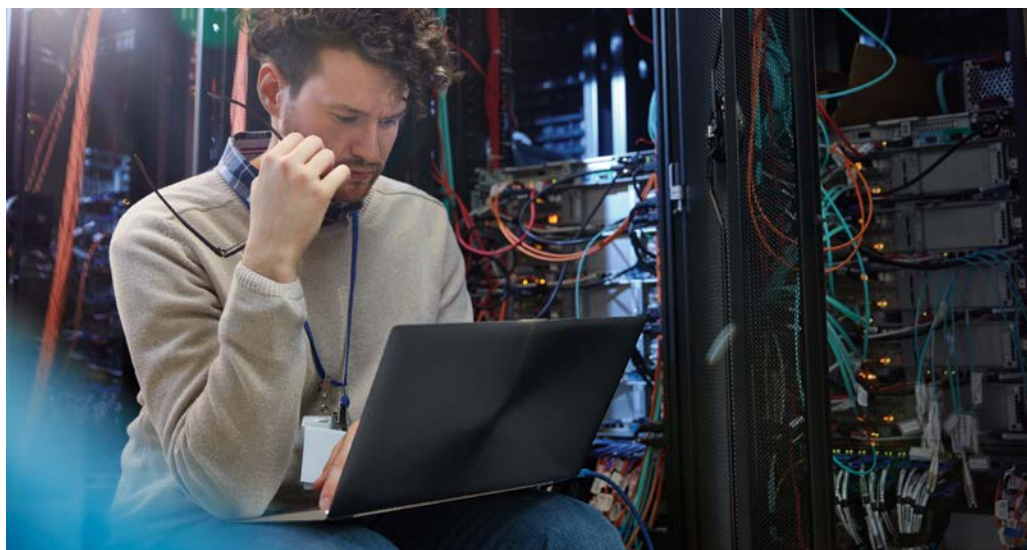


Betrug im Zahlungsverkehr – so können Sie Ihr Unternehmen schützen

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

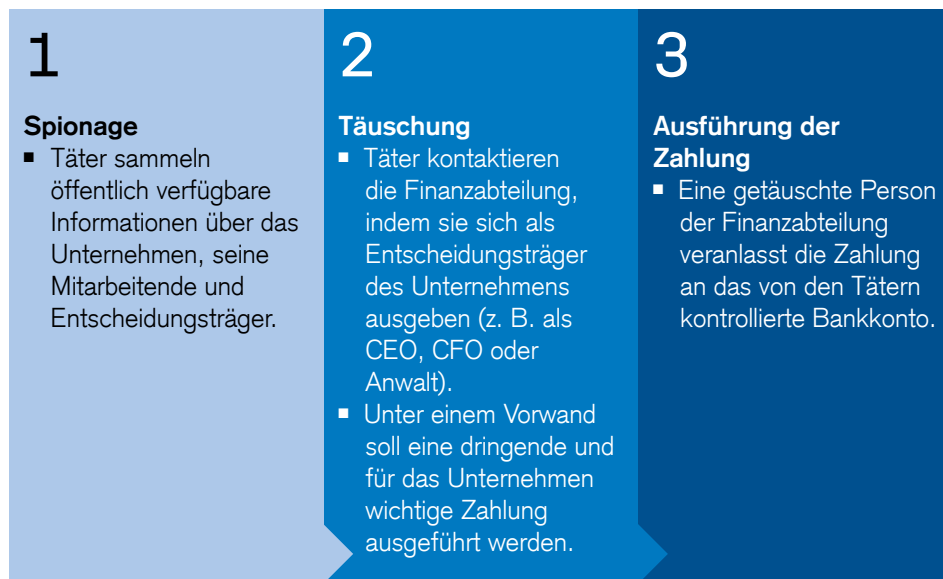
- Täter kontaktieren die Finanzabteilung des Unternehmens per E-Mail.
- Unter einem Vorwand soll eine fällige Zahlung an ein bislang unbekanntes Bankkonto ausgeführt werden.

3

**Ausführung der
Zahlung**

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

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.

Bitte beachten Sie, dass die Credit Suisse (Schweiz) AG keine Gewähr hinsichtlich Inhalt und Vollständigkeit der obigen Empfehlungen geben kann. Es handelt sich dabei lediglich um Verhaltensempfehlungen, die das Risiko von Betrugsfällen mindern, solche aber nicht ausschliessen können.



CREDIT SUISSE (Schweiz) AG

Postfach
CH-8070 Zürich
credit-suisse.com

Die bereitgestellten Informationen dienen Werbezwecken. Sie stellen keine Anlageberatung dar, basieren nicht auf andere Weise auf einer Berücksichtigung der persönlichen Umstände des Empfängers und sind auch nicht das Ergebnis einer objektiven oder unabhängigen Finanzanalyse. Die bereitgestellten Informationen sind nicht rechtsverbindlich und stellen weder ein Angebot noch eine Aufforderung zum Abschluss einer Finanztransaktion dar. Diese Informationen wurden von der Credit Suisse Group AG und/oder mit ihr verbundenen Unternehmen (nachfolgend «CS») mit grösster Sorgfalt und nach bestem Wissen und Gewissen erstellt. Die in diesem Dokument enthaltenen Informationen und Meinungen repräsentieren die Sicht der CS zum Zeitpunkt der Erstellung und können sich jederzeit und ohne Mitteilung ändern. Sie stammen aus Quellen, die für zuverlässig erachtet werden. Die CS gibt keine Gewähr hinsichtlich des Inhalts und der Vollständigkeit der Informationen und lehnt, sofern rechtlich möglich, jede Haftung für Verluste ab, die sich aus der Verwendung der Informationen ergeben. Ist nichts anderes vermerkt, sind alle Zahlen ungeprüft. Die Informationen in diesem Dokument dienen der ausschliesslichen Nutzung durch den Empfänger. Weder die vorliegenden Informationen noch Kopien davon dürfen in die Vereinigten Staaten von Amerika versandt, dorthin mitgenommen oder in den Vereinigten Staaten von Amerika verteilt oder an US-Personen (im Sinne von Regulation S des US Securities Act von 1933 in dessen jeweils gültiger Fassung) abgegeben werden. Ohne schriftliche Genehmigung der CS dürfen diese Informationen weder auszugsweise noch vollständig vervielfältigt werden. Ihre personenbezogenen Daten werden in Übereinstimmung mit der Datenschutzerklärung der Credit Suisse verarbeitet, die an Ihrem Wohnsitz über die offizielle Website der Credit Suisse <https://www.credit-suisse.com> abrufbar ist. Die Credit Suisse Group AG und ihre Tochtergesellschaften nutzen unter Umständen Ihre grundlegenden personenbezogenen Daten (z. B. Kontaktangaben wie Name und E-Mail-Adresse), um Ihnen Marketingunterlagen in Zusammenhang mit ihren Produkten und Dienstleistungen bereitzustellen. Falls Sie solche Unterlagen nicht mehr erhalten möchten, wenden Sie sich bitte jederzeit an Ihre Kundenberaterin oder Ihren Kundenberater.

Copyright © 2020 Credit Suisse Group AG und/oder mit ihr verbundene Unternehmen. Alle Rechte vorbehalten.