PRÄVENTION

INFORMIERT

Sichere Kommunikation im Unternehmen: So schützen Sie sich vor Betrugsversuchen

Einfallsreich und raffiniert versuchen Kriminelle mit unterschiedlichen Methoden Unternehmen um hohe Geldsummen zu betrügen. Dabei nutzen Sie geschickt Schwachstellen in der Kommunikation aus. Wir erklären die wichtigsten Maschen und geben Ihnen passende Verhaltenstipps.

Was ist CEO-Fraud?

Beim CEO-Fraud (Chef Executive Officer), auch bekannt als Geschäftsführer-Betrug oder Fake President, geben sich Kriminelle als hochrangige Führungskräfte aus. Unter einem dringenden Vorwand bringen sie Mitarbeitende aus Finanzabteilung und Buchhaltung dazu, große Geldbeträge zu überweisen. Zur Kontaktaufnahme nutzen sie gefälschte E-Mail-Adressen oder verschleierte Telefonnummern. Dieses Insiderwissen erlangen sie u. a. über veröffentlichte Berichte, das Handelsregister oder Social Media.

Was ist BEC-Fraud?

Beim BEC-Fraud (Business Email Compromise) nutzen Betrügerinnen und Betrüger bereits etablierte Geschäftsbeziehungen zwischen Unternehmen aus. Durch Phishing- oder Hackingattacken spähen sie sensible Zugangsdaten aus. Rechnungsdokumente, Zahlungs- und Kundendaten werden abgefangen und manipuliert. Sie täuschen die Identität eines Geschäftspartners vor und schleusen gefälschte Rechnungen in deren Kommunikationswege ein. Rechnungssteller, Form und Inhalt sind oftmals richtig – die Kontoverbindung weicht jedoch ab. Oder sie geben an, dass sich die Bankverbindung geändert hätte. Rechnungszahlungen landen so auf dem Konto der Kriminellen.

Was ist Fake Customer?

Bei der Variante des Fake Customer geben sich Betrügerinnen und Betrüger als Großkunden aus. Sie bringen Unternehmen dazu, Produkte oder Dienstleistungen bereitzustellen, ohne diese zu bezahlen. Dabei bestellen sie Waren im großen Stil und täuschen Zahlungsbereitschaft vor. Die Lieferung geht oftmals ins Ausland und wird unterwegs umgeleitet. Die Anlieferung erfolgt in Lagerhallen oder „Self-Store“-Lagerplätzen, die online von Einzelpersonen angemietet werden können.

Unsere Tipps

- Achten Sie darauf, welche Informationen Sie über Ihr Unternehmen veröffentlichen.
- Informieren Sie Ihre Mitarbeitenden über die Betrugsmaschen.
- Führen Sie klare Abwesenheitsregelungen und interne Kontrollmechanismen ein, insbesondere für ungewöhnliche Überweisungsaufträge oder veränderte Bankverbindungen:
  - Überprüfung der Absendeadressen, E-Mails und Internetseiten des Auftraggebers.
  - Verifizierung der Zahlungsaufforderung beim genannten Auftraggeber, z. B. per Rückruf.
  - Kontaktaufnahme mit Vorgesetzten oder der Geschäftsleitung.
- Installieren und aktualisieren Sie regelmäßig Ihre Sicherheitssoftware.
- Nutzen Sie eine Zwei-Faktor-Authentifizierung für E-Mail-Konten und andere wichtige Systeme, um unbefugten Zugriff zu verhindern.
- Wenden Sie sich im Betrugsfall schnellstmöglich an Ihre Bank, um die Zahlung zu stoppen und das Geld zurückzuholen.
- Erstatten Sie Strafanzeige bei der Polizei.

Weitere Informationen und Tipps erhalten Sie unter www.polizei-beratung.de.

Landeskriminalamt Baden-Württemberg
Referat Prävention
Taubenheimstraße 85
70372 Stuttgart
Telefon: 0711 5401 3458
E-Mail: praevention@polizei.bwl.de

Stand: Juli 2024