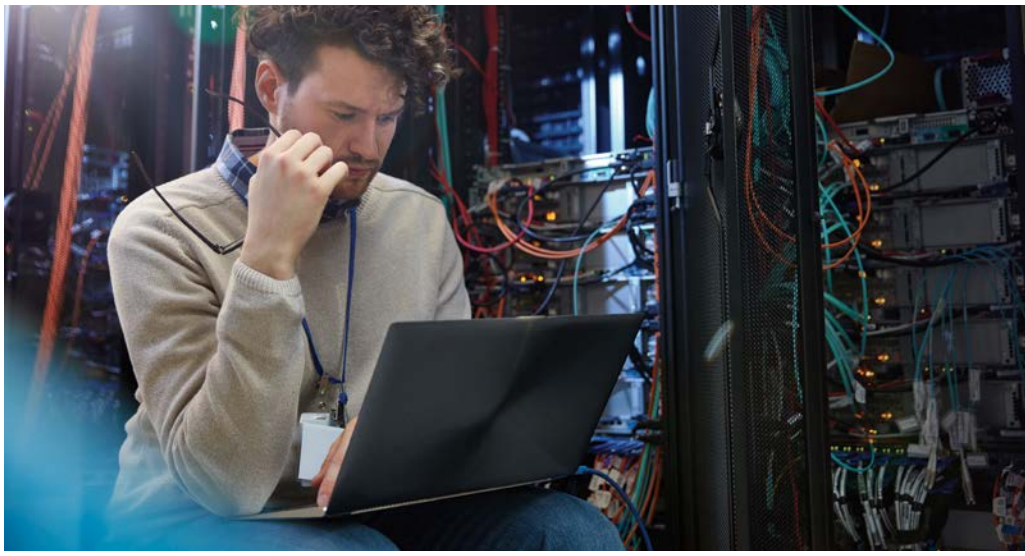
Betrug im Zahlungsverkehr – so können Sie Ihr Unternehmen schützen

Betrug im Zahlungsverkehr führt bei Schweizer Unternehmen zu beträchtlichen finanziellen Schäden – Tendenz zunehmend. Welches sind Warnsignale und wie können Sie sich bzw. Ihr Unternehmen aktiv davor schützen?



Business E-Mail Compromise

Business E-Mail Compromise gilt als eine der grössten Cyber-Bedrohungen sowohl für die Wirtschaft als auch für ein einzelnes Unternehmen. Wie ein solcher Betrug abläuft, sehen Sie hier:

1

Spionage

- Täter sammeln öffentlich verfügbare Informationen über das Unternehmen und seine Mitarbeitenden.
- Täter dringen in die IT-Infrastruktur des Unternehmens oder eines Geschäftspartners ein (z. B. mittels Phishing-Attacke).

2

Täuschung

- Täter kontaktieren die Finanzabteilung des Unternehmens per E-Mail.
- Unter einem Vorwand soll eine fällige Zahlung an ein bislang unbekanntes Bank konto ausgeführt werden.

