

# Euler Hermes Deutschland

Euler Hermes Deutschland  
Niederlassung der Euler Hermes SA, 22746 Hamburg

Division Specialty  
Department Business Fidelity

Tel. +49 (0) 40/88 34-2155  
Fax +49 (0) 40/88 34-2091  
EHKV02VSV  
@eulerhermes.com

Hamburg, 20.04.2016

## **Betrugswarnung – „Fake President“**

Sehr geehrte Damen und Herren,

mit Euler Hermes als Vertrauensschadenversicherer haben Sie einen starken Partner an Ihrer Seite, wenn es um den Schutz vor Vertrauensschäden geht.

Wir möchten jedoch nicht erst für Sie da sein, wenn der Schaden bereits eingetreten ist. Es liegt uns auch daran, Ihr Unternehmen vor drohenden Schäden zu schützen. Aus diesem Grunde wollen wir Sie vor bestimmten Betrugsszenarien warnen, durch die in letzter Zeit eine Vielzahl von zum Teil beträchtlichen Schäden verursacht wurden.

### **Szenario 1 - Betrug durch Vorspiegelung einer falschen Identität – „Fake President Fraud“**

Bei dieser Betrugsmasche geben sich die Täter als ein Organ des versicherten Unternehmens - meist ein Vorstandsmitglied - aus und bitten per E-Mail oder Fax einen Mitarbeiter, der im Unternehmen für die Bankgeschäfte verantwortlich ist, eine dringende Überweisung auszuführen. Dem Mitarbeiter wird dabei vorgespiegelt, dass es sich um eine höchst geheime und vertrauliche Angelegenheit handelt, von der strategische Weichenstellungen im Unternehmen abhängen. Die Betroffenen, die sich einerseits aufgrund des besonderen Vertrauens durch den Vorstand geschmeichelt fühlen, andererseits aufgrund der angeblichen Wichtigkeit der Transaktion erheblich unter Druck stehen, führen diese Überweisungen meist zügig aus. Fast immer erfolgen die Geldtransfers auf ausländische Konten, vor allem in Asien und Osteuropa. Fliegt der Betrug dann auf, sind die Konten dort meist leergeräumt oder eine Rückholung wird aufgrund des ausländischen Rechtssystems erheblich erschwert.

Häufig werden gezielt Mitarbeiter in ausländischen Niederlassungen des Unternehmens angesprochen. Das erschwert den Mitarbeitern die persönliche Kontaktaufnahme mit den verantwortlichen Organen im Unternehmen, von denen die vermeintlichen Anweisungen kommen.

# Euler Hermes Deutschland

Blatt 2 zum Schreiben vom 20.04.2016

## **Szenario 2 Betrug durch Umleitung von Zahlungsströmen – „Payment Diversion“**

In diesen Fällen geben sich die Betrüger als Geschäftspartner oder Lieferanten des versicherten Unternehmens aus und erreichen durch gefälschte Mitteilungen, dass die Bezahlung für Waren oder erbrachte Dienstleistungen auf abweichende Konten erfolgt. Die Umsetzung dieser Form des Betruges wird ermöglicht durch eine gefälschte Mitteilung an das versicherte Unternehmen, dass sich die bisher vereinbarten Bankverbindungen geändert haben und der Zahlungsverkehr nun über die neue Bankverbindung abgewickelt werden soll.

## **Szenario 3 - Betrug durch Nutzung einer fremden Identität – „Fake Identity Fraud“**

Auch bei diesem Betrugsszenario geben sich die Täter als ein bereits existierender Kunde oder als ein Neukunde des versicherten Unternehmens aus und ordern schriftlich Waren. Mit plausiblen Erklärungen wird dann die Lieferung an eine abweichende Lieferadresse verlangt. Da die Identität einer tatsächlich existierenden Firma genutzt wird, schöpfen die Betrugsoffer zunächst keinen Verdacht. Oft fliegt der Betrug erst dann auf, wenn Zahlungsverzug eintritt und die tatsächlich existierende Firma gemahnt wird. Wird dann die Lieferadresse durch die Polizei überprüft, werden die Geschäftsräume verlassen vorgefunden und die Ware ist selbstverständlich längst weiter verschoben worden.

## **Was können Sie tun?**

- Schaffen Sie klare Prozesse und Zuständigkeiten in Ihrem Unternehmen. Wo irgend möglich, sollte ein Vieraugenprinzip bei allen finanzrelevanten Transaktionen eingeführt werden. Stellen Sie klare Regeln auf, die festlegen, wie bei Ausnahmefällen vorzugehen ist, wenn beispielsweise eine besonders hohe oder dringliche Zahlung veranlasst werden soll.
- Verifizieren Sie die Zahlungsinformation oder die Bestellung per E-Mail. Nach Möglichkeit sollte ein Anruf bei Ihnen bekannten Mitarbeitern oder der Zentrale des angeblichen Kunden erfolgen. Die Telefonnummer sollte dabei nicht aus der E-Mail entnommen werden, sondern beispielsweise aus internen Unternehmensaufzeichnungen oder von der Internetseite der Firma.
- Ebenso sollten bei Änderungen der Bankkontodaten oder abweichenden Zahlungsempfängern die Angaben durch eine sichere Methode wie Brief, Kontobestätigung und Rückruf zwecks Authentizitätsprüfung bestätigt werden.
- Ermuntern Sie Ihre Mitarbeiter bei jeder angeblichen Meldung der Unternehmensleitung, die vom Inhalt, Stil oder Wortlaut unüblich ist oder sogar Fehler enthält, sich an die betreffende Person zu wenden oder zumindest den unmittelbaren Vorgesetzten zu informieren.
- Einbeziehung der Polizei - im Falle eines Angriffs sollten Sie Anzeige erstatten.

# Euler Hermes Deutschland

Blatt 3 zum Schreiben vom 20.04.2016

- **Informieren Sie alle Ihre Angestellten weltweit über dieses Betrugsvorgehen, sensibilisieren Sie sie für diese Gefahr und gestalten Sie entsprechende Verhaltensrichtlinien.** Besonders Mitarbeiter, die in sensiblen Bereichen in den Finanzabteilungen arbeiten, sollten auf die Bedrohung hingewiesen werden.

Dieses Informationsschreiben dient lediglich zur allgemeinen Information und kann nicht zur Begründung eines Deckungsanspruchs herangezogen werden. Der Deckungsumfang ergibt sich aus Ihrem Versicherungsschein, den jeweils vereinbarten Allgemeinen Bedingungen für die Vertrauensschadensversicherung und den gesetzlichen Regelungen des VVG.

Bitte beachten Sie, dass nur unsere AVB VSV Premium – im Rahmen des geltenden Sublimits (Schäden – verursacht durch Dritte) – grundsätzlich Deckungsschutz für die von uns geschilderten Schadenszenarien, insbesondere "FAKE PRESIDENT"- FRAUD, bieten.

Haben Sie noch Fragen? Wenden Sie sich bitte an Ihren Ansprechpartner vor Ort oder sprechen uns direkt an.

Mit besten Grüßen

Kai Olbrich

Rüdiger Kirsch

Euler Hermes Deutschland  
Niederlassung der Euler Hermes SA