11 OPFER SIND GENUG.

Erstellt in Kooperation und Zusammenarbeit mit dem BKA Wiesbaden.

.BK BUNDESKRIMINALAMT

Bundeskriminalamt

Das Bundeskriminalamt informiert über den CEO-Betrug.

Über die Betrugsform

Beim CEO-Betrug geben sich Täter als Geschäftsführer (CEO) des Unternehmens aus und veranlassen einen Mitarbeiter zur Überweisung eines größeren Geldbetrages ins Ausland.

Über die Täter

Vorbereitung: Die Täter durchstöbern auf der Suche nach potentiellen Unternehmen Jahresberichte, das Firmenbuch, den Internetauftritt oder Werbebroschüren. Dabei legen sie ihr Augenmerk auf Angaben zu Geschäftspartnern und künftigen Investments. Für die Täter sind An- und Abwesenheiten von Interesse, da sie daraus einen Zeitpunkt für die Kontaktaufnahme herleiten. Zusätzlich nutzen sie soziale Netzwerke, in denen Mitarbeiter ihre Funktion und Tätigkeit oder persönliche Details preisgeben. Auf diese Weise, dem so genannten „social engineering", verschaffen sich die Täter notwendiges Insiderwissen.

Tatbegehung: Die Täter nehmen mit den ausgeforschten Mitarbeitern Kontakt auf und geben sich als deren Geschäftsführer oder Vorstände aus. Dabei fordern sie eine dringende Überweisung größerer Geldbeträge auf Konten ins Ausland. Als Vorwand für eine strikte Geheimhaltung wird z.B. eine angebliche Unternehmensübernahme genannt. Die erste Kontaktaufnahme durch den CEO erfolgt in der Regel über E-Mail, wobei die E-Mail-Adressen manipuliert werden. In weiterer Folge wird die Dringlichkeit durch eine Drittperson, einem Juristen, Geschäftspartner oder Berater telefonisch bestätigt.

Schäden: Die Kriminellen konnten auf diese Weise in Österreich in den letzten Jahren einen zweistelligen Euro-Millionenbetrag erbeuten. Der Schaden ist aber nicht nur finanzieller Natur, sondern er verunsichert die Unternehmer und die Mitarbeiter.

Unsere Hilfe

Wir wollen Ihnen helfen, damit Ihr Unternehmen nicht Opfer eines CEO-Betrugs wird und haben die wichtigsten Schutzmaßnahmen für Sie zusammengefasst. Informieren Sie Ihre Mitarbeiter über dieses Phänomen! Führen Sie klare Abwesenheitsregelungen und interne Kontrollmechanismen ein. Achten Sie darauf, welche Informationen über Ihr Unternehmen öffentlich sind bzw. wo und was Sie und Ihre Mitarbeiter im Zusammenhang mit Ihrem Unternehmen publizieren. Spamfilter bieten bei diesem Phänomen keinen Schutz gegen einen Angriff!

Welche Schritte sollen vor der Durchführung von ungewöhnlichen Zahlungsanweisungen beachtet werden:

Überprüfen Sie eingelangte E-Mails auf die korrekte Schreibweise der Absenderadresse. Verwenden Sie dazu die Antwortfunktion und kontrollieren Sie die Absenderadresse genau.

Verifizieren Sie durch gezielte Rückfragen die Zahlungsanweisung über einen anderen Kommunikationskanal, wie z.B. ein persönliches Gespräch.

Hinterfragen Sie Zahlungsanweisungen auf unbekannte oder neue Konten. Seien Sie bei atypischen Länderkennzeichen des IBAN besonders vorsichtig und skeptisch.

Bewahren Sie Ruhe. Die Täter versuchen Sie durch Zeitdruck zu einer unüberlegten Überweisung zu drängen.

Kontaktieren Sie bei Verdacht eine vorgesetzte Person. Lassen Sie sich nicht verunsichern und halten Sie den gewohnten Prozess und das Vier-Augen-Prinzip unbedingt ein.

Notfallplan

Rascher Kontakt mit Bank: Wenn Sie den Verdacht haben Opfer dieses Betrugsmodells geworden zu sein, dann wenden Sie sich sofort an Ihre Bank, um die Zahlung umgehend stoppen zu lassen.

Anzeige bei der Polizei: Natürlich hilft Ihnen auch die Polizei. Zeigen Sie den Sachverhalt an der nächsten Polizeidienststelle an. Nehmen Sie bitte dazu alle Ihnen vorliegenden Unterlagen mit.

Kontakt: Im Bundeskriminalamt steht Ihnen eine Ansprechstelle unter **ceo-fraud@bmi.gv.at** zur Verfügung.