bankenverband

Zielscheibe Unternehmen: **Cyberkriminalität**

Berlin, Oktober 2019

Inhalt

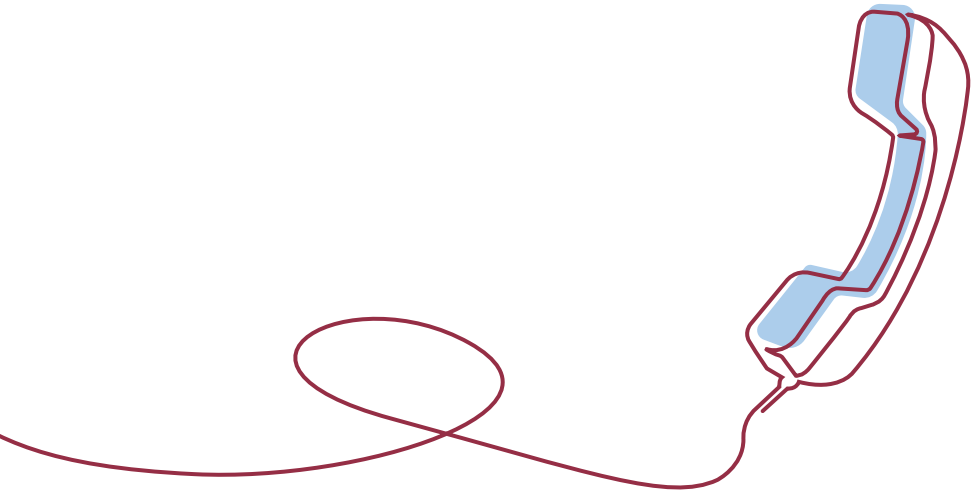
Vorwort

Unternehmen stehen zunehmend im Visier von Cyber-Kriminellen. 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 Betrugsmaschen, die unter dem Begriff „Social Engineering“ zusammengefasst werden, sind nicht einfach zu erkennen. Wie Sie Ihr Unternehmen schützen können, erfahren Sie in dieser Broschüre.

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 Informationsbeschaffung über das Unternehmen voraus (z.B. über den Internetauftritt, öffentliche Register, beruflich und privat genutzte soziale Netzwerke). Die Strategien der Angreifer sind vielfältig. Allen gemein ist, dass menschliche Eigenschaften wie z.B. 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 (z.B. in der Buchhaltung) bekommt eine gefälschte Nachricht vom vermeintlichen



Geschäftsführer (CEO oder CFO) des Unternehmens. Das kann nicht nur schriftlich sein: Es sind Fälle bekannt, in denen Stimmen durch KI-gestützte Programme simuliert werden. Es handelt sich um selbstlernende Stimmimitationssoftware. Der Tonfall und die Sprechweise des vermeintlichen Gesprächsführers werden dabei am Telefon nachgeahmt. Der Betrüger gibt dem betreffenden Mitarbeiter zum Beispiel den Auftrag eine dringende, vertrauliche Finanztransaktion durchzuführen. Die Kriminellen passen die Gründe dabei dem Unternehmen an: Beispielsweise geht es um Firmenübernahmen, Strafzahlungen oder Ähnliches. In jedem Falle erhält der Mitarbeiter die Anweisung, den gesamten Vorgang auch innerhalb der eigenen Firma „streng geheim“ zu halten. Nach einer ersten Kontaktaufnahme 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, z.B. 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 in diesem Fall ist es, Zahlungen auf eine andere Bankverbindung umzuleiten, indem er die rechtmäßige Kontonummer 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, zum Beispiel eines Lieferanten, mitgeteilt wird. Bekannt sind aber auch Fälle, in denen vermeintliche Änderungen von Gehaltskonten mitgeteilt werden oder Aushänge in Mietshäusern über einen angeblichen Eigentümerwechsel informieren. Eine besonders perfide Art eine neue Bankverbindung einzuschleusen ist,

wenn es den Tätern gelingt, sich in eine bestehende E-Mail-Kommunikation zwischenzuschalten. 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 „Support Calls" folgen die Zeichnungsberechtigten der Firma den Anweisungen der Betrüger (z.B. das Einstecken von Autorisierungsmedien, die Eingabe von Banking- oder Signatur-PINs bzw. die Gewährung des Fernzugriffs auf den Rechner im Unternehmen). Jetzt werden Zugangsdaten geändert und Zahlungen, selbst mit verteilten Unterschriften, elektronisch autorisiert. Um den Angriff zu verschleiern, wird in Verbindung mit dem vermeintlichen „Update" der Banking-Software angekündigt, dass das Onlinebanking für die Folgetage 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.

