CEO-Betrug: Falsche „Chefs" kontaktieren Mitarbeiter der Finanz-Abteilung einer Firma telefonisch und per E-Mail und veranlassen sie zur Überweisung größerer Summen ins Ausland.

Hohe Verluste

Durch Betrüger, die sich als „Chefs" ausgeben, wurden Dutzende Firmen geschädigt. In Österreich enstanden durch den „CEO-Betrug" bisher über 90 Millionen Euro an Schaden.

Eine echt aussehende E-Mail eines angeblich Vorgesetzten und vertrauenswürdige Anrufe eines vermeintlichen Rechtsanwalts machten es möglich, dass die Finanzabteilung einer oberösterreichischen Firma etwa 54 Millionen Euro auf ausländische Konten überwies. Erst bei einer Cashflow-Kontrolle wurde erkannt, dass größere Summen abgeflossen waren. Im Dezember 2015 erhielt die Buchhalterin des Unternehmens die erste gefälschte E-Mail, in der der „Vorstandsvorsitzende" auf die geplante Übernahme eines Unternehmens hinwies. Danach erfolgten zwei Telefonate eines vermeintlichen Rechtsanwalts. Daraufhin wurde die erste Summe, etwa 1,5 Millionen Euro, überwiesen.

Vom Dezember 2015 bis Jänner 2016 wurden in 17 Überweisungen 54 Millionen Euro an verschiedene Konten ausländischer Banken überwiesen. Die letzte Überweisung von ca. 1,5 Millionen wurde retourniert, da die Buchhalterin den BIC-Code falsch eingetragen hatte. Acht Millionen Euro sollen auf chinesischen Konten eingefroren sein. An das Geld heranzukommen ist aber schwierig, weil es mit China keine Rechtshilfeabkommen gibt.

„Österreichische Firmen werden vermehrt zur Zielscheibe solcher Angriffe", sagt Mag. Claus Kahn, Leiter des Büros 7.1 (Betrug, Fälschung und Wirtschaftskriminalität) im Bundeskriminalamt. Über 50 derartige Fälle von CEO-Betrug registrierte die Polizei in Österreich bisher. Der Schaden beträgt über 90 Millionen Euro. „Die meisten Fälle waren Vorbereitungsbehandlungen und Versuche", betont Kahn. In drei Fällen gelang es den Tätern, Firmen massiv zu schädigen. Die Dunkelziffer schätzt der Wirtschaftskriminalist als hoch ein. Viele Unternehmer würden aus Scham und Angst vor Reputationsverlust schweigen. Nur börsennotierte Firmen müssen den Betrug offenlegen.

„Absolute Diskretion". Die Masche der Betrüger ist einfach: Sie geben sich als Geschäftsführer (Chief Executive Officer – CEO), Vorstand oder leitender Mitarbeiter eines Konzernes aus und kontaktieren Mitarbeiter der Finanzabteilung dieses Unternehmens. Die erste Kontaktaufnahme erfolgt meist per Telefon. „In der Regel ruft zuerst ein Betrüger an, der sich als Anwalt ausgibt und dem Mitarbeiter eine Finanztransaktion ankündigt", berichtet Betrugsermittler Horst Hakala vom Bundeskriminalamt. Der „Rechtsanwalt" macht nur kryptische Anmerkungen und weist den Mitarbeiter darauf hin, dass sich der „Finanzvorstand" persönlich bei ihm melden werde, denn die Sache sei sehr vertraulich. Tatsächlich wendet sich der „Finanzvorstand" kurze Zeit später persönlich per E-Mal an den Mitarbeiter. Die Mails enthalten die korrekten Namen der berechtigten Geschäftsführer oder Vorstandsmitglieder des Unternehmens. In den Mails wird nochmals darauf hingewiesen, dass die Sache vertraulich sei und dass nur auf diese, von den Tätern manipulierte E-Mail-Adresse geantwortet werden soll. Dadurch wollen die Betrüger sicherstellen, dass der Angestellte nicht die (richtige) Mail-Adresse des Vorgesetzten eingibt. Dies wird mit dem Umstand begründet, dass es gegenüber der Finanzmarktaufsicht eine Dokumentationspflicht gebe. „Wesentliche Merkmale dieser Betrugsform sind der Hinweis auf die Geheimhaltung des Projektes und die direkte Kommunikation zwischen der Geschäftsleitung und dem Mitarbeiter der Finanzabteilung", erklärt Claus Kahn.

Die E-Mail-Nachricht des vermeintlichen CEOs lautet zum Beispiel: „Wir bereiten die Übernahme eines Unternehmens vor, dies betrifft insbesondere die finanzielle Transaktion. Die Angelegenheit muss absolut vertraulich behandelt werden. Niemand sonst, auch nicht innerhalb unseres Hauses, wird zur Zeit darüber informiert. Aufgrund Ihrer Diskretion und bisher einwandfreien Arbeit in unserem Unternehmen möchte ich Ihnen die Verantwortung für dieses Projekt übertragen."

