

INFORMIEREN. AGIEREN. VORBEUGEN.



[Vorsicht vor „Planenschlitzern“ >](#)  
[< Das vernetzte Auto](#)

## CEO-Fraud auf dem Vormarsch

### Falsche Chefs erschleichen hohe Geldsummen



Per Telefon oder E-Mail melden sich die Betrüger bei ihren potenziellen Opfern

© Polizei Rheinland-Pfalz

Seit 2014 beobachtet man in Deutschland ein neuartiges, speziell gegen Unternehmen gerichtetes Betrugsphänomen. Professionell agierende Täter nutzen gezielt die Abwesenheit der Geschäftsführung aus und veranlassen mit gefälschten E-Mails und Anrufen mit vorgetäuschten Legenden autorisierte Mitarbeiter der Buchführungs- und Finanzabteilungen dazu, hohe Geldbeträge auf vorgegebene Zielkonten im Ausland zu überweisen. Das bereits aus dem europäischen Ausland bekannte Phänomen wird als „CEO-Fraud“, „Business E-Mail Compromise“, „Geschäftsführer-Schwindel“ oder „digitaler Enkeltrick“ bezeichnet und ist ein Teilphänomen des Betruges mittels „Social Engineering“ – eine Methode, um durch Manipulation an Informationen zu gelangen.

### Fälle in Deutschland nehmen zu

In den letzten Monaten wurden der **Polizei** vermehrt Fälle der Betrugsmasche gemeldet – unter anderem in NRW, Bayern und Rheinland-Pfalz. So werden etwa bei der Kripo in Trier und Wittlich derzeit mehrere Ermittlungsverfahren geführt, in denen Betrüger meist größere Unternehmen um hohe Geldbeträge gebracht haben. Bei einem Trierer Unternehmen nahm im April 2017 ein bisher unbekannter Täter sowohl per E-Mail als auch telefonisch Kontakt zu einem Mitarbeiter der Buchhaltung auf und gab sich als Geschäftsführer des Unternehmens aus. Er forderte den Mitarbeiter zu einer dringenden Überweisung einer hohen sechsstelligen Summe auf ein ausländisches Bankkonto auf. Die Überweisung sei geheim und müsse sehr schnell und unauffällig durchgeführt werden. Um dieser Anweisung Nachdruck zu verleihen,

meldete sich telefonisch auch ein angeblicher Rechtsanwalt und übte zusätzlichen Druck auf den Mitarbeiter aus. Der überwies das Geld schließlich auf das genannte Konto. Glücklicherweise konnte die Überweisung noch so rechtzeitig gestoppt werden, dass in diesem Fall kein finanzieller Schaden entstand. Insgesamt sind beim **Polizeipräsidium** Trier derzeit sieben solcher Ermittlungsverfahren bekannt. In den meisten Fällen erkannten die Mitarbeiter jedoch die Betrugsabsicht oder die Bank stoppte die Überweisung. Lediglich in einem Fall waren die Täter erfolgreich.

## Täter gehen strategisch vor

Bei den Tätern handelt es sich um professionell agierende Betrüger, die bei der Tatausführung die Rolle einer Autoritäts- bzw. Vertrauensperson einnehmen und somit das **Opfer** steuern. So wird zum Beispiel mitgeteilt, dass ein wichtiges Geschäftsvorhaben vertraulich behandelt werden und in der Umsetzung schnell ablaufen müsse. Sie wirken authentisch und lassen Aufträge zur Durchführung von Überweisungen völlig plausibel und nachfragefrei erscheinen. Hierzu versenden die Täter in der Regel E-Mails mit täuschend ähnlichen oder gefälschten Absenderadressen sowie Telefonnummern und lassen so den Vorgesetzten als vermeintlichen Absender erscheinen. In diesen E-Mails werden Insiderinformationen eines streng geheimen Firmenkaufs oder einer Firmenübernahme vorgetäuscht. In einigen Fällen erklären die „Chefs“ in einer Besprechung unabkömmlich und telefonisch nicht erreichbar zu sein.

## Diese Anhaltspunkte sollten stutzig machen

Ein Mitarbeiter eines Unternehmens sollte hellhörig werden, wenn er vom vermeintlichen CEO Zahlungsaufträge aufgrund einer angeblich „streng geheimen“ Firmenakquisition erhält und dabei vielleicht noch folgende Vorgehensweisen festgestellt werden:

- ▶ Personen mit Handlungsberechtigung werden gezielt angesprochen
- ▶ Vertrauensbeweis wird gefordert
- ▶ Absender verleiht besonderen Nachdruck / Weisung „höchste Geheimhaltungsstufe“
- ▶ Rückfragen werden nicht zugelassen
- ▶ Der Kontakt erfolgt via Telefon/Fax und E-Mail (leicht zu fälschen, zu verschleiern, zu hacken)



