Business-E-Mail-Crime & Social Engineering

Zahlungsverkehr Betrugsprävention, Frankfurt am Main

Cybercrime gegen Unternehmen setzt direkt beim Mitarbeiter an.

Was sind die Gründe dafür, dass Hacker eher auf den Mitarbeiter setzen:

- Verschiedene Produkte für das Electronic Banking
- National größere Unterschiede bei den eingesetzten Technologien und Autorisierungsmedien.
- Die in Deutschland verwendeten Zahlungsverkehrsprodukte haben ein hohes technisches Sicherheitsniveau.

Fazit

- Im Ausland seit Jahren praktizierte Betrugsszenarien hielten 2015 breiten Einzug im deutschsprachigen Raum.
- Die Täter setzen bei ihrem Angriff gezielt auf die Täuschung eines Mitarbeiters im Unternehmen, um …

01 Erpressung

… diesen oder das Unternehmen im Anschluss zu erpressen.

02 Zahlungen

… ihn dazu zu bringen, scheinbar rechtmäßige Zahlungen auszulösen.

03 Zugriff

… Zugriff auf den Arbeitsplatzrechner des Mitarbeiters zu erlangen, um selbst Zahlungen auszulösen, z. B. über eine Fernwartungssoftware (Remote Access).

Betrugsszenarien

Agenda

Betrugsszenario: Remote Access Tool

Der Betrug mit sonst nützlicher Fernwartungssoftware

- Im Retail-Banking erfolgt der Betrug oft als Microsoft-Techniker-Anruf.
- Bei Unternehmen wird vorbereitend Wissen zur Firma gesammelt.
- Später ruft ein vermeintlicher Bankmitarbeiter beim Mitarbeiter des Unternehmens an. Unter einem Vorwand wird zum Beispiel technische Unterstützung für ein notwendiges Update Ihres Zahlungssystems aufgedrängt.
- Installiert der Mitarbeiter - wie vom Anrufer gefordert - ein Remote Access Tool (eine sonst nützliche Support-Software), erhält der Täter durch den Mitarbeiter im Unternehmen Zugriff auf den Arbeitsplatzrechner.
- Der Mitarbeiter wird aufgefordert, Zugangsdaten in ungewöhnlichen Feldern zu erfassen. Somit sind Passwörter für den Täter mitlesbar. Durch den erlangten Zugriff und die Zugangsdaten werden Zahlungen autorisiert.
- Später soll das Online Banking aufgrund der Durchführung eines manuellen Updates nicht erreichbar sein. In Wirklichkeit werden nur die Zugangsdaten vom Täter abgeändert, um Ihnen die Kontrolle über Ihr Konto zu entziehen.

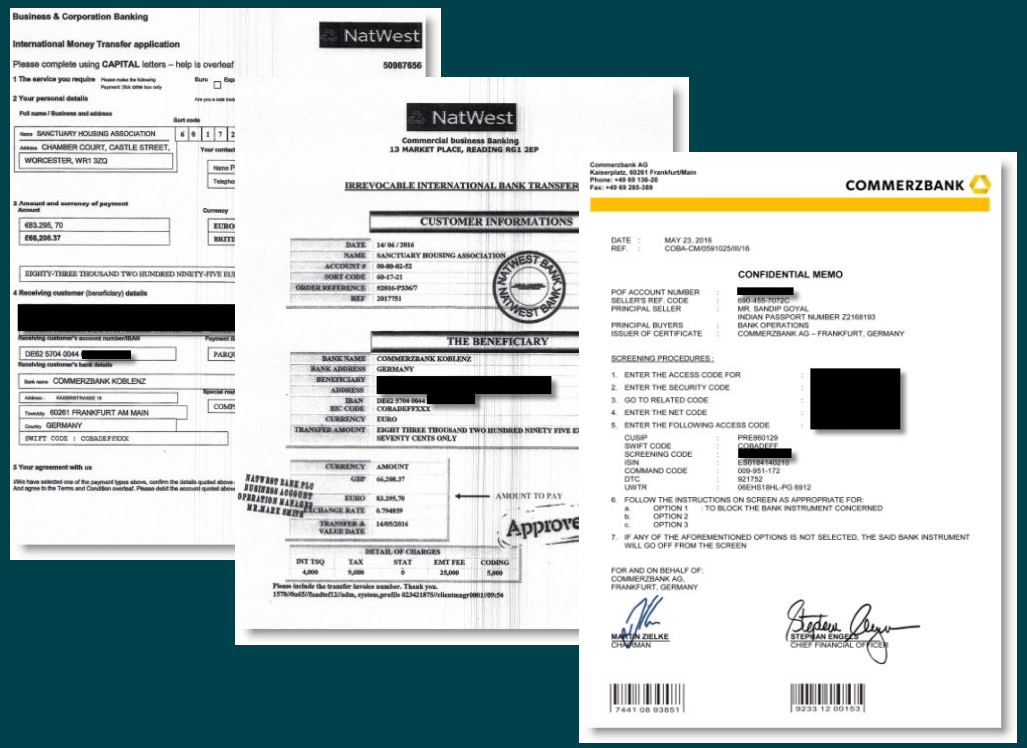
TeamViewer
AnyDesk
fastviewer
ATERA
ninjaOne
netviewer

