bankenverband

BGA
Bundesverband
Großhandel, Außenhandel,
Dienstleistungen e.V.

fokus | unternehmen

# Zielscheibe Unternehmen: Cyberkriminalität

Eine Information der privaten Banken

Berlin, April 2017


# Zielscheibe Unternehmen: Cyberkriminalität

Unternehmen stehen zunehmend im Visier von Cyberkriminellen. Zunächst werden Firmen hierbei über das Internet ausspioniert. Im Anschluss steht ein Mitarbeiter im Mittelpunkt dieser Betrugsversuche, der geschickt manipuliert wird und arglos vertrauliche Daten des Unternehmens preisgibt oder Zahlungen an Fremdkonten anweist. Diese neuen Betrugsmaschen, die unter dem Begriff „Social Engineering“ zusammengefasst werden, sind nicht einfach zu erkennen. Wie Sie Ihr Unternehmen schützen können, erfahren Sie in diesem Faltblatt.

## Wie gehen die Täter vor?

Hinter dem Begriff „Social Engineering“ verbergen sich Telefonanrufe in böswilliger Absicht, E-Mails oder andere Manipulationen, die Mitarbeiter dazu bringen sollen, bestimmte Handlungen auszuführen oder Informationen preiszugeben. Vielen der nachfolgenden Betrugsarten geht eine gezielte Beschaffung von Informationen über das Unternehmen voraus (zum Beispiel über den Internetauftritt, öffentliche Register, beruflich und privat genutzte soziale Netzwerke). Die Strategien der Angreifer sind vielfältig. Allen gemein ist, dass menschliche Eigenschaften wie zum Beispiel Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt werden. Mitarbeiter werden so manipuliert, dass sie gutgläubig handeln und dabei das eigene Unternehmen unbewusst schädigen.

### Der „Chef-Betrug“ („CEO-Fraud“ oder „Fake President“)

Ein zahlungsberechtigter Mitarbeiter (zum Beispiel in der Buchhaltung) bekommt eine gefälschte Nachricht vom vermeintlichen Geschäftsführer (CEO oder CFO) des Unternehmens. In diesem Schreiben gibt er dem betreffenden Mitarbeiter den Auftrag, eine vertrauliche Finanztransaktion durchzuführen. Als Gründe werden Firmenübernahmen, Strafzahlungen, Steuerflucht oder Ähnliches angeführt. In jedem Fall erhält der Mitarbeiter die Anweisung, den gesamten Vorgang auch innerhalb der eigenen Firma „streng geheim“ zu halten. Nach einer ersten Kontaktaufnahme per E-Mail können im weiteren Verlauf auch Anrufe oder E-Mails vermeintlich beauftragter Berater oder Rechtsanwälte folgen. Oft wird der Anschein der Glaubhaftigkeit dieser Aufträge durch gefälschte Dokumente bekräftigt, zum Beispiel durch Rechnungen oder notariell beglaubigte Urkunden. Ziel ist die Veranlassung einer angeblich dringlichen Zahlung in erheblicher Höhe auf ein fremdes Bankkonto, das sich häufig im Ausland befindet. Diese Betrugsvariante kann sich unter Umständen so oft wiederholen, bis dem betroffenen Unternehmen der Betrug auffällt.

### Die geänderte Bankverbindung („Mandate-Fraud“)

Ziel des Täters ist es in diesem Fall, Zahlungen auf eine betrügerische Bankverbindung umzuleiten, indem er die rechtmäßige Kontonummer – mit oder ohne Rechnungsbezug – durch seine eigene Bankverbindung ersetzen lässt. Dies kann mit Hilfe einer einfachen E-Mail erfolgen, in der eine neue Bankverbindung vermeintlich im Namen eines Geschäftspartners mitgeteilt wird. Bekannt sind aber auch Fälle mit postalischer Zustellung zu angeblich geänderten Gehaltskonten oder Aushänge in Mietshäusern zu einem vermeintlichen Eigentümerwechsel. Eine besonders perfide Art, eine neue Bankverbindung einzuschleusen, liegt vor, wenn es den Tätern gelingt, sich in eine bestehende E-Mail-Kommunikation einzuschalten. Der Betrug wird in der Regel erst dann erkannt, wenn der rechtmäßige Zahlungsempfänger auf den fehlenden Geldeingang hinweist.

