Dezember 2016

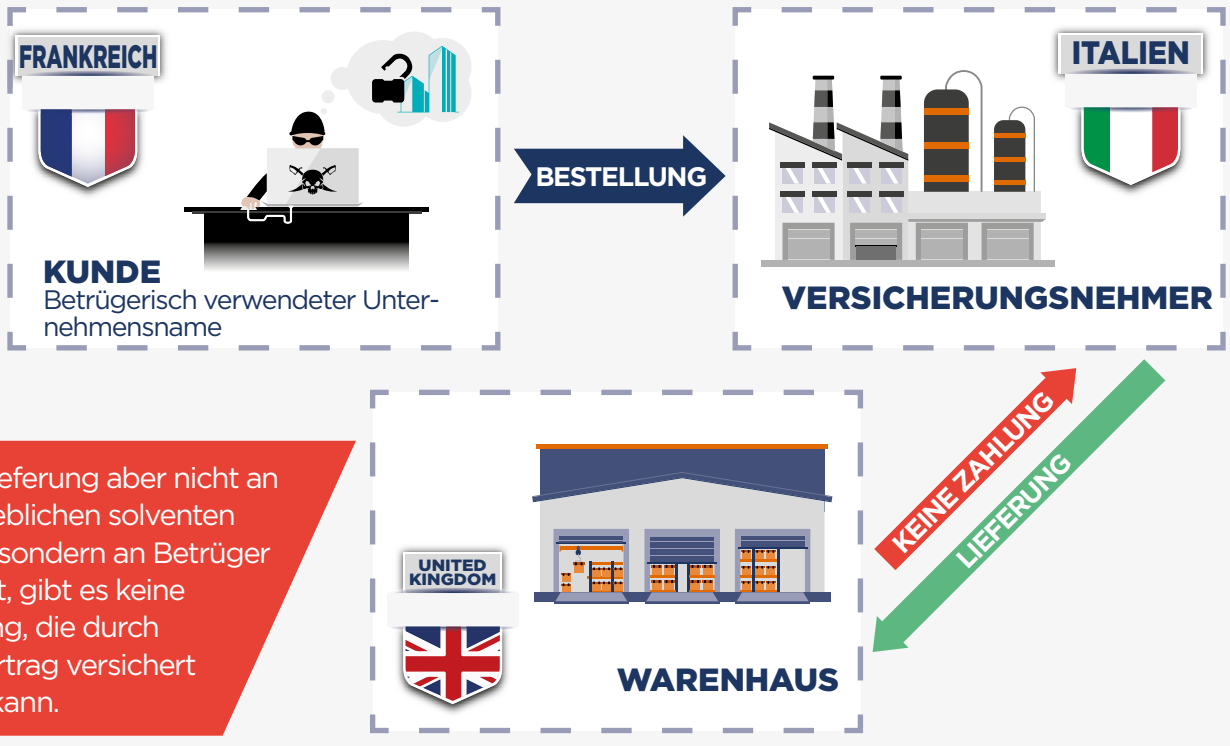
WARNUNG VOR IDENTITÄTSBETRUG BEI UNTERNEHMEN

Identitätsbetrug bei Unternehmen ist ein “blühendes Geschäft” in der B2B-Welt. Der Umfang und die ständige Ausbreitung des Betrugs erfordern proaktive Maßnahmen zum Schutz des Unternehmensvermögens und seiner Identität.

Die Verwendung von falscher Unternehmensidentität oder falschen Unternehmensdaten einer anderen Gesellschaft für gesetzwidrige Handlungen stellt ein erhebliches Betriebsrisiko dar.
In den vergangenen Wochen erhielt Coface Informationen zu mehreren Betrugsfällen im Zusammenhang mit Identitätsdiebstahl, daher rufen wir zu erhöhter Vorsicht auf.

In der Praxis nutzen Betrüger die geschäftliche Identität tatsächlich bestehender Unternehmen, vorzugsweise mit guten Zahlungsverhalten und einem guten Ruf, um Waren und Leistungen von unseren Kunden/Versicherungsnehmern zu erhalten.
Das neueste Betrugsmuster, mit dem wir in letzter Zeit konfrontiert wurden, kann wie folgt beschrieben werden:

Beispiel: Betrug mit Unternehmensidentität



Da die Lieferung aber nicht an den angeblichen solventen Kunden, sondern an Betrüger erfolgt ist, gibt es keine Forderung, die durch einen Vertrag versichert werden kann.

Zur Durchführung ihrer Geschäfte sind die Betrüger sehr gut organisiert. Um in einem Unternehmen ein Kundenkonto eröffnen zu können, beantragen sie Telefonverbindungen, erstellen E-Mail-Adressen, fälschen Bestellformulare, kaufen Gründungsurkunden und Finanznachweise des Handelsregisters.
Aus diesem Grund sollten beim Eingang von Bestellungen einige Vorsichtsmaßnahmen beachtet werden, insbesondere, wenn diese aus dem Ausland oder von einem neuen Kunden kommen.

Tatsächlich ist ein gefälschtes Bestellformular nie perfekt. Zur Vermeidung eines gefälschten Auftrags lohnt sich der Aufwand einer kurzen Überprüfung immer.
Wenn Ihre Einkaufs-/Vertriebsabteilung eine Bestellung erhält, kann die folgende Checkliste zur Erkennung von Problembereichen Hilfestellung bieten.

Bitte beachten Sie:

- Vergleichen Sie das Firmenlogo auf der Website mit dem Logo auf der Bestellung. Es könnte abweichen.
- Vergleichen Sie das Format der E-Mail-Adresse (Name der Person oder des Unternehmens) Ihres Ansprechpartners mit den Adressen auf der Website (oft unter dem Link “Kontakt”), da meist für alle Mitarbeiter des Unternehmens das gleiche Format gilt. Jeder Unterschied sollte verdächtig erscheinen (z. B.: david_smith@company.fr wird zu d.smith@company-service.com oder smith_david@company-group.eu....) Seien Sie besonders vorsichtig bei allgemeinen E-Mail-Adressen, z. B.: accountancy_company.com

Betrüger benutzen meist die Namen von Personen, die tatsächlich in dem Unternehmen arbeiten.

- Vergleichen Sie das Format der Telefonnummern (insbesondere die ersten beiden Ziffern)
- Prüfen Sie, ob das Unternehmen in dem Land, in das die Lieferung erfolgen soll, eine Geschäftstätigkeit ausübt, dort eine Niederlassung oder ein Projekt betreibt.
- Syntax- oder Rechtschreibfehler könnten im Bestellformular auftauchen, insbesondere in den Besonderen Bestimmungen. Bitte prüfen sie diese Dokumente also sorgfältig und erstellen Sie interne Prozesse zur Überprüfung der Echtheit der Dokumente.
- Fragen Sie sich, ob die Geschäftstätigkeit des Kunden zu Ihrer Geschäftstätigkeit passt.

Vertrauen ist gut, Kontrolle ist besser: Sollten Zweifel bestehen (Auftrag, Änderungen der Bankverbindung, ...), fordern Sie von Ihrem Kunden eine Bestätigung an und stellen Sie sicher, dass die Mitarbeiter Ihres Rechnungswesens die Brisanz des Themas erkennen.
Nicht zu vergessen: Fälle von Phishing und Zahlungen auf gefälschte Bankkonten sind immer noch aktuell. Daher ist immer darauf zu achten, dass alle Änderungsanfragen (Adressen, Bankkonto) mit Ihrem Lieferanten abgestimmt und bestätigt werden.

FAXE UND E-MAILS SIND NICHT SICHER

coface
FOR SAFER TRADE