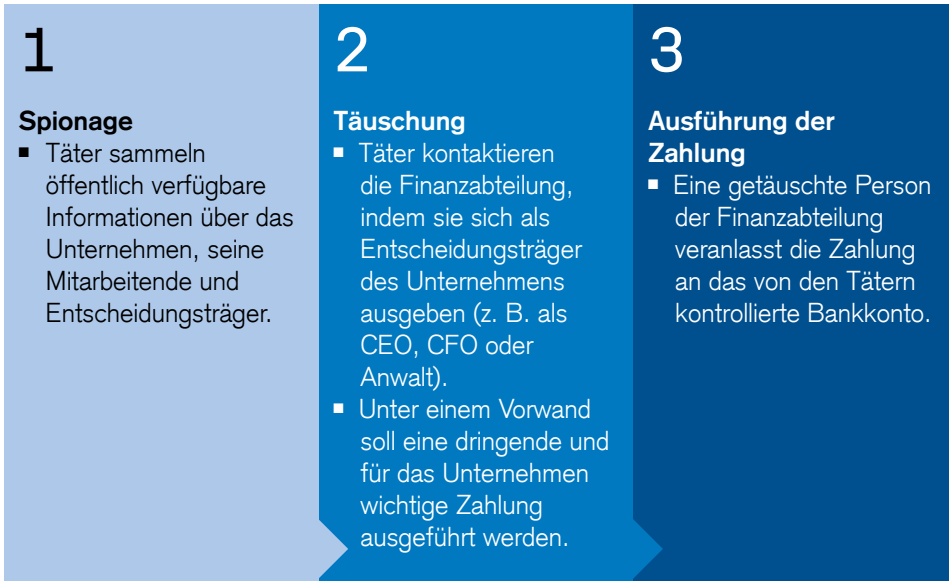
3

Ausführung der Zahlung

- Eine getäuschte Person der Finanzabteilung veranlasst die Zahlung an das von den Tätern kontrollierte Bankkonto.

CEO-Betrug

Ein erfolgreicher CEO-Betrug kann Ihr Unternehmen ruinieren. Die Betrüger wollen an Ihr Firmenvermögen. Wie ein solcher Betrug abläuft, sehen Sie hier:



Das müssen Sie wissen:

- Jedes Unternehmen kann Ziel von Betrügern werden, ungeachtet der Grösse, der Branche oder des Domizils.
- Eine schwach geschützte IT-Infrastruktur öffnet den Betrügern Tür und Tor.
- E-Mail-Kommunikation ist nicht sicher und kann manipuliert werden.

Als Unternehmer sind Sie diesen Risiken nicht hilflos ausgeliefert. Mit den folgenden Verhaltensmassnahmen erschweren Sie den Betrügern das Handwerk und vermeiden damit finanzielle Schäden.

So können Sie sich schützen:

- Schützen Sie Ihre IT-Infrastruktur nach aktuellsten Standards.
- Etablieren Sie mit Ihren Kunden und Lieferanten unterschiedliche Kommunikationskanäle und halten Sie diese aktuell (z. B. Telefon, Mobile, E-Mail, Postanschrift).
- Sollten Sie von Ihren Geschäftspartnern abweichende Zahlungsinstruktionen (z. B. andere Bank/Kontonummer) erhalten, verifizieren Sie diese. Wichtig: Tun Sie dies über einen sicheren Kanal, z. B. über eine bereits validierte Telefonnummer.
- Installieren Sie Buchhaltungsprozesse, welche die Ausführung von betrügerischen Transaktionen verhindern, d. h.:
  - Instruieren Sie Ihre relevanten internen Abteilungen hinsichtlich der Phänomene Business E-Mail Compromise und CEO-Betrug.
  - Vermeiden Sie Einzelzeichnungsrechte.
  - Halten Sie Ihre Mitarbeitenden dazu an, verdächtige Beobachtungen und Ereignisse umgehend einer internen zentralen Stelle zu melden.
- Prüfen Sie, welche Informationen Sie über Ihr Unternehmen und Ihre Angestellten veröffentlichen wollen. Beschränken Sie diese auf ein Minimum.
- Erwägen Sie eine Strafanzeige, wenn Sie von Betrug betroffen sind; auch dann, wenn kein finanzieller Schaden entstanden ist.
- Informieren Sie im Ereignisfall unverzüglich Ihre Hausbank. So kann Ihre Bank die notwendigen Schutzmassnahmen ergreifen und im Schadensfall eine betrügerische Transaktion reklamieren.

Für Rückfragen steht Ihnen Ihre Kundenberaterin oder Ihr Kundenberater gerne zur Verfügung.

CREDIT SUISSE (Schweiz) AG
Postfach
CH-8070 Zürich
credit-suisse.com

SMMI 3 C2611 12.2020