Allianz

Allianz Trade

DIE CHECKLISTE FÜR DEN ERNSTFALL

Was tun bei Zahlungsbetrug via Internet?

Die wichtigste Regel in sogenannten Fake-President- und Payment-Diversion-Fällen: Schnell handeln!

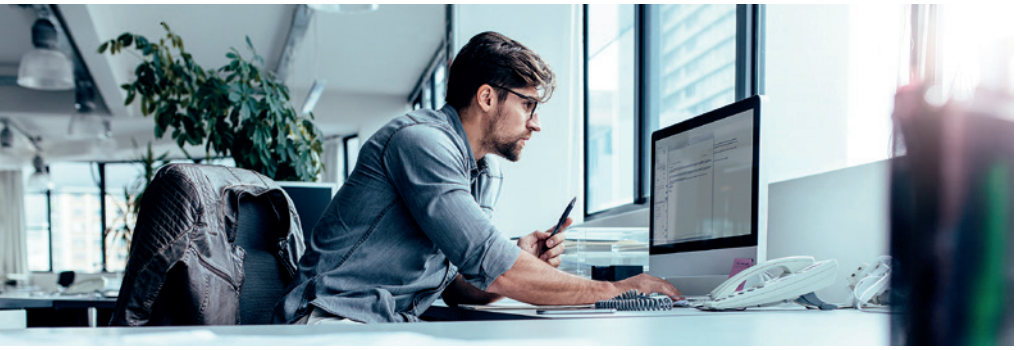
Geschwindigkeit ist im Fall von Cyberkriminalität entscheidend. Die Täter operieren im Internet und nutzen dessen Geschwindigkeit; das Überwinden von Staatsgrenzen gehört zu ihrem Tatplan und soll es Ihnen möglichst schwer machen, die Ihnen entzogenen Vermögenswerte wiederzuerlangen.
Dem können Sie nur durch rasches und zielgerichtetes Handeln begegnen. Verfahren Sie daher bitte entsprechend unseren Handlungsempfehlungen. Diese schaffen nach unserer Erfahrung die besten Möglichkeiten, um den Ihnen entstandenen Schaden wiedergutzumachen oder zumindest zu reduzieren bzw. einen Schaden gleich zu verhindern.

1. Unterrichten Sie sofort Ihre Bank von dem Schadenfall und fügen Sie alle verfügbaren Unterlagen bei.

- Bitten Sie darum, dass die **Überweisung nicht ausgeführt** wird[1].
- Sollte die Überweisung bereits ausgeführt sein, bitten Sie Ihre Bank (u. U. auch deren Geschäftsleitung), **umgehend** die Empfängerbank per SWIFT[2]-Mitteilung vom Verdacht einer Straftat zu unterrichten, diese um Rücküberweisung des Betrages zu bitten sowie eine Geldwäsche-Verdachtsanzeige zu stellen.
- Lassen Sie sich von Ihrer Bank eine **Ausfertigung** der SWIFT-Mitteilung für Ihre Unterlagen **aushändigen.**

[1] Im Regelfall wird die Überweisung im elektronischen Bankenverkehr bereits ausgeführt worden sein.

[2] Banken kommunizieren weltweit einheitlich über das sogenannte SWIFT-System, mit dem Meldungen innerhalb kürzester Zeit gesichert zwischen Banken ausgetauscht werden können.



Fake President Fraud

Bei dieser Betrugsmasche geben sich die Täter als ein Organ des Unternehmens – meist ein Vorstandsmitglied oder Geschäftsführer – aus. Sie bitten per E-Mail oder Fax eine für die Bankgeschäfte verantwortliche Person im Unternehmen, eine dringende Überweisung auszuführen. Durch die **Vorspiegelung der falschen Identität** werden Zahlungen auf externe Konten angewiesen.

Payment Diversion Fraud

Betrug durch Umleitung von Zahlungsströmen, beispielsweise durch **Vorspiegelung von angeblich neuen Kontodaten** des Lieferanten.

