Detailinformationen Betrugswarnung „Fake President“: Betrug durch Schein-Geschäftsführer

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.

Die Sensibilisierung Ihrer Mitarbeiter ist für ein Vermeiden solcher Schäden ausschlaggebend. Die Unternehmen, die u.a. ihre Geschäftsführung, Finanzabteilungen, Tochtergesellschaften im In- und Ausland sowie die dortige Buchhaltung eingehend informiert haben, konnten dadurch Betrugsversuche vereiteln.

Wir haben für Sie auf den folgenden Seiten umfangreiche Informationsmaterialien zusammengestellt, die das genaue Vorgehen bei den jeweiligen Betrugsmaschen beschreiben – und was Sie als Unternehmen dagegen tun können. Sie finden diese Materialien auch elektronisch zum Download auf unserer Webseite, sowohl in deutscher als auch in englischer Sprache, um auch die Information von ausländischen Einheiten Ihres Unternehmens zu erleichtern.

Bitte informieren Sie Ihre Mitarbeiter und ggfs. Ihre Tochtergesellschaften über dieses Betrugsvorgehen und leiten Sie die beigefügte Betrugswarnung weiter.

Wir beobachten drei unterschiedliche Betrugsszenarien, bei denen jeweils ein Identitätsdiebstahl zugrunde liegt:

1) „Fake President Fraud“: Durch die Vorspiegelung einer falschen Identität werden Zahlungen auf externe Konten angewiesen.

„Das Schreiben ist absolut vertraulich. Ich habe Sie ausgewählt wegen Ihrer Diskretion und Ihrer hervorragenden Leistungen, um für eine geplante streng vertrauliche Übernahme die damit verbundenen finanziellen Transaktionen auszuführen. Niemand außer Ihnen – auch nicht innerhalb unseres Hauses, ist derzeit über die Planungen informiert.“

So oder ähnlich lautet häufig der Inhalt von E-Mails (oder selten auch Faxen) vom „falschen Chef“. Die Täter hacken sich ins Intranet und spähen dort meist über mehrere Tage Korrespondenzen aus, analysieren Duktus und Umgangsformen und fälschen dann den Mailaccount des Vorstandchefs. „Fake President“ wird diese Masche deshalb auch genannt.

Bei dieser Betrugsmasche geben sich die Täter als ein Organ des versicherten Unternehmens – meist ein Vorstandsmitglied oder Geschäftsführer – 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.

Häufig geht diese E-Mail mit Anweisungen an einen Mitarbeiter in der Buchhaltung in einer Tochtergesellschaft, da die Wahrscheinlichkeit höher ist, dass Mitarbeiter den obersten Chef nicht persönlich kennen. Distanz, Respekt und ein geschmeicheltes Ego erleichtern die Betrugsmasche in der Regel erheblich. Zudem wirft es weniger Fragen auf, wenn er den/die Mitarbeiter/in bittet, ihn weder persönlich noch telefonisch zu kontaktieren oder anzusprechen, nur per E-Mail. Die Begründungen für den E-Mail Verkehr sind teilweise absurd und gehen bis zur „schriftlichen Dokumentation für Aufsichtsbehörden“.

In vielen Fällen wird der Mitarbeiter gebeten, eine mit der Transaktion betraute Anwaltskanzlei zu kontaktieren, um das weitere Vorgehen detailliert zu besprechen. Der falsche Chef liefert die Kontaktdaten in seiner E-Mail mit. Der Kontakt in der angeblichen Kanzlei spricht in der Regel akzentfreies Deutsch und übt häufig erheblichen Druck auf die Mitarbeiter aus, was die strenge Geheimhaltung betrifft.

Die Betroffenen, die sich einerseits aufgrund des besonderen Vertrauens durch den Vorstand geschmeichelt fühlen, anderseits 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.

Neue Variante: Fake IT Security
Zuletzt ist vereinzelt eine neue Variation des Fake President Betrugs aufgetreten. Der Erstkontakt erfolgt wie in den bisher verbreiteten Betrugsfällen per E-Mail. Anschließend ruft jedoch ein „falscher IT Security Mitarbeiter" bei dem betreffenden Mitarbeiter an, um ihm mitzuteilen, dass bei ihm ein Fake President Betrugsversuch unternommen habe, den man aber identifiziert habe. Da man die Täter aber auf frischer Tat ertappen wolle, solle der Mitarbeiter einfach „weiter zum Schein mitspielen" – auch zum Schein die Überweisungen / Finanztransaktionen tätigen. Vorstand und IT Security seien involviert und hätten entsprechende Vorsorgemaßnahmen getroffen, dass die Überweisung nur zum Schein getätigt wird und so abgesichert, dass kein finanzieller Schaden entstehen könne.

Da der Anrufe ein Betrüger ist, ist das Geld natürlich weg. Der weitere Verlauf der Betrugsfälle ist wie bei der klassischen Fake President Variante.

2) „Payment Diversion Fraud": Betrug durch Umleitung von Zahlungsströmen, beispielsweise durch Vorspiegelung von angeblich neuen Kontodaten des Lieferanten.