TIPP: Haben Sie technische Hilfe erbeten und es ruft Sie hierzu der erwartete Ansprechpartner an, dann ist ein Betrug unwahrscheinlich. Drängt Ihnen jemand Software auf und versucht Ihnen Probleme glaubhaft zu machen, welche Sie nicht wahrnehmen, wird es vermutlich Betrug sein!

Betrugsszenario: Gefälschte Zahlungsbestätigung

Die Lieferung der Ware wird verlangt, die Zahlung ist aber nur vorgetäuscht.

- Es wird ein Geschäft angebahnt und dafür auch eine Teilzahlung oder Vorkasse vereinbart.
- Die Ware wird produziert und für den Kunden hergestellt. Die Anzahlung erfolgt ordnungsgemäß.
- Kurz vor dem Liefertermin schickt der Empfänger einen vermeintlich echten Zahlungsbeleg, einen Kontoauszug oder sogar eine angebliche SWIFT-Bestätigung seiner Bank, dass die Zahlung erfolgt ist.
- Die Ware wird verschickt.
- Es stellt sich später heraus, dass es sich um eine Scheinfirma (Briefkastenfirma) gehandelt hat.
- Die Zahlungsbestätigungen waren gefälscht. Das Geld kommt nie an. Das vermeintliche Konto des Auftraggebers existiert meist gar nicht.

