

► Prävention kompakt

Auf diesen Seiten finden Sie nützliche Erklärungen von Begriffen rund um das Thema Prävention von A wie A.C.A.B. bis Z wie Zoll.



CEO-Fraud

Beim CEO-Fraud („Chef-Trick“) geben sich Täter als Geschäftsführer (CEO) eines Unternehmens aus und veranlassen einen Mitarbeiter zum Transfer eines größeren Geldbetrags ins Ausland. Zuvor sammeln sie jegliche Art von Informationen über den Betrieb.

Fiktive Chefs verschicken Mails

Zur Tatvorbereitung verschaffen sich die Täter zunächst das für den Betrug notwendige Insiderwissen über das anzugreifende Unternehmen. Dazu nutzen sie vor allem Informationen, die Unternehmen in Wirtschaftsberichten, im Handelsregister, auf ihrer Homepage oder in Werbebroschüren veröffentlichen. Dabei legen sie ihr Augenmerk insbesondere auf Angaben zu Geschäftspartnern und künftigen Investments. Auch soziale Netzwerke wie Facebook, LinkedIn oder Xing, in denen Mitarbeiter ihre Funktion und Tätigkeit oder persönliche Details preisgeben, sind für sie eine wichtige Informationsquelle. So bringen die Angreifer zum Beispiel in Erfahrung, wann der Chef im Urlaub ist und wo er ihn verbringt. Die Täter finden bei ihrer Recherche auch heraus, wer in der Firma für wichtige Überweisungen und Geldtransfers zuständig ist. Anschließend nehmen sie Kontakt mit diesem Mitarbeiter auf und geben sich als Geschäftsführer (CEO), Leitende Angestellte oder Handelspartner aus. Dabei fordern sie – etwa unter dem Vorwand einer angeblichen Unternehmensübernahme oder geänderten Kontoverbindung – den Transfer eines größeren Geldbetrages auf asiatische Konten in China und Hongkong, aber auch in osteuropäische Staaten. Die Kontaktaufnahme erfolgt schließlich über E-Mail oder Telefon, wobei E-Mail-Adressen verfälscht und Telefonnummern verschleiert werden. Oft werden die ausführenden Mitarbeiter unter Zeitdruck gesetzt und zur strikten Geheimhaltung der Überweisung aufgefordert.

Mittelständler, aufgepasst!

Die ersten Fälle dieser Betrugsmasche traten in den USA auf. Inzwischen wird das Phänomen weltweit beobachtet. Seit 2013 häufen sich die Fälle auch in Deutschland. Das Bundeskriminalamt zählte seitdem mehr als 60 Betrugsfälle mit einem Gesamtschaden von 106 Millionen Euro. Zu den bekanntesten Opfern von CEO-Fraud gehört unter anderem der bayerische Autozulieferer Leoni mit einem Schadensvolumen von 40 Millionen Euro. Die Betrugsform erfasst allerdings nicht nur Großunternehmen, sondern fokussiert sich zunehmend auch auf eigentümergeführte Kleinunternehmen und Mittelständler.

Präventive Empfehlungen

Lassen sie sich von Ihren Geschäftsbanken über mögliche Schutzmechanismen gegen ungewollte Überweisungen beraten.

Überprüfen Sie Ihr internes Kontrollsystem in den Zahlungsverkehrs- und Stammdatenprozessen.

Testen Sie regelmäßig sowohl Ihre technische als auch organisatorische Informationssicherheit.

Klären Sie Ihre Führungskräfte und Sachbearbeiter über die Gefahr auf und sensibilisieren Sie ihre Mitarbeiter dafür, auf E-Mails mit Überweisungsanforderungen skeptisch zu reagieren.

Führen Sie ggf. (CEO-Fraud-Awareness-)Schulungen für das im Unternehmen relevante Personal durch.

Siehe auch:

[Phishing](#)

[Cybercrime](#)

[Malware/Spyware](#)

[Zurück](#)

© Verlag Deutsche Polizeiliteratur