In diesen Fällen hacken sich die Betrüger in die Server von Geschäftspartnern. Sie geben sich als Geschäftspartner oder Lieferant des versicherten Unternehmens aus und erreichen durch gefälschte E-Mail Mitteilungen, dass die Bezahlung für Waren oder erbrachte Dienstleistungen auf abweichende Konten erfolgt.

Die Umsetzung dieser Form des Betrugs wird ermöglicht durch ein gefälschtes Schreiben an das versicherte Unternehmen, dass sich die bisher vereinbarten Bankverbindungen geändert haben und der Zahlungsverkehr nun über die neue Bankverbindung abgewickelt werden soll. In diesem Schreiben sind auch Kontaktdaten angegeben und die Betrüger setzen darauf, dass der Mitarbeiter in der Buchhaltung zur Überprüfung der Echtheit der Mitteilung die dort aufgeführten gefälschten Telefonnummern nutzt.

Wird diese Änderung nicht mit den im firmeneigenen System registrierten Kontaktdaten telefonisch überprüft, ist das Geld in der Regel binnen weniger Stunden weg. Der Betrug fällt erst dann auf, wenn sich der Lieferant mit Mahnungen meldet, dass die Rechnung nicht fristgerecht bezahlt wurde.

3) „Fake Identity Fraud": Umleitung von Warenströmen an eine andere vermeintlich andere Lieferadresse des Kunden.

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 – ebenfalls per E-Mail nach vorherigem Identitätsdiebstahl.

Da die Identität einer tatsächlich existierenden Firma genutzt wird, schöpfen die Betrugsopfer 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, um solche Betrugsszenarien zu verhindern?

- **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 – auch alle Mitarbeiter in den Tochtergesellschaften im In- und Ausland, die mit Zahlungsströmen zu tun haben. Sie sind besonders häufig Ziel der Betrugsversuche. Das Informationsmaterial steht elektronisch auf Deutsch und Englisch zur Verfügung.

- **Automatische Abwesenheitsnotizen der Geschäftsführung, Führungskräften oder Mitarbeitern in der Finanzbuchhaltung liefern Außenstehenden oft viele Informationen**, beispielsweise wie lange der Geschäftsführer außer Haus, auf Dienstreise oder im Urlaub ist. Diese Informationen erleichtern einen Betrugsversuch, weil der echte Chef in seiner Abwesenheit in den seltensten Fällen angesprochen werden kann. Überdenken Sie daher die Nutzung automatischer Abwesenheitsnotizen bei Geschäftsführung und in der Finanzbuchhaltung.

- **Eine vollständige Signatur in allen E-Mails erschwert den Betrugsversuch**. E-Mails ohne Signatur sind leichter zu imitieren, da die Fehlerquelle wesentlich geringer ist. Name, Position, Unternehmen, Kontaktdaten inklusive Durchwahlen sowie relevante Daten aus dem Handelsregister sind wesentlich schwerer zu fälschen und erleichtert es Ihren Mitarbeitern, gefälschte Absender leichter zu identifizieren.

- **Überprüfen Sie eingehende E-Mails sorgfältig auf Ihre Richtigkeit** – sowohl den Anzeigenamen vorne als auch die folgende E-Mail-Adresse selbst. Auch wenn vermeintlich der Name des Chefs erscheint, kann die zugrunde liegende Adresse zu einem Account außerhalb des Unternehmens führen. Mit einem Klick auf den Namen kann das geprüft werden. Oft unterscheiden sich diese nur durch einen Buchstaben (ss statt s oder g statt q), so dass sie auf den ersten Blick nicht immer gleich erkennbar sind.

- **Schaffen Sie klare Prozesse und Zuständigkeiten in Ihrem Unternehmen**. Wo irgend möglich, sollte ein Vieraugenprinzip bei allen finanzerheblichen 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.

- **Compliance Schulungen und entsprechende Online-Trainings** oder Webinare helfen, die Mitarbeiter für die konzernweiten internen Prozesse zu sensibilisieren und ein mögliches Fehlverhalten frühzeitig zu erkennen.

- **Verifizieren Sie die Zahlungsinformation oder die Bestellung per Telefon**. Nach Möglichkeit sollte ein Anruf bei Ihnen bekannten Mitarbeitern oder der Zentrale des angeblichen Kunden erfolgen. Die Telefonnummer sollte dabei nicht aus der möglicherweise gefälschten 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.

- **Überprüfen Sie eingehende E-Mails auf Anrede, Stil und mögliche Schreibfehler**. 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. Siezt ein Geschäftsleiter seine Mitarbeiter zum Beispiel und spricht ihn in der E-Mail plötzlich mit Du an oder umgekehrt, sollten Mitarbeiter hellhörig werden.

- **Einbeziehung der Polizei** - im Falle eines Angriffs sollten Sie Anzeige erstatten.

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.

Weitere Informationen finden Sie auch auf unserer Webseite http://www.eh-cybercrime.de/.

Mit besten Grüßen

Björn Albert

Rüdiger Kirsch

Euler Hermes Deutschland
Niederlassung der Euler Hermes SA