



Erste Hilfe bei Überweisungsbetrug

Überweisungsbetrug, auch „CEO-Betrug“ genannt, ist eine Methode, bei der Betrüger durch das Versenden von betrügerischen E-Mails Mitarbeiter eines Unternehmens dazu bringen, Überweisungen auf Bankkonten von Betrügern zu tätigen. Von dort wird das Geld entweder auf weitere Konten unterverteilt oder bar abgehoben. Die Zielgruppe für solche Betrugsversuche ist sehr gemischt, es kann kleinere familiengeführte Unternehmen genauso treffen wie Mittelständler oder große, internationale Unternehmen.

Die Empfängerkonten der Betrüger können überall auf der Erde liegen, jedoch ist eine Häufung von Fällen festzustellen, in denen Geld an eine Bank in Hongkong, Festlandchina oder anderen Ländern Südostasiens überwiesen werden soll.

2020 lag der Gesamtschaden bei ca. 43 Milliarden USD, woran erkennbar wird, dass es sich hierbei um ein globales Problem handelt, welches von jedem Unternehmen ernst genommen werden sollte.

Modus Operandi

Die Betrüger hacken sich in der Regel in das E-Mail-System des betroffenen Unternehmens ein und beobachten dessen E-Mail-Verkehr über einen längeren Zeitraum, teilweise mehrere Monate. Dabei analysieren die Betrüger den Schreibstil der jeweiligen Mitarbeiter und bringen zum Teil auch persönliche Informationen (Urlaubspläne, Familienhintergrund, etc.) in Erfahrung, um ihre E-Mails möglichst authentisch zu verfassen.

Sind genug Informationen gesammelt, erfolgt der Angriff. Dabei erhält der für die Ausführung von Überweisungen zuständige Mitarbeiter eine E-Mail. Diese scheint meist vom Geschäftsführer selbst (daher CEO-Betrug) oder einem wichtigen Geschäftspartner zu kommen, der zur Anweisung von Zahlungen ermächtigt ist. Die E-Mail-Adressen sind oft identisch mit den E-Mail-Adressen der Geschäftsführer oder aber nur minimal verändert. Daher lässt sich anhand der E-Mail-Adresse nicht gleich Verdacht schöpfen. Allerdings haben die E-Mails andere Merkmale, die einen aufmerksamen Leser warnen können:

- Die E-Mail ist als „streng vertraulich“ gekennzeichnet und der Empfänger wird gebeten, über den Inhalt Stillschweigen zu bewahren.
- Die Überweisung muss sehr kurzfristig erfolgen und in der Regel für ein im Ausland befindliches Investitionsprojekt.
- Der Betrag soll sofort per Eilüberweisung angewiesen werden und dem vermeintlichen CEO/Geschäftspartner umgehend der Überweisungsbeleg zugeleitet werden.
- Der Verfasser bittet darum, ihn nicht telefonisch, sondern ausschließlich per E-Mail zu kontaktieren, zum Beispiel weil er zurzeit im Urlaub oder auf Dienstreise befindlich ist. In vielen Fällen entspricht dies sogar den Tatsachen, da die Betrüger über die ausgespähten E-Mails vorab Informationen sammeln.

In einer abgewandelten Form des CEO-Betrugs wird über längere Zeit die Kommunikation eines Unternehmens mit dessen Lieferanten in Hongkong oder Festlandchina verfolgt. Die Betrüger versenden dann eine E-Mail, in der darum gebeten wird, Geld für ein laufendes Projekt nicht auf das bereits bekannte Konto zu überweisen. Stattdessen soll auf ein anderes Konto überwiesen werden, da das Unternehmen die Bank gewechselt habe, oder aber das bekannte Konto „wegen Audits geschlossen“ sei.

Ist das Geld auf dem Konto der Betrüger eingegangen, kommt es häufig vor, dass in engem zeitlichem Zusammenhang weitere Überweisungsanforderungen eingehen. Diese betreffen zum Beispiel „weitere Projekttranchen“ oder Ersatzteile für eine vermeintlich erworbene Maschine.

Erste Hilfe bei CEO-Betrug

Ist ein Unternehmen Opfer des CEO-Betrugs geworden, zählt oft jede Sekunde, um das Geld, oder zumindest einen Teil davon, zurückzuerhalten. Internationale Überweisungen werden heute in der Regel über das SWIFT-System abgewickelt. Wann und wie schnell das System den Betrag überweist, hängt von den beteiligten Banken ab.