„Um die Sache unverdächtig erscheinen zu lassen, ersuchen die Betrüger den Mitarbeiter per E-Mail bekannt zu geben, wie die finanzielle Bedeckung aussieht", erläutert Claus Kahn. Ein halbe Stunde später erhält der

FOTOS: FOTOLIA/DESSAUER, FOTOLIA/GAJ RUDOLF

CEO-Betrugsfälle: Bisher waren über 50 Firmen in Österreich betroffen, der Schaden betrug über 90 Millionen Euro.

Buchhalter erneut eine E-Mail des „Finanzvorstands“. Er fragt den Buchhalter, ob es mit heutigem Datum möglich sei, eine Zahlung von knapp einer Million Euro anzuweisen, ohne Fragen aufzuwerfen. Die Zahlungsanweisung wird als PDF übermittelt. Die Empfängerfirma ist eine Scheinfirma. Die Unterschrift des Zeichnungsberechtigten haben die Täter etwa von einem Jahresabschlussbericht des Unternehmens kopiert und eingefügt.

In einem Fall erfolgten innerhalb von sechs Tagen weitere E-Mails und Telefonate an bzw. mit dem Buchhalter. Es gab neun Zahlungsanweisungen nach Asien mit mehreren Millionen Euros. Der Schaden der Firma betrug etwa 20 Millionen Euro. „Die Beträge sind mit manuellen Zahlungsanweisungen überwiesen worden“, erklärt ein Betrugsermittler vom Landeskriminalamt Salzburg, der in vier Betrugsfällen in Salzburg ermittelte. Die Zahlungsanweisungen sind bei jeder Bank erhältlich, es sind keine TAN-Codes. sondern es ist nur die Unterschrift des Zeichnungsberechtigten erforderlich.

Das Geld wird über Zwischenstufen auf ausländische Konten überwiesen, vorwiegend nach Asien. Die Betrüger beheben das Geld so schnell wie möglich. Sie verwendeten eine Anonymisierungs-Software, mit der sie ihre IP-Adresse und Ihren Standort simulieren können. Sie generierten E-Mail-Adressen unter anderem mit yopmail.com. Das ist ein Dienst, der es ermöglicht, eine kostenfreie, temporäre E-Mail-Adresse zu erstellen, die Nachrichten nur acht Tage speichert. Dennoch passieren Fehler. In einer E-Mail wurden in der „Von-Zeile“ zwei Absender angeführt. Einer davon hieß: *kopie.bafin@berlin.com*. *BaFin* ist die Bundesanstalt für Finanzdienstleistungsaufsicht in Deutschland. In Österreich ist es die *Finanzmarktaufsicht (FMA)*. „Die Täter setzen den Angestellten unter Druck, indem sie die Sache als vertraulich und dringend einstufen“, sagt Horst Hakala. „Da fallen einem Mitarbeiter solche Fehler oft nicht auf.“

Ein Maschinenbauunternehmen in Bayern wäre 2015 beinahe um elf Millionen Euro betrogen worden. Ein Mitarbeiter des international tätigen Unternehmens erhielt eine streng vertrauliche E-Mail vom vermeintlichen Geschäftsführer des Gesamtunternehmens. In der Mail hieß es, dass es um Geheimverhandlungen gehe bezüglich der Übernahme eines weiteren Tochterunternehmens. Der Prokurist wurde aufgefordert, eine Million Euro als Anzahlung zu überweisen. Weitere Details würde er von einem Anwalt erhalten, der mit der Angelegenheit betraut sei. Der Anwalt meldete sich bei dem Prokuristen per E-Mail. Er erklärte ihm, dass die Sache diskret abgewickelt werden müsse, um die Firmenübernahme nicht zu gefährden. Er übermittelte dem Angestellten die Transaktionsdaten. Er wurde aufgefordert, Stillschweigen zu bewahren und sein privates E-Mail-Konto für die weitere Kommunikation zu verwenden.

Die bayerischen Ermittler gehen davon aus, dass der angebliche CEO und der Anwalt ein und dieselbe Person waren. „Da der Täter auf Grund seines Auftretens als Geschäftsführer erheblichen Druck auf den Mitarbeiter ausübte und der Sachverhalt auf Grund der aktuellen Unternehmenssituation plausibel erschien, gab der Mitarbeiter die Zahlung frei“, teilte die Bayerische Polizei am 17. August 2015 mit. Ein weiterer Versuch der Kriminellen, eine Überweisung von zehn Millionen Euro zu erwirken, weckte das Misstrauen des Proku-

Foto: Fotolia/Lavizzara

CEO-Betrug: Die ergaunerten Gelder gelangen über Zwischenstufen nach Asien.

risten. Die Transaktion konnte in letzter Minute gestoppt werden.