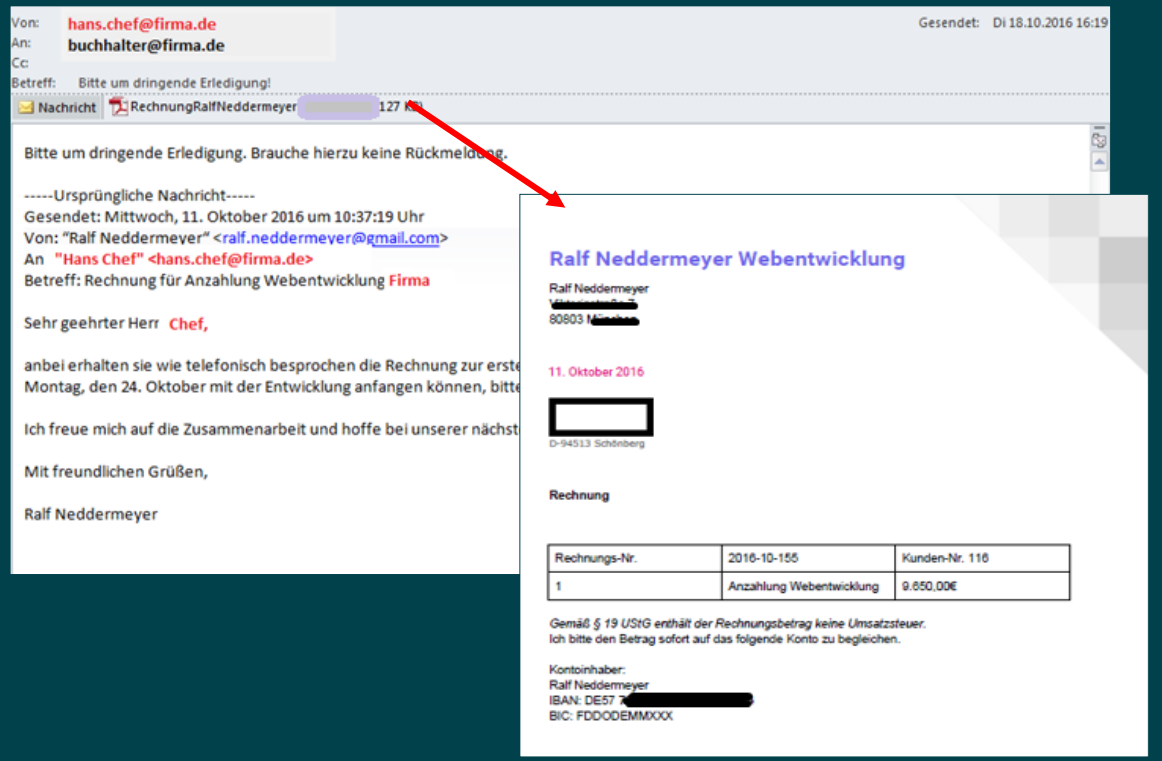


TIPP: Eine Überweisung hat die Rechtsform, dass sie befreiend ist, wenn der Betrag auf dem Konto des Empfängers gutgeschrieben ist. Daher prüfen Sie vermeintliche Zahlungsbelege auf Fälschungsindizien und sichern Sie internationale Geschäfte mit neuen Geschäftspartnern ab. Recherchieren Sie im Internet.

Betrugsszenario: Rechnungsbetrug

Der Rechnungsbetrug wird neu erfunden, wenn der vermeintliche Chef die Überweisung will oder ein Anwalt auf Bezahlung von Außenständen drängt.

- In einer Variante, wird eine letzte Mahnung an den Buchhalter verschickt. Wenig später meldet sich ein Anwalt der Firma und bittet um Begleichung. Auf Wunsch werden gefälschte Rechnungen und Aufträge sofort nachgeschickt.
- In einer anderen Variante erhält der Buchhalter eine vermeintliche Weiterleitung des eigenen Vorgesetzten, mit der Bitte um Begleichung. Im Anhang eine Rechnung und eine erfundene Historie zum Auftrag.
- In aktuellen Varianten erhält der Mitarbeiter nur die Frage des Vorgesetzten, wieviel Geld noch auf dem Konto ist und ob heute noch eine Auslandsüberweisung getätigt werden kann. Auf die Antwort erfolgt der Auftrag.
- Schäden im Einzelfall zwischen 10.000 EUR und 180.000 EUR.
- Achten Sie auf die Echtheit des Absenders. Ein falscher Buchstabe ist eine andere Adresse. Die Übersicht der Inbox enthält NICHT den Absender.