Tipps **zum Schutz**

1. Prüfen Sie risikobehaftete Prozesse

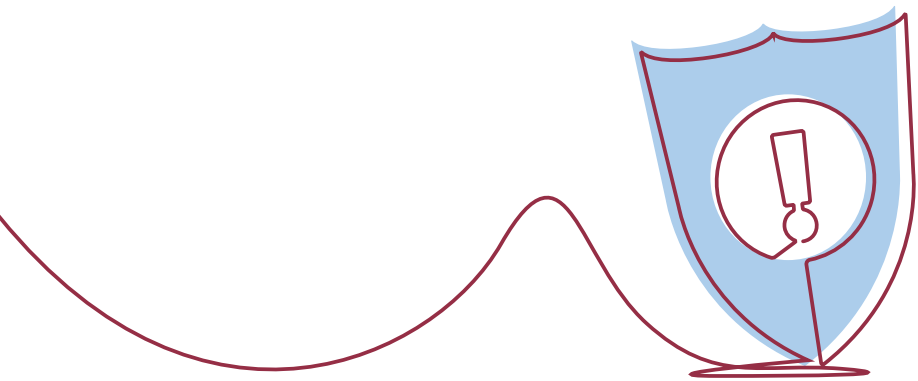
An welcher Stelle in Ihrem Unternehmen könnte ein Einfallstor für diese Betrugsversuche liegen? Nicht erst Zahlungseingabe oder Zahlungsfreigabe sind sicherheitskritisch. Auch Stammdatenänderungen (Kontoverbindungen, Versandadressen) sollten über gezielte Kontrollen oder festgelegte Prozesse abgesichert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

2. Etablieren Sie eine offene Unternehmenskultur und lassen Sie Rückfragen zu

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

3. Sensibilisieren Sie Ihre Mitarbeiter für einen bewussten Umgang mit Sozialen Medien

Kontaktanfragen von Unbekannten über Social-Media-Netzwerke sollten nicht leichtfertig akzeptiert werden. Schaffen Sie in



Ihrem Unternehmen ein Bewusstsein dafür, dass veröffentlichte Daten in solchen Netzwerken immer darauf zu prüfen sind, wie sie gegen die Person selbst genutzt werden können, zum Beispiel für einen Identitätsdiebstahl.

4. Lassen Sie beim Öffnen von E-Mails unbekannter Absender Vorsicht walten

Sensibilisieren Sie Ihre Mitarbeiter für einen vorsichtigen Umgang mit E-Mails. Selbst wenn der vermeintliche Absender seriös erscheint, sollte die E-Mail-Adresse überprüft werden. Passt die E-Mail-Adresse zum Absender, kann die 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 und

Antivirensoftware. Lassen Sie Updates automatisch installieren und fordern Sie Mitarbeiter auf, regelmäßig Passwörter zu ändern, auch für die Telefonanlage sowie auf allen mit dem Internet verbundenen Systemen. Software, die von Dritten ungefragt aufgedrängt wird, sollte nicht installiert werden.

6. Prüfen Sie die Vergabe von Nutzerrechten und sorgen Sie für 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 ein Sechs-Augen-Prinzip) an. Vermeiden Sie dagegen die Vergabe von Einzelvollmachten.

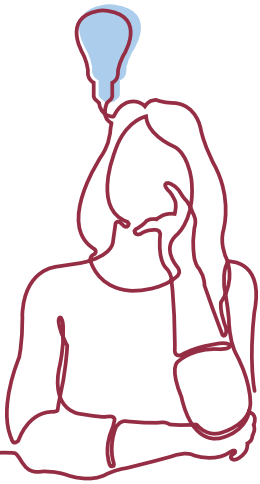
7. Schulen Sie zu neuen Betrugsszenarien

Führen Sie regelmäßig Schulungen zu diversen Betrugsszenarien durch, um Ihre Mitarbeiter für das Thema zu sensibilisieren. Erklären Sie Ihnen, wie die Betrüger vorgehen und worauf man achten sollte.

8. Prüfen Sie mit gesundem Menschenverstand

Appellieren Sie an Ihre Mitarbeiter: Jeder 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 können nur dann zurückgegeben werden, wenn sie dem Empfängerkonto noch nicht gutgeschrieben wurden; 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 Bankverbindung des angeblichen Empfängers mit, auf das die Zahlung überwiesen werden sollte. Wir empfehlen Ihnen immer eine Anzeige bei der Polizei zu erstatten, auch im Versuchsfall.

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

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

Als Beirat haben Experten die Arbeit an dieser Publikation unterstützt.
Hierfür danken wir:

Michael Alber
Geschäftsführer
Bundesverband Großhandel, Außenhandel, Dienstleistungen

Dr. Alexander Barthel
Leiter der Abteilung Wirtschafts- und Umweltpolitik
Zentralverband des Deutschen Handwerks

Dr. Christian Fahrholz
Leiter des Referats Geld und Währung, Unternehmensfinanzierung, Unternehmenssicherung
Deutscher Industrie- und Handelskammertag

Stephan Jansen
Geschäftsführer
Verband Deutscher Bürgschaftsbanken

Albrecht von der Hagen
Hauptgeschäftsführer
Die Familienunternehmer

Fabian Wehnert
Abteilungsleiter Mittelstand und Familienunternehmen
Bundesverband der Deutschen Industrie

So erreichen Sie den Bankenverband

Bundesverband deutscher Banken
Postfach 040307
10062 Berlin
+49 30 1663-0

bankenverband@bdb.de
bankenverband.de

Herausgeber:
Bundesverband deutscher Banken e. V.
Inhaltlich Verantwortlicher:
Oliver Santen
Gestaltung:
ressourcenmangel an der panke GmbH
Druck:
Buch- und Offsetdruckerei H. Heenemann GmbH & Co. KG

Berlin, Oktober 2019