Social Engineering. Die Täter spionieren die Unternehmen vorher aus. „Sie wissen, wie die Firma organisiert ist, wer wofür zuständig ist, welche Aufträge es gibt, wer die Geschäftspartner sind, ob zum Beispiel eine Firmenübernahme im Ausland bevorsteht“, erläutert Claus Kahn. Die Betrüger informieren sich über Firmenwebseiten oder soziale Netzwerke über das Unternehmen und über Mitarbeiter. Sie finden heraus, in welcher Sprache im Unternehmen kommuniziert wird, verschaffen sich Zugang zu den E-Mail-Konten der Mitarbeiter und suchen in E-Mails Informationen über Geschäftspartner. Sie nehmen mit der Firma telefonisch Kontakt auf und versuchen, Details über die Firmenstruktur zu erfahren, indem sie vorgeben, ein ausländischer Geschäftspartner zu sein. Auch die Abwesenheitsinformation einer Mail kann den Betrügern Details verraten; etwa wann und wo ein leitender Mitarbeiter auf Dienstreise ist und wie die E-Mail-Signatur des Unternehmens aussieht.

Geld retour. Ein Mitarbeiter der Finanzabteilung einer Firma in Schweden bemerkte, dass Betrüger vermutlich mit der CEO-Fraud-Masche versuchten, eine Geldüberweisung auf ein Konto einer Bankfiliale in Graz zu erwirken. Der Schwede verständigte die Staatsanwaltschaft in Graz. Bei der Überprüfung des Kontos fiel den Betrugsermittlern des Landeskriminalamts Steiermark auf, dass eine größere Summe einer Firma aus Dänemark über dieses Konto auf eine Bank nach China transferiert worden war.

Die Kriminalpolizei ermittelte in sechs Fällen in der Steiermark wegen des Verdachts des CEO-Betrugs. In drei Fällen blieb es beim Versuch und in drei Fällen gelang es den Betrügern, die Überweisung größerer Summen zu veranlassen. Das überwiesene Geld konnte wiedererlangt werden. Wenn Polizei, Staatsanwaltschaft und Geschädigte rasch reagieren, ist eine Sicherstellung des Geldes innerhalb einer bestimmten Frist möglich. Für die Ermittler ist es wichtig, dass sie von einer Anzeige schnell Kenntnis erlangen, die in der Regel in einer Polizeiinspektion erstattet wird.

Hohe Verluste. Die ersten CEO-Fraud-Delikte wurden vor etwa zehn Jahren registriert. Europäische Firmen sind seit 2013 im Fokus der Betrüger. In den vergangenen zwei Jahren betrug der Schaden durch CEO-Betrug laut Europol weltweit 1,7 Milliarden Dollar. In Frankreich wurden seit 2010 bekanntermaßen 1.000 Unternehmen geschädigt, der Schaden beträgt über 400 Millionen Euro. In Deutschland waren es 80 Fälle mit einem Schaden von 60 Millionen Euro und in Luxemburg 95 Fälle mit 33 Millionen Euro Schaden. In Österreich sprechen die Ermittler momentan von einer Welle an CEO-Betrugsfällen mit bisher über 90 Millionen Euro Schaden. Die Täter konnten bisher kaum identifiziert werden, sie agieren vom Ausland aus. Die Polizei setzt auf Prävention. An Banken und an die Wirtschaftskammer Österreich ergingen Warnhinweise.

Europol hat aufgrund der Zunahme der Zahl an Fällen von „CEO-Fraud“ den Focal Point „Apate“ eingerichtet. Apate ist der Name eines griechischen Dämons des Betrugs und der Täuschung. Auf Latein heißt er Fraus. Noch vor dem Sommer plant Europol in Wien eine Tagung. Vertreter des Bundeskriminalamts und von Strafverfolgungsbehörden aus 16 europäischen Staaten werden bei der Tagung Maßnahmen gegen den „CEO-Betrug“ erörtern.

Siegbert Lattacher

CEO-FRAUD

Präventionstipps

- Erhöhte Aufmerksamkeit bei E-Mails, in denen die Überweisung hoher Summen gefordert wird.
- Zahlungsanweisungen per E-Mail hinterfragen, auch wenn sie über das interne Firmennetz versendet werden.
- Überprüfen, ob der im Feld „Empfänger“ angezeigte Name auch zu der „dahinter“ befindlichen Mail-Adresse gehört. Bei vielen E-Mail-Programmen werden Name und Adresse angezeigt, wenn man mit dem Mauszeiger über den angezeigten Namen fährt.
- Form und Schreibweise in solchen Anweisungen beachten: Schlechte Übersetzungen und Rechtschreibfehler sind ein Indiz für Betrugsfälle.
- Wer bereits eine Überweisung veranlasst hat, soll mit der Bank die Möglichkeit einer Rückbuchung erörtern.
- Klare, transparente Regeln im Unternehmen, Mitarbeitersensibilisierung.
- Strikte Einhaltung eines Vier-Augen-Prinzips bei Geldzahlungen.
- Rasche Mitarbeiterinformation bei verdächtigen E-Mails oder Anrufen.
- Festlegen von Höchstgrenzen für Überweisungen.
- Festlegen von Vorgehensweisen für Entscheidungen (z. B. Geschäftspartner ändert seine Kontonummer).
- Wer geschädigt wird, sollte umgehend Anzeige in einer Polizeiinspektion erstatten.

FOTO: FOTOLIA/CHUNKING