Banken

FFU Frankreich für Unternehmen

Grundlagenwissen

Betrug: Schützen Sie sich!

Oktober 2020

Betrüger gehen heutzutage immer professioneller vor, und wenn es ihnen gelingt, so können die Schäden für ein Unternehmen gravierend sein: finanzielle – und Datenverluste, Blockieren der Unternehmenstätigkeiten oder gar der Verlust vertraulicher Informationen.

Wenn ein Unternehmen international tätig wird, steigt das Risiko, Betrugsversuchen zum Opfer zu fallen. Des Weiteren ist es im Interesse eines jeden Unternehmens, insbesondere nach dem Corona-Lockdown, sich gegen Betrug abzusichern, um die Unternehmenstätigkeiten zu schützen. Schon mit sehr einfachen Maßnahmen kann eine sehr große Wirkung erzielt werden.

Statistisch betrachtet ist der Betrug des „falschen Lieferanten“ mit 28 % aller Betrugsversuche die gängigste Technik. Hierbei fälschen die Betrüger die Identität eines Lieferanten und kontaktieren seine Kunden, um sie über eine Änderung der Bankdaten (IBAN) zu informieren. Die Kunden tätigen ihre Überweisungen dann auf die „neue“ IBAN und erhalten weder die Waren noch eine Rückerstattung. Um sich dagegen zu schützen, können Sie ganz einfach folgende Maßnahmen treffen:

- Sichern Sie Ihre Datenbank mit Lieferantenkontakten und führen Sie ein Verfahren ein, um das Ändern von Lieferanteninformationen als einen sensiblen Vorgang zu definieren.
- Bevor Sie Informationen ändern, tätigen Sie IMMER einen Kontrollanruf auf eine Ihnen bereits bekannte Telefonnummer des Lieferanten.

An 2. Stelle der Betrugsversuche steht direkt nach dem Betrug des „falschen Lieferanten“ mit 23% der sogenannte „CEO-Betrug“. Das Verfahren ist immer dasselbe: Der Betrüger fälscht die Identität eines Anwalts, eines Notars oder die Identität des Geschäftsführers und fordert die Tätigung von Überweisungen aus dringenden und vertraulichen Gründen.

Auf diesen Betrug folgt meist ein zweiter Akt, wo die Identität der Polizei gefälscht wird. Der falsche Polizist fordert das Unternehmen auf, die Überweisungen erneuert vorzunehmen, um die Betrüger „auf frischer Tat“ zu ertappen. Natürlich ist es meist unmöglich, das Geld zurückzuerlangen. Der CEO-Betrug lässt sich durch folgende Mittel einfach bekämpfen:

- Tätigung eines systematischen Kontrollanrufs beim Geschäftsführer, um den Vorgang zu bestätigen,
- Das vier-Augen-Prinzip zur Bestätigung von Überweisungen,

CIC Est DACH Firmenkunden Die Partner Bank für Ihr Frankreichgeschäft

CIC Est
Agence Entreprises Europe
31 rue Jean Wenger Valentin
F-67000 Strasbourg

+33 (0)3 88 37 73 37
cic-est@ffu.eu
www.cic.fr/fr/banques/entreprises

- Ein personalisierter Bankzugang für jeden Zugangsberechtigen,
- Die Überprüfung von IBAN-Angaben mit Sepamail Diamond.

Gerne können Sie Ihren Firmenkundenberater hierauf ansprechen: Bei der CIC haben wir einfache und sichere Lösungen, um gegen CEO-Betrug vorzugehen. Unsere Firmenkundenberater unterstützen Sie gerne.

Bei dem dritten Betrugsversuch handelt es sich um einen „falschen Techniker“, der ein Software-Update oder eine Software-Überprüfung vorgibt. Die Überprüfung der Kompatibilität des PCs mit der starken Authentifizierung wird zudem als Grund für den Eingriff angegeben. Anhand einer Phishing-Email mit einem gefälschten Link oder einer falschen Internetseite, übernimmt der Betrüger die Kontrolle über den Computer. So werden meist Spyware, Malware oder Ransomware installiert oder Überweisungen getätigt. Dies gefährdet die Vertraulichkeit der Daten. Ferner können Firmenkonten auf diesem Wege im Handumdrehen geleert werden. Um gegen den Betrug des „falschen Technikers“ vorzugehen, sollten Sie Folgendes beachten:

- Klicken Sie nie auf einen Link und öffnen Sie nie einen Anhang, der Ihnen von einem unbekannten Absender zugesandt wurde.
- Halten Sie Ihre Anti-Virus Software und Ihren PC immer auf dem neusten Stand.
- Wenden Sie sich im Zweifelsfall direkt an Ihre IT-Abteilung.
- Benutzen Sie NIE einen USB-Stick, den Sie zufällig gefunden haben und dessen Herkunft Sie nicht kennen.

In Rahmen der Identitätsfälschung wird auch die Identität von staatlichen Ämtern gefälscht. Zurzeit fälschen Betrüger oft die Identität des französischen Finanzamts (*Direction Générale des Finances Publiques*) und verlangen verschiedene Unterlagen (Kopien offener Rechnungen, Kontaktdaten von Mitarbeitern aus der Buchhaltung, Lieferanten- und Kundeninformationen, Vertragskopien etc.), unter dem Vorwand einer Prüfung des „Einhaltens internationaler Vorschriften und SEPA-Bedingungen“.

Solche Daten werden anschließend verwendet, um betrügerische Überweisungen gegenüber Kunden und Lieferanten zu tätigen. Wir weisen darauf hin, dass Staatsbehörden solche Daten nie verlangen! Generell sollten Sie stets auf die E-Mail-Adresse des Absenders achten.

Nehmen Sie das Thema Datenschutz nicht auf die leichte Schulter und gehen Sie stets umsichtig vor. Schützen Sie Ihren PC und Ihr Handy durch entsprechende Sicherheitssoftware und nehmen Sie auf Dienstreisen nur die nötigsten Informationen mit.

Die einfachste und effizienteste Maßnahme gegen Betrug ist die regelmäßige Sensibilisierung des Personals. Gern können die Firmenkundenberater der CIC das Thema

CIC Est DACH Firmenkunden Die Partner Bank für Ihr Frankreichgeschäft

CIC Est
Agence Entreprises Europe
31 rue Jean Wenger Valentin
F-67000 Strasbourg

+33 (0)3 88 37 73 37
cic-est@ffu.eu
www.cic.fr/fr/banques/entreprises

im Rahmen eines Kundentermins ansprechen und Ihrem Unternehmen entsprechende Unterlagen zur Verfügung stellen. Sprechen Sie uns diesbezüglich gerne an! Mehr als 80% der Betrugsversuche werden durch eine menschliche Reaktion oder dank interner Verfahren abgewehrt.

Ihre deutschsprachige Ansprechpartnerin:

CIC Est — DACH Firmenkunden — Die Partner Bank für Ihr Frankreichgeschäft

Noémie Vogt
Vertriebsassistentin

vogt@ffu.eu
+33 (0)3 88 37 73 41