2. Stellen Sie sicher, dass keine weiteren Zahlungen mehr geleistet werden und weiterhin eingehende E-Mails der mutmasslichen Täter umgehend der in Ihrem Haus zuständigen Stelle vorgelegt werden.

3. Sichern Sie alle verfügbaren Unterlagen, die direkt oder indirekt mit dem Schadenfall zu tun haben können, elektronisch und in Papierform wie z. B.

- E-Mails
- Kontoauszüge
- Überweisungsaufträge
- Telefonnotizen und dergleichen

4. Zeigen Sie uns den Schadenfall sofort an und fügen Sie alle vorhandenen Unterlagen bei.

- Gemeinsam mit Ihnen können wir Massnahmen auch im Ausland abstimmen, um den **weiteren Abfluss Ihrer Gelder zu stoppen.**
- **Je eher Sie uns unterrichten**, umso grösser sind die Chancen, einen gemeinsamen Weg zu finden, um den entstandenen Schaden wiedergutzumachen oder zumindest einzugrenzen.
- Je länger Sie warten, desto grösser sind die Chancen für die Täter, die Gelder weiter zu transferieren und die Wiedererlangung zu erschweren oder unmöglich zu machen.

5. Erstatten Sie Strafanzeige bei der für Sie zuständigen Staatsanwaltschaft und fügen Sie alle Ihnen zur Verfügung stehenden Unterlagen bei.

- Stimmen Sie das weitere Vorgehen mit dieser ab, gerade auch für Rechtshilfeersuchen ins Ausland.
- Lassen Sie sich das **Aktenzeichen** und möglichst auch den Namen der zuständigen Fachkraft der Staatsanwaltschaft mitteilen und teilen Sie uns diese Informationen mit.

6. Sensibilisieren Sie nochmals Ihre Mitarbeiter entsprechend unserer Betrugswarnung und für folgende Warnsignale:

- In einem bestehenden E-Mail-Verkehr tauchen plötzlich **neue Teilnehmer** auf.
  - Überprüfen Sie die E-Mail-Adressen.
  - Die Täter verwenden oft E-Mail-Adressen, die einer echten und Ihnen vermeintlich bekannten ähnlich sind, aber in einzelnen Buchstaben oder Zeichen abweichen.
- Seien Sie misstrauisch, wenn Sie eine **E-Mail von einem Mitglied der Geschäftsleitung** erhalten, in der Sie gebeten werden, **Zahlungen in erheblicher Höhe ins Ausland** vorzunehmen. Lassen Sie sich die Anweisung auf anderem Weg bestätigen – selbst wenn Sie um Verschwiegenheit gebeten werden und den Dienstweg ausser Acht zu lassen.
  - Oftmals wird für die Abwicklung der Zahlung an eine **eingeschaltete Rechtsanwaltskanzlei** verwiesen, die sich in der Folge mit Ihnen in Verbindung setzt, um weitere Anweisungen zu erteilen.
  - Überprüfen Sie, ob es die Kanzlei und die für diese auftretenden Rechtsanwälte überhaupt gibt. Die Einschaltung einer Kanzlei dient dazu, zusätzlichen Druck auszuüben und den Anschein der Rechtmässigkeit und Seriosität des behaupteten Geschäfts zu schaffen.
- Seien Sie misstrauisch, wenn ein Geschäftspartner **Zahlungen auf ein anderes Konto** als das langjährig verwendete wünscht. Lassen Sie sich dies von Ihrem Ansprechpartner Ihres Geschäftskunden zum Beispiel mit normaler Post bestätigen. **Verwenden Sie für Ihre Rückfrage in keinem Fall die Kontaktdaten, die in der verdächtigen E-Mail enthalten sind.**

Euler Hermes Switzerland
Office Lausanne
Office Lugano

Richtiplatz 1
Chemin de Bérée 52B
Via Guido Calgari 3

8304 Wallisellen
1010 Lausanne
6900 Lugano

fidelity.ch@allianz-trade.com
www.allianz-trade.ch
T +41 848 544 544