### Gefälschte Rechnungen

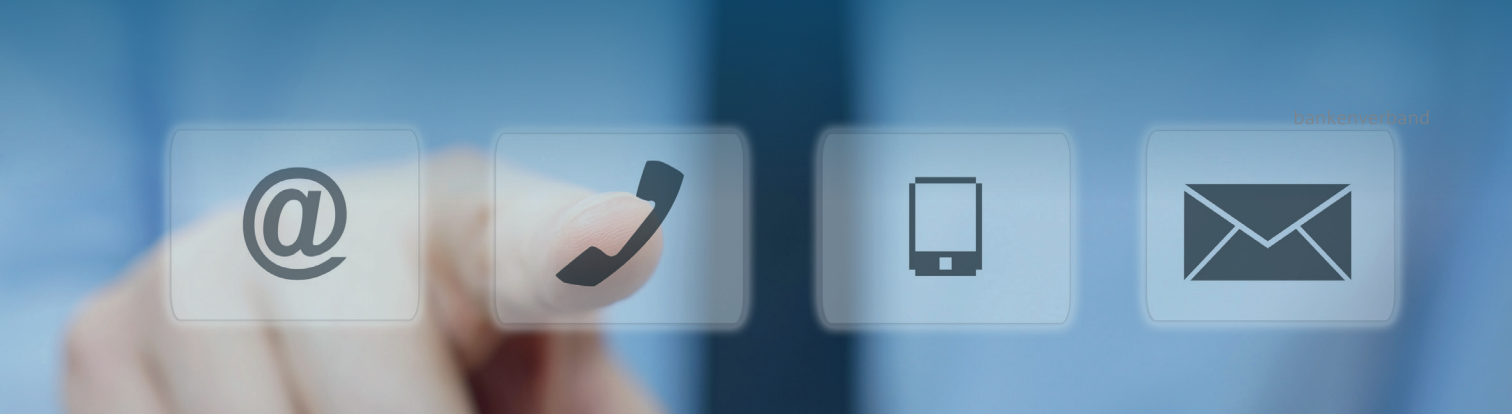
Die Täter versenden gefälschte Rechnungen über Fantasieleistungen, die in Bezug auf Inhalt und Leistung durchaus einer erwarteten Rechnung entsprechen können. Teils werden nachgebildete Briefbögen im Layout von realen Geschäftspartnern verwendet, in denen die Bankverbindung geändert wurde. Interne Kontrollmechanismen können beispielsweise dadurch ausgehebelt werden, dass die E-Mail mit Rechnungsanhang als vermeintliche Weiterleitung des Chefs getarnt wird, der um dringende Erledigung bittet und dazu keine Rückmeldung benötigt.

### Betrug durch Überzahlung

Das Opfer erhält bei dieser Betrugsmethode einen nicht zuzuordnenden Geldeingang. Im weiteren Verlauf des Geschehens meldet sich eine dritte Person und fordert Teile des Geldbetrags zurück. Diese dritte Person kann ein vermeintlich neuer Geschäftspartner sein, der den Zusammenhang zu einem viel geringeren Auftrag herstellt. Die Überzahlung ist per Scheckeinreichung direkt an die Bank erfolgt. Trotzdem spricht der Betrüger von einer Überzahlung aufgrund eines Fehlers seiner Buchhaltung. Erfolgt hier eine Rückzahlung des überschüssigen Betrages durch das Opfer, platzt kurze Zeit später der Scheck. Es sind auch andere Szenarien bekannt, in denen das spätere Opfer betrügerische Zahlungswege oder Kontonummern genannt bekommt, um die vermeintliche Fehlbuchung zu korrigieren.

### Die Betrugsvariante mit der Fernwartungssoftware (Remote Access Tool)

Kriminelle geben sich als Spezialbetreuer der Bank aus und behaupten, es stünde ein Update der Banking-Software an, für das alle Zeichnungsberechtigten zur Verfügung stehen müssten. In den folgenden vermeintlichen „Supportcalls“ folgen die Zeichnungsberechtigten der Firma den Anweisungen der Betrüger (zum Beispiel das Einstecken von Autorisierungsmedien, die Eingabe von Banking- oder Signaturpins bzw. die Gewährung des Fernzugriffs auf den Rechner im Unternehmen). In Verbindung mit dem vermeintlichen „Update“ der Banking-Software wird angekündigt, dass das Online Banking für die Folgetage zunächst nicht erreichbar sei. Es sind auch Fälle bekannt, in denen mittels der Zugangsdaten Kontoauszüge heruntergeladen und dann verfälscht an Kunden verschickt wurden. Dadurch wird verhindert, dass die Manipulation zeitnah aufgedeckt werden kann. Tatsächlich werden Zugangsdaten geändert und Zahlungen, selbst mit verteilten Unterschriften, elektronisch autorisiert.




## Tipps zum Schutz

### 1. Prüfen Sie risikobehaftete Prozesse

An welcher Stelle in Ihrem Unternehmen könnte ein Einfallstor für diese Betrugsversuche liegen? Nicht nur Zahlungseingabe oder Zahlungsfreigabe sind sicherheitskritisch. Auch Stammdatenänderungen (Kontoverbindungen, Versandadressen) sollten über gezielte Kontrollen abgesichert sein (auch bei Gehältern).