Mitarbeiter sollten im Umgang mit E-Mails, in denen es um Zahlungsanweisungen geht, besonders aufmerksam sein

© Antonioguilem, fotolia

Neben erhöhter Aufmerksamkeit im Umgang mit E-Mails, in denen es um Zahlungsanweisungen von zum Teil sehr hohen Summen geht, helfen klare, transparente Regeln im Unternehmen. In den meisten Fällen schützt schon der Blick auf die „Reply-to“-Adresse in der E-Mail. Diese stimmt in der Regel nicht mit der richtigen Adresse des Geschäftsführers oder des die Zahlung veranlassenden vermeintlichen Managers überein, sondern verweist auf das Postfach eines Freemail-Anbieters. Auch die in der E-Mail verwendete Sprache kann ein Indiz auf einen Betrüger sein. Mitarbeiter sollten vor der Überweisung unbedingt persönlich Kontakt mit dem Geschäftsführer, einem Vorstandsmitglied oder der Rechtsabteilung aufnehmen.

## Was tun, wenn es schon zu spät ist?

Wenn Geschäftsführer oder Mitarbeiter den Verdacht haben, **Opfer** von **CEO-Fraud** geworden zu sein, sollten sie sich umgehend an die örtliche Polizeidienststelle wenden und Anzeige erstatten, auch wenn der Betrugsversuch noch rechtzeitig erkannt wurde. Falls bereits eine Zahlung angewiesen wurde, sollten Bankbevollmächtigte schnellstmöglich versuchen, die Transaktion beim Kreditinstitut zu stoppen oder bereits überwiesenes Geld von der Bank zurückbuchen zu lassen. Wurde das Geld schon ins Ausland überwiesen, sollte ein

### Social Engineering

**CEO-Fraud** gilt als Teilphänomen des „Social Engineering“. Diese Form von **Trickbetrug** beschreibt eine zwischenmenschliche Beeinflussung mit dem Ziel, die Person zur Preisgabe von vertraulichen Informationen,

örtlicher Rechtsanwalt im Empfängerland von der geschädigten Firma sofort beauftragt werden, um auf zivilrechtlichem Wege eine Kontosperre bzw. ein Verfügungsverbot zu erwirken. Weitere Informationen, Tipps und Warnhinweise hat das [Bundeskriminalamt](#) in einem aktuellen [Flyer zum Thema CEO-Fraud](#) zusammengestellt. KL (21.07.2017)

zum Kauf eines Produktes oder zur Freigabe von Finanzmitteln zu bewegen. Dabei werden das persönliche Umfeld des Opfers ausspioniert oder Identitäten vorgetäuscht, um geheime Informationen oder unbezahlte Dienstleistungen zu erlangen.

#### **Folgende Artikel könnten Sie auch interessieren:**

-  [Minderwertige T-Shirts, gefälschte Sportschuhe](#)
-  [Cybercrime – Angriffe auf Unternehmen](#)
-  [Auftrag gegen Bargeld](#)
-  [„Fake Customer-Trick“ schädigt Firmen](#)

[Alle Artikel dieser Kategorie](#)

## **Weitere Infos für Polizisten**



**Korruption verursacht Schäden in Millionenhöhe**

### **Auftrag gegen Bargeld**

Die behördliche Baugenehmigung oder die Auftragsvergabe einer Firma...[\[mehr erfahren\]](#)

---



**Rechtsstaatsklassen für Geflüchtete in Hessen**

### **„Fit für den Rechtsstaat“**

Geflüchtete, die nach Deutschland kommen, stehen vor einer Vielzahl...[\[mehr erfahren\]](#)

---



Im Team gegen Internetkriminelle

## Die neue Abteilung Cybercrime im BKA

Seit April gibt es im [Bundeskriminalamt](#) (BKA) die neue Abteilung „CC“...[\[mehr erfahren\]](#)

---



Ersatzteildiebstahl an Kraftfahrzeugen

## Hohes Risiko, lukratives Geschäft

Zwischen Mitte März und Ende April 2017 gab es allein im Raum Köln 13...[\[mehr erfahren\]](#)

---



NRW-Initiative greift ein, bevor Kinder zu Intensivtätern werden

## „Kurve kriegen“

Die [Polizei](#) in Nordrhein-Westfalen kümmert sich mit der Initiative...[\[mehr erfahren\]](#)

---

© Verlag Deutsche Polizeiliteratur

---

## Cookie Einstellungen



- Statistiken
- Essentiell

Wir nutzen Cookies auf unserer Website, die in unserer [Datenschutzerklärung](#) beschrieben sind. Wir verwenden anonyme Statistiken, um unsere Website zu verbessern. Bitte unterstützen Sie unsere

wichtige Präventionsarbeit und akzeptieren Sie alle Cookies. Vielen Dank!

Ablehnen  Alle akzeptieren