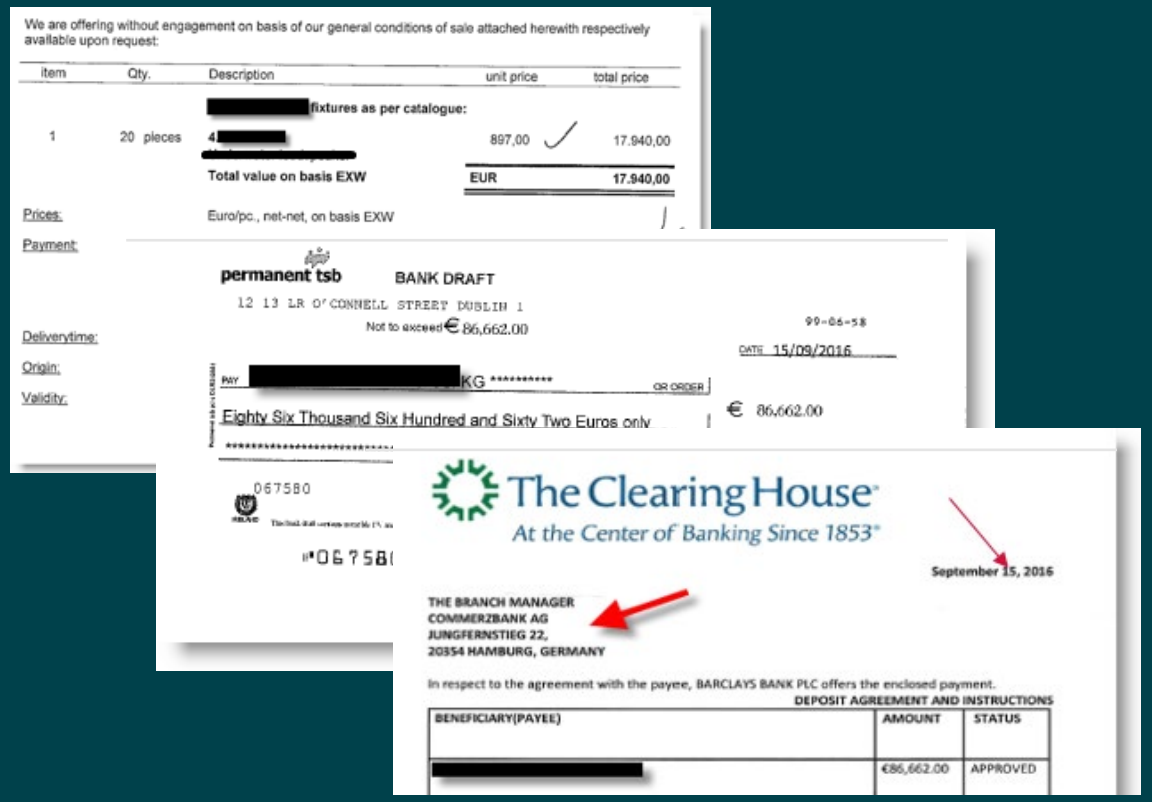


TIPP: Klären Sie Ihre Mitarbeiter über diese Betrugsform auf. Rechnungen sollten nicht ohne entsprechenden Vorgang oder Auftrag bezahlt werden. Nutzen Sie Outlook-Funktionen, die signalisieren, ob sich ein Empfänger innerhalb Ihrer Organisation befindet oder außerhalb.

Betrugsszenario: Schecküberzahlung

Der Scheck platzt. Ihre Rücküberweisung ist final.

- **Traditionelle Form:** Bei einer Bestellung oder Buchung wird die Bezahlung per Scheck erfragt. Der Scheck ist dann über eine zu hohe Summe ausgestellt und man bittet um Rücküberweisung des „versehentlich“ überzahlten Betrags.
- **Neue Form:** Ihre Firma geht auf einen Auftrag ein. Sie bitten um Überweisung unter Angabe Ihrer IBAN. Dadurch kennt der Täter die Adresse Ihrer Bank.
- Ein überhöhter Scheck wird mit einem gefälschten Anschreiben direkt an die Bank geschickt. Im Anschreiben wird die Gutschrift auf Ihr Konto verlangt.
- Erfolgt die Einreichung, haben Sie einen nicht zuordenbaren Habenumsatz.
- Etwas später erreicht Sie eine E-Mail des Täters, die vorgibt, dass die haus-eigene Buchhaltung versehentlich zwei Vorgänge vermischt habe. Ihnen wurde daher zu viel Geld „überwiesen“, der Betrag einer anderen Rechung.
- Der Täter weiß, dass Sie nur die Gutschrift kennen, den Scheck aber nie in den Händen hielten. Er bittet um Rücküberweisung des Differenzbetrags. Der Scheck ist gefälscht und „platzt“.