### 2. Offene Unternehmenskultur: Lassen Sie Rückfragen zu

Bei ungewöhnlichen Geschäftsvorfällen oder Vorgängen sollten Rückfragen immer bis in die Führungsebene möglich sein: Eine telefonische Rückversicherung bei einem Ansprechpartner oder Vorgesetzten im Unternehmen kann Betrug verhindern.

### 3. Bewusster Umgang mit Social Media

Kontaktanfragen von Unbekannten sollten nicht leichtfertig akzeptiert werden. Schaffen Sie bei Ihren Mitarbeitern ein Bewusstsein dafür, dass veröffentlichte Daten in sozialen Netzwerken und im Internet im Allgemeinen darauf zu prüfen sind, wie sie gegen die Person selbst genutzt werden können.

### 4. Vorsicht beim Öffnen von E-Mails von unbekannten Absendern

Sensibilisieren Sie Ihre Mitarbeiter für einen vorsichtigen Umgang mit E-Mails unbekannter Absender. Selbst wenn der vermeintliche Absender der E-Mail seriös erscheint, sollte die E-Mail-Adresse überprüft werden. Passt die erscheinende E-Mail-Adresse zum Absender, kann die E-Mail geöffnet werden. Falls nicht, sollte die E-Mail gelöscht werden. Generell sollte jeder E-Mail-Inhalt darauf geprüft werden, ob er glaubwürdig bzw. plausibel erscheint. Dies gilt auch für alle Links und Bilder in der betreffenden E-Mail. Passen die Links nicht zum Absender, sollte die E-Mail an den zuständigen IT-Support weitergeleitet und im Nachgang gelöscht werden.

### 5. Sorgen Sie für IT-Sicherheit

Sichern Sie Ihre Systeme ab: Implementieren Sie Firewalls, Antivirensoftware, Updates und ändern Sie Startpasswörter, auch auf der Telefonanlage sowie auf allen mit dem Internet verbundenen Systemen. Software, die von Dritten ungefragt aufgedrängt wird, sollte nicht installiert werden.

### 6. Vergabe von Nutzerrechten und sichere Autorisierungsprozesse

Vergeben Sie Nutzerrechte nur in dem Umfang, wie sie von den Anwendern zur Erledigung ihrer Aufgaben benötigt werden. Übermäßig viele Nutzerrechte stellen ein erhöhtes Risiko dar. Bei der Vergabe von Autorisierungsrechten wenden Sie als Minimalstandard das Vier-Augen-Prinzip (gegebenenfalls bei hohen Zahlungsbeträgen auch das Sechs-Augen-Prinzip) an. Vermeiden Sie dagegen die Vergabe von Einzelvollmachten.

### 7. Schulungen zu neuen Betrugsszenarien

Führen Sie regelmäßig Schulungen zu diversen Betrugsszenarien durch, um Ihre Mitarbeiter für das Thema zu sensibilisieren.

### 8. Mit gesundem Menschenverstand prüfen

Appellieren Sie an Ihre Mitarbeiter: Jeder ungewöhnliche Sachverhalt sollte mit gesundem Menschenverstand betrachtet werden. Erhöhte Aufmerksamkeit ist der beste Schutz für Ihr Unternehmen.

## Was tun, wenn es doch passiert ist?

Kontaktieren Sie umgehend Ihre Bank, insbesondere wenn die Zahlung noch „frisch“ ist, denn Zahlungen werden nur dann garantiert zurückgegeben, wenn sie dem Empfängerkonto noch nicht gutgeschrieben sind, unter Umständen aber auch dann, wenn über das Geld noch nicht verfügt wurde.

Auch wenn ein Betrug rechtzeitig abgewendet werden konnte: Teilen Sie Ihrer Bank die Daten des Kontos mit, auf das die Zahlung überwiesen werden sollte. Wir empfehlen Ihnen immer – auch im Versuchsfall – eine Anzeige bei der Polizei.

Weitere Informationen finden Sie bei der Zentralen Ansprechstelle Cybercrime (ZAC) unter **www.allianz-fuer-cybersicherheit.de.**

Allgemeine Hinweise zur Cyber-Sicherheit gibt es auch unter **www.bsi.bund.de.**

Impressum:
Herausgeber: Bundesverband deutscher Banken e.V., Postfach 040307, 10062 Berlin | Verantwortlich: Iris Bethge | Druck: PieReg Druckcenter Berlin | Gestaltung: doppel:punkt redaktionsbüro janet eicher, Bonn | Fotos: istockfoto (scyther5, Marco_Piunti, BernardaSv), fotolia (fotogestoeber, Sergey Nivens)

## So erreichen Sie den Bankenverband


Per Post:
Bundesverband deutscher Banken
Postfach 040307
10062 Berlin

Per Telefon:
+49 30 1663-0

Per E-Mail:
bankenverband@bdb.de

Internet:
bankenverband.de
unternehmen.bankenverband.de

Social Media:


Scannen Sie diesen QR-Code
für weitere Publikationen der Reihe
fokus|unternehmen.