erreichbarkeiten ist entscheidend für den Erfolg des Betrugs. Machen Sie den Spam-Filter für Mitarbeiter der Finanzabteilung besonders undurchlässig und untersagen Sie automatische Abwesenheits-Email-Meldungen.
3. Die Kriminellen nutzen gerne die Sommerferien, da zu dieser Zeit viele Aufgaben von Stellvertreterinnen und Stellvertretern übernommen werden. Richten Sie als CEO einen Notfallkommunikationskanal (z.B. Pager) ein, auf dem Sie auch in den Ferien innert Stunden von Personen mit Banküberweisungskompetenz erreichbar sind. Legen Sie Maximalbeträge fest, die ohne Ihre mündliche Zweitbestätigung nicht überwiesen werden dürfen.

Quellen : *Deutsches Bundeskriminalamt Broschüre CEO-Fraud Warnhinweis*
it-markt.ch NCSC warnt vor CEO-Betrug