Es muss dringend verhindert werden, dass das Geld dem Betrügerkonto gutgeschrieben wird. Das heißt, die Überweisung muss gestoppt werden, solange das Geld sich noch im Transfer befindet. Eine Überweisung von den USA oder Europa nach Asien kann entweder sehr schnell gehen, wenn die Absender- und Empfängerbank direkte Kontakte unterhalten. Die Überweisung kann aber auch bis zu ein oder zwei Tage in Anspruch nehmen, wenn das Geld über Transferbanken fließt, was oft bei Zahlungen nach China der Fall ist. In dieser Spanne muss gehandelt werden, denn wenn das Geld gutgeschrieben wurde, sinken die Chancen sehr schnell, es wiederzuerlangen.

Folgende Schritte sollten daher umgehend eingeleitet werden:

1. Informieren Sie Ihre eigene Bank.

Es muss unverzüglich die eigene Bank über die betrügerische Überweisung informiert werden, mit der Bitte, die Überweisung zu stoppen. Dies kann möglich sein, solange das Geld noch nicht vom Konto abgebucht wurde oder noch auf einem Zwischenkonto der Bank vorhanden ist.

Sobald das Geld allerdings die eigene Bank verlassen hat und in den internationalen Zahlungsstrom eingeflossen ist, kann die Überweisung nicht mehr einseitig durch die Hausbank gestoppt werden.

2. Bitten Sie Ihre Bank, eine SWIFT-Nachricht an die Empfängerbank zu versenden.

Hat das Geld bereits die Konten der eigenen Bank verlassen, so ist die eigene Bank umgehend zu instruieren, eine SWIFT-Nachricht an die Empfängerbank zu senden. Diese sollte den Hinweis enthalten, dass es sich um eine betrügerische Überweisung handelt und die dringende Bitte, das Geld nicht auf dem Empfängerkonto gutzuschreiben, sondern wieder zurück zu überweisen.

Dies ist solange möglich, wie das Geld noch nicht auf dem Empfängerkonto gutgeschrieben wurde, also noch auf einem Zwischenkonto der Empfängerbank vorhanden ist. Wurde das Geld allerdings bereits dem Konto der Betrüger gutgeschrieben, so sind der Empfängerbank in der Regel die Hände gebunden. Die Vertragsbeziehungen der Bank mit ihren Kunden gestatten es in der Regel nicht, Geld vom Kundenkonto wieder abzubuchen, wenn nicht eindeutige Hinweise auf einen Betrug vorliegen. Eine einfache SWIFT-Nachricht ist nicht als eindeutiger Hinweis anerkannt.

Innerhalb weniger Stunden wird die Hausbank eine Antwort per SWIFT erhalten, in der mitgeteilt wird, ob der Betrag sichergestellt werden konnte oder ob das Geld bereits dem Empfängerkonto gutgeschrieben wurde.

3. Zeigen Sie den Betrug bei der deutschen Polizei an.

Nachdem die Empfängerbank informiert wurde, sollte bei der heimischen Polizei eine Anzeige wegen Betrug gegen Unbekannt erstattet werden. Bei Fällen mit Auslandsbezug besteht leider wenig Aussicht, dass die Ermittlung konkrete Ergebnisse bringt. Oft möchte aber die lokale Polizei im Empfängerland (siehe unten) eine solche Anzeige vorgelegt bekommen.

4. Zeigen Sie den Betrug bei der Hongkonger Polizei an.

Konnte das Geld bis jetzt nicht sichergestellt werden, so ist eine Strafanzeige bei der lokalen Polizei notwendig. In Hongkong kann die Strafanzeige in englischer Sprache per E-Mail, Fax oder online eingereicht werden. Zuständig ist die „**Joint Financial Intelligence Unit**“ (JFIU) der Hongkonger Polizei.

Die Kontaktdaten sind wie folgt:

Tel.: +852 2866 3366
Fax: +852 2529 4013
E-Mail: jfiu@police.gov.hk

Weiterhin besteht die Möglichkeit, die Anzeige direkt online zu erstatten:

<https://www.erc.police.gov.hk/cmisercc/CCC/PolicePublicPage?language=en>

Davon sollte Gebrauch gemacht werden, da dies der schnellste und einfachste Weg ist, den Fall an die lokale Polizei zu übermitteln.