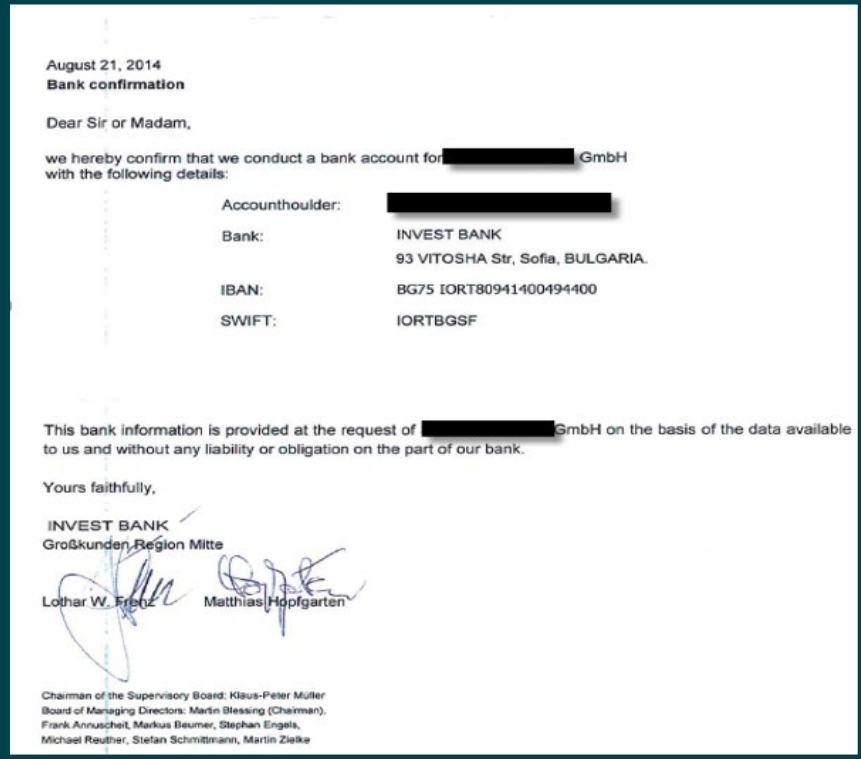


TIPP: Prüfen Sie genau, ob die Gutschrift eine Scheckeinreichung ist. Ein Scheck kann je nach Land mindestens 10 Tage zurückgegeben werden, manchmal auch über mehrere Monate. Wir rufen Sie vor Einreichung durch Dritte an. Sollte eine Scheckeinreichung nicht von Ihnen veranlasst worden sein, kontaktieren Sie umgehend Ihre Bank.

Betrugsszenario: Payment Diversion

Wenn sich plötzlich die Bankverbindung ändert.

- Vermeintliche Korrektur der Bankverbindung eines Geschäftspartners.
- Diese kann unmittelbar auf eine echte E-Mail mit einer Rechnung folgen, wenn das E-Mail-System Ihres Geschäftspartners kompromittiert wurde.
- Auch gefälschte Bankverbindungs-Änderungen im Namen eines Mitarbeiters zur Umleitung von Gehaltszahlungen sind bekannt.
- Mögliche Eingangskanäle sind E-Mail, Telefax oder per Brief.
- Erfolgt die Änderung ohne einen Rechnungsbezug, so passiert dies meist bei Unternehmen, die nach festen Verträgen auf Lieferung oder Leistung bezahlen (Bergbau, Reiseunternehmen, Chemie, Automobilzulieferer etc.).
- Der Betrug wird bei Änderung erst mit der Mahnung des Geschäftspartners bemerkt. Oft geht Zeit verloren, wenn erst noch eine Nachforschung zur falschen Überweisung beauftragt wird.



August 21, 2014
Bank confirmation

Dear Sir or Madam,

we hereby confirm that we conduct a bank account for [redacted] GmbH with the following details:

Accounthoulder:	[redacted]
Bank:	INVEST BANK 93 VITOSHA Str, Sofia, BULGARIA.
IBAN:	BG75 IORT80941400494400
SWIFT:	IORTBGSF

This bank information is provided at the request of [redacted] GmbH on the basis of the data available to us and without any liability or obligation on the part of our bank.

Yours faithfully,

INVEST BANK
Großkunden Region Mitte

Lothar W. Frenz Matthias Hopfgarten

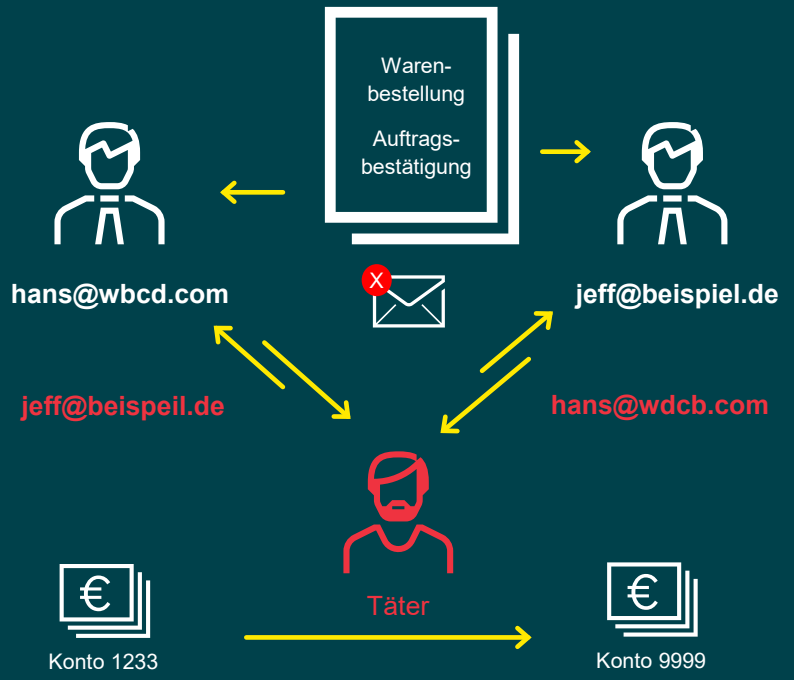
Chairman of the Supervisory Board: Klaus-Peter Müller
Board of Managing Directors: Martin Blessing (Chairman),
Frank Annuscheit, Markus Beumer, Stephan Engels,
Michael Reuther, Stefan Schmittmann, Martin Zielke