Wird der Report über einen dieser Wege eingereicht, so ist unbedingt zu raten, nach kurzer Zeit telefonisch nachzuhaken, dass der Report empfangen wurde und bereits bearbeitet wird.

Da die JFIU derzeit aufgrund der Vielzahl von Online-Betrüger überlastet ist, ist es ratsam, eine Person vor Ort zu kontaktieren, die die Strafanzeige persönlich bei der Polizei aufgibt. Dies verleiht dem Fall mehr Nachdruck und vereinfacht es, in den nächsten Tagen die Polizei aufzusuchen und nach dem Stand der Dinge zu fragen.

Als Kontaktperson vor Ort bietet sich vor allem ein erfahrener Anwalt an, der nicht nur die Strafanzeige einleiten kann, sondern auch später bei der Wiedererlangung des Geldes behilflich ist. Sinn und Zweck der Strafanzeige ist, dass die Polizei der Empfängerbank einen „Letter of No Consent“ zustellt, mit welchem die Bank die Anweisung erteilt, das Konto bis auf weiteres einzufrieren. Dies wird allerdings erst geschehen, wenn die Bank der Polizei den derzeitigen Kontostand mitteilt. Sollte das Geld auf dem Konto nicht mehr vorhanden sein bzw. nur noch ein geringer Restbetrag (unter 100.000 Hongkong-Dollar, das sind ca. 11.000 Euro), wird die Polizei den Fall schließen.

Alternativ kann auch beim Hongkonger Gericht durch einen Anwalt der Erlass einer einstweiligen Anordnung auf Einfrieren des Kontos („Mareva Injunction“) gestellt werden. Ein solcher Antrag ist allerdings wesentlich teurer als eine Anzeige bei der Bank, dauert länger und hat lediglich denselben Erfolg.

Weiterer Verfahrensablauf

Wurde das Konto mit ausreichend Geld erfolgreich eingefroren, so ist ein lokaler Anwalt zu beauftragen, eine Klage wegen ungerechtfertigter Bereicherung gegen den Kontoinhaber einzureichen. Nachdem die Klage dem Beklagten zugestellt wurde, hat dieser 14 Tage Zeit, seine Klagebereitschaft anzuzeigen. In der Regel geschieht dies nicht, da die Betrüger kein Interesse an einer Gerichtsverhandlung haben. Nach diesen 14 Tagen wird ein Versäumnisurteil ergehen, mit welchem in das Konto vollstreckt werden kann und die Bank wird dann das Geld zurück überweisen.

Ab Einreichung der Klage bis zum Erhalt des Urteils vergehen in der Regel ca. 5 bis 6 Monate und die Anwaltskosten liegen in der Regel bei 4.000 bis 6.000 Euro. Nach Erhalt des Urteils ist dieses in das (eingefrorene) Bankkonto zu vollstrecken („Garnishee Proceedings“), wozu mit weiteren ca. 3 bis 4 Monaten und zusätzlichen Kosten von ca. 3.000 bis 4.000 Euro zu rechnen ist.

Eine Erstattung der Prozesskosten ist in der Regel nur in einem eher nominellen Rahmen von bis zu etwa 500 Euro möglich, so dass der Großteil der Anwalts- und Gerichtskosten vom Geschädigten zu tragen ist.

Teilweise kommt es allerdings vor, dass sich der Kontoinhaber vor Gericht tatsächlich verteidigen möchte, da er der Ansicht ist, er hätte Anspruch auf das Geld oder ihm stünden andere Verteidigungsmittel zur Verfügung. In einem solchen Fall geht das Verfahren in ein ordentliches Gerichtsverfahren über, welches in der Regel 20 bis 25 Monate dauert und Kosten von ca. 30.000 bis 50.000 Euro auslöst. Von daher ist dieser Schritt genau zu überlegen, da auch zeitintensive Reisen nach Hongkong zur Zeugenaussage notwendig werden.

Stand: Juli 2021

Dieses Merkblatt wurde vom Deutsch-Hongkonger Rechtsanwalt Stefan Schmierer verfasst.

E-Mail: sschmierer@rs-lawyer.com.hk <mailto:sschmierer@rs-lawyers.com.hk>

Website: <https://www.rs-lawyers.com.hk/>

Die Anwaltsliste des Generalkonsulats finden Sie unter:

<https://hongkong.diplo.de/hk-de/service/-/1439070>