TIPP: Sichern Sie Ihre E-Mail-Kommunikation ab. Eine unverschlüsselte E-Mail hat den Charakter einer Postkarte. Schützen Sie Ihre Stammdaten, wie Bankverbindungen und Lieferanschriften Ihrer Geschäftspartner. Verlangen Sie dies auch von Ihren Vertragspartnern. Eine Änderung hinterfragen Sie am besten auf einem anderen „Kanal“ (z.B. Anruf).

Betrugsszenario: Man in the middle (PD)

Irgendwo in einem der E-Mail-Replys ändert sich plötzlich der Absender um nur ein - zwei Zeichen.

- Geschäftspartner bahnen ein Geschäft an und tauschen zu Beginn auch persönliche Fragen aus. Dann folgt der Auftrag.
- Sie bemerken nicht, wie sich über die Zeit der Kommunikation auf einmal andere, ähnlich aussehende E-Mail-Adressen einschleichen.
- Da der Inhalt dem Original quasi entspricht und auch der Nachrichtenverlauf als Historie anhängt, wird auch kein Verdacht geschöpft, wenn sich bei Rechnungsstellung die Bankverbindung ändert.
- Hier wurde manipulierend in die Bankdaten der Rechnung eingegriffen! Die Rechnung wird aber erwartet und auch freigezeichnet.
- Der Betrug wird erst mit der Mahnung Ihres Geschäftspartners bemerkt oder wenn die Ware beim Bezahler nicht ankommt.
- Oft geht Zeit verloren, wenn erst eine Nachforschung zur falschen Überweisung beauftragt wird.



TIPP: Sichern Sie Ihre E-Mail-Kommunikation ab. Eine unverschlüsselte E-Mail hat den Charakter einer Postkarte. Schützen Sie Ihre Stammdaten, wie Bankverbindungen und Lieferanschriften Ihrer Geschäftspartner. Verlangen Sie dies auch von Ihren Vertragspartnern. Eine Änderung hinterfragen Sie am besten auf einem anderen „Kanal“ (z.B. Anruf).

Betrugsszenario: CEO-Fraud (vs. Chefbetrug)

Der einzelne Mitarbeiter wird zur Drohne des Täters. Das Vertrauen zur Hausbank wird ausgenutzt

- Ihre Firma wird teilweise Monate vor dem Betrug ausspioniert. Daten werden über das Internet, über öffentliche Register, beruflich genutzte Soziale Medien und über teils belanglos erscheinende Anrufe gesammelt.
- Der Mitarbeiter erhält eine E-Mail oder einen Anruf; vermeintlich vom Chef. Er wird mit einer vertraulichen Finanzsache betraut und soll Kontakt zu einem Berater/Rechtsanwalt einer namhaften Kanzlei/Beratungsgesellschaft aufnehmen.
- Ihm wird die Vertraulichkeit immer wieder deutlich gemacht. Noch benötigte Informationen werden erfragt: Konten, Guthaben, Vollmachten.
- Der Mitarbeiter erhält später einen vorab unterschriebenen Überweisungsauftrag.
- Löst der Mitarbeiter die Überweisung aus, werden weitere „Zahlungen“ erforderlich. Der Täter ruft an, bis der Betrug auffällt oder kein Geld mehr da ist.

Von: **Hans Chef:** hans.chef@firma.de,
<cc.bafin@munich.com>
Gesendet: Montag, 15. Februar 2016 11:13
An: [redacted]
Cc: cc.bafin@munich.com
Betreff: vertraulich

Sehr geehrte Frau [redacted]

zurzeit bereiten wir die Übernahme eines Unternehmens vor, dies betrifft insbesondere die erforderlichen finanziellen Transaktionen.

Die Angelegenheit muss absolut vertraulich behandelt werden. Niemand sonst, auch nicht innerhalb unseres Hauses, wird zurzeit darüber informiert.

Die öffentliche Bekanntmachung des Übernahmeangebots erfolgt in Kürze.

Aufgrund Ihrer Diskretion und bisher einwandfreien Arbeit in unserem Unternehmen möchte ich Ihnen die Verantwortung für dieses Projekt übertragen.

Ich bitte Sie, umgehend Herr Dr. Mueller von der Kanzlei KPMG (tomas.mueller@consultant.com) zunächst unsere Bankverbindung für die weitere Bearbeitung zu übermitteln.

Da die gesamte Transaktion absolut vertraulich behandelt werden muss bitte ich Sie, den Stand der Transaktion nur mit mir ausnahmslos per E-Mail abzustimmen.

Weiter bitte ich Sie, mich in dieser Angelegenheit weder persönlich noch telefonisch zu kontaktieren. Jede Erörterung der geplanten Übernahme erfolgt ausnahmslos per E-Mail an Sie oder mich, auch um eine ausreichende Dokumentation gemäß den BAFin Richtlinien sicherzustellen.

Ich zähle auf Ihre Diskretion und bedanke mich schon jetzt für Ihre Mitarbeit.

Mit freundlichen Grüßen

Geschäftsführer

TIPP: Rufen Sie uns auch bei einem CEO-Fraud-Versuch immer an – selbst wenn der Mitarbeiter die E-Mail erkannt hat. Klären Sie über diese Betrugsform auf. Nutzen Sie Outlook-Funktionen, die zeigen, ob sich ein Empfänger innerhalb Ihrer Organisation befindet.

Betrugsszenario: CEO-Fraud

01 Der vermeintliche Chef betraut den Mitarbeiter unter absoluter Vertraulichkeit mit einer Aufgabe. Er soll einem Dritten (Anwalt, Unternehmensberatung, Kanzlei) alle notwendige Informationen per E-Mail mitteilen.

02 Der Mitarbeiter wird danach von der dritten Person kontaktiert, geschickt beruhigt und manipuliert. Ziel ist die Erlangung weiterer Informationen (Limite, Autorisierungen, notwendige Unterschriften).

03 Der Mitarbeiter erhält den Auftrag, eine Zahlung auszulösen; durchaus mit bereits geleisteten Unterschriften, die er zuvor als notwendig bekannt gegeben hat (verteilte Unterschrift). Dabei wird er gekonnt in den Mailverkehr zwischen den vermeintlichen Chef und der dritten Person einbezogen.

04 Der uns als Bank bekannte und vertraute Mitarbeiter beauftragt die Zahlung mit der gebotenen Dringlichkeit. Rückfragen werden meist aufgrund der Vertraulichkeit nicht beantwortet.

Betrugsszenario: CEO-Fraud

05 Probleme werden mit dem vermeintlichen Chef geklärt. Nicht autorisierte Unterschriften sollen nun z. B. auf der Basis des Handelsregisters autorisiert werden.

06 Es wird mit Fälschungen von Dokumenten, Ausweisen, Beglaubigungen und BaFin-Unterlagen gearbeitet. Dabei wird der Mitarbeiter im Unternehmen auch instrumentalisiert, Druck auf die Bank auszuüben. Die Zahlung sei ja schließlich dringlich.

07 Verlangte Absicherungen und Bestätigungen werden geliefert.

08 Reicht der Kontostand für die Zahlung nicht aus, wird der Mitarbeiter mit der Frage nach einer Überziehung zur Bank geschickt. Ein Ausgleich wird zum Folgetag zugesagt, und zwar über Gelder die vermeintlich vom Mutterkonzern oder der Tochtergesellschaft kommen sollen. Gibt es diese nicht, gibt der Täter sich auch mit kleineren Beträgen zufrieden.

09 Die Rückfrage der Bank, ob es sich um Betrug handeln könnte, wird verneint: „Die Zahlung ist OK.“

Selbst die Rückfrage der eigenen Compliance-Abteilung im Unternehmen wird mit dem Verweis auf die gebotene Vertraulichkeit abgewiesen.

Betrugsszenario: Erpressung

Was ist Ihr Nutzen Daten preiszugeben?

Regel Nr. 1: Wenn etwas kostenfrei ist,
dann zahlen Sie mit Ihren Daten.

- Mögliches Szenario: Ein Mitarbeiter hat seine Informationen z.B. auf Xing und wird über Headhunter oder Consultants mit falscher Identität als Kontakt angefragt. Mit der Bestätigung legt er sein Netzwerk und seine Daten offen, wenn er die nicht ohnehin schon aufgrund fehlender Datenschutzeinstellungen jedermann anzeigt.
- Hat der Mitarbeiter in privat genutzten Sozialen Medien den gleichen Namen – führt dort private Informationen offen oder akzeptiert Freundschaftsanfragen persönlich nicht bekannter Kontakte – und ist vielleicht mit seinen eigenen Kindern verlinkt, die wiederum posten, wo sie regelmäßig zum Sport gehen – entsteht ein Erpressungspotenzial!
- Andere Variante: Spam-Erpressungsmails geben vor, Zugriff auf die Kamera Ihres Laptops gehabt zu haben und drohen mit der Veröffentlichung der aufgezeichneten Inhalte, wenn Sie nicht ...
- Neue Bedrohung in Social Media: Sextortion

Social Media

XING

Linked in

Facebook

twitter

Betrugsszenario: Erpressungstrojaner

Der Kunde wird über Schadsoftware oder einen Hack angegriffen. Die Dateien der Firma werden kopiert und verschlüsselt.

- Prävention ist der einzige kostengünstige Weg. Investieren Sie in Ihre IT-Sicherheit und IT-Überwachung!
- Plötzliches Desaster-Szenario. Wenn eine Firma verschlüsselt ist, helfen nur noch Offside-Backups und Offsite-Notfallpläne!
- Keine Backups mehr? Dann ist der Schaden oft höher, als die erpresste Summe. Zahlen? Erhält man einen Schlüssel? Rettet man die Daten?
- Melden Sie den Vorgang der Versicherung, sofern sie cyberversichert sind.
- Uns bekannter größter erpresster Einzelbetrag in Bitcoin: 240 Mio. EUR
- **Wir empfehlen nicht zu zahlen!**
- DSGVO nicht vergessen! Wer einen relevanten Zwischenfall nicht in 72 Stunden anzeigt, kann mit Bußgeldern belegt werden?
- Wir empfehlen dringend: Binden Sie die Polizei (Zentrale Ansprechstelle Cybercrime des LKA) mit ein.
- Überlassen Sie die Arbeit IT-Forensikern. Die eigene IT hat oft nicht die notwendigen Skills und/oder Kapazitäten zur Bewältigung der Lage. Eine Entschlüsselung im Nachgang ist fast nie möglich.

Videos

01 Secuso.org auf Youtube (Deutsch)

In diesem Video geht es um Fallstricke in der E-Mail-Bearbeitung. Wie erkenne ich echte von falschen Links und worauf muss ich achten. Secuso.org ist aus der Uni Darmstadt entstanden und hat mehrere solche Videos im Netz.
https://youtu.be/4xIU1lPJs_4

02 Fusion.net auf Youtube (Englisch)

Es geht in diesem Video um ein Beispiel einer Social Hackerin, die auf Anfrage eines Reporters demonstriert, wie leicht ein „Social Hack“ ist. Eigentlich soll sie nur die E-Mail-Adresse des Reporters herausfinden, übernimmt aber am Ende sein gesamtes Account bei ihrem Mobilfunk-anbieter mit Hilfe einer einfachen Täuschung, die wiederum Hilfsbereitschaft beim angerufenem Hotline-Mitarbeiter erzeugt.
https://youtu.be/lc7scxvKQOo

03 Gravoc auf YouTube (Englisch)

In dem animierten Kurzklipp geht es um die typischen Eckpunkte, die man zur Vermeidung von Social Engineering wissen sollte. Der Angriff erfolgt meist über Kanäle, die man zunächst nicht im Blick hat.
https://youtu.be/Vo1urF6S4u0


COMMERZBANK