COMMERZBANK
Die Bank an Ihrer Seite

CEO-/CFO-Fraud aus Sicht der Bank

Düsseldorf | 6. Juli 2016

Was ist ein CEO-/CFO-Fraud:

- Eine gefälschte, scheinbar interne Mail weist einen Mitarbeiter an, eine Transaktion durchzuführen. Die Weisung kommt meist vom Management und avisiert einen Anruf, z. B. den eines betrauten Anwalt.
- Eins von vielen uns bekannten Szenarien, mit denen der Mitarbeiter getäuscht werden soll, ist eine anstehende Fusion, die aufgrund der Börsennotierung des eigenen Unternehmens streng vertraulich ist.
- Angepasste Modi Operandi, z. B. Strafzahlungen in der Automobilzulieferindustrie oder die Steuerfahndung im eigenen Haus, sind weniger verbreitet.
- Es bleibt nicht bei einer E-Mail. Der Mitarbeiter wird gekonnt über zuvor erlangtes Wissen zu seiner Person und zum Unternehmen textlich und telefonisch manipuliert (Druck, Strafzahlung).

Einige Irrtümer:

Auf so etwas fällt bei uns keiner rein.

Wir haben ja gar keinen CEO oder CFO.

Bei uns kann keiner allein unterschreiben.

Solche Summen bekommen wir schnell mit.

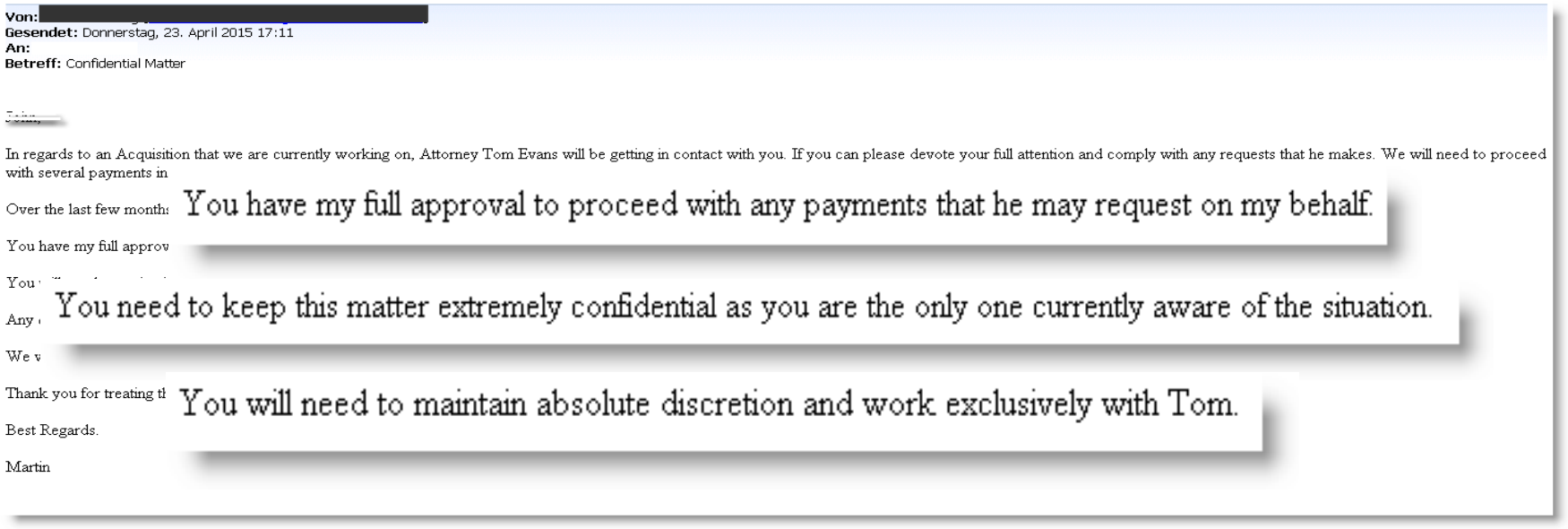
Solche Summen überweist bei uns keiner, ohne zu fragen.

Millionen haben wir sowieso nicht auf dem Konto.

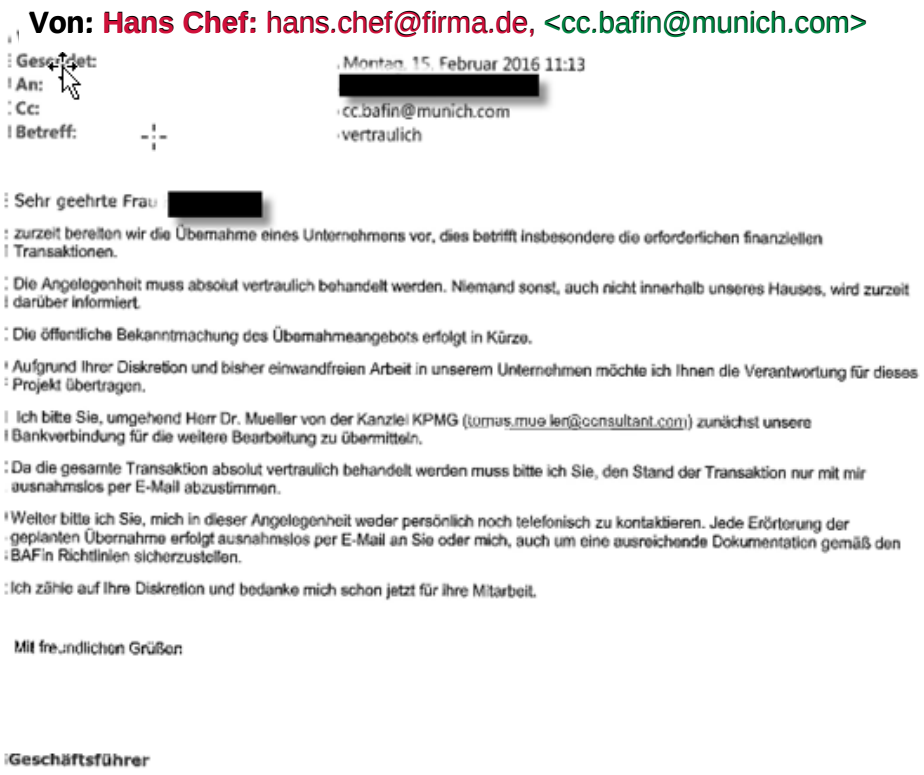
An solche Daten kommen die bei uns ja gar nicht heran.

Fraud-Szenarien in der Praxis: Spear Phishing (CFO-/CEO-Fraud)

- Uns bekannte Vorbereitungszeiten liegen bei ca. zwei Monaten bis eineinhalb Jahren.
- Es wird ein Moment abgewartet, an dem auf Basis öffentlicher Informationen eine fingierte Geschichte gut aufgebaut werden kann. (z. B. Übernahmegerüchte in der Presse)
- Der Betrug wird meist dann begonnen, wenn bekannt ist, dass notwendige Ansprechpartner für eine Rückversicherung innerhalb der Firma nicht erreichbar sind.
- E-Mail-Adressen werden gekonnt vorgetäuscht oder schlicht gefälscht.



Fraud-Szenarien in der Praxis: Spear Phishing (CFO-/CEO-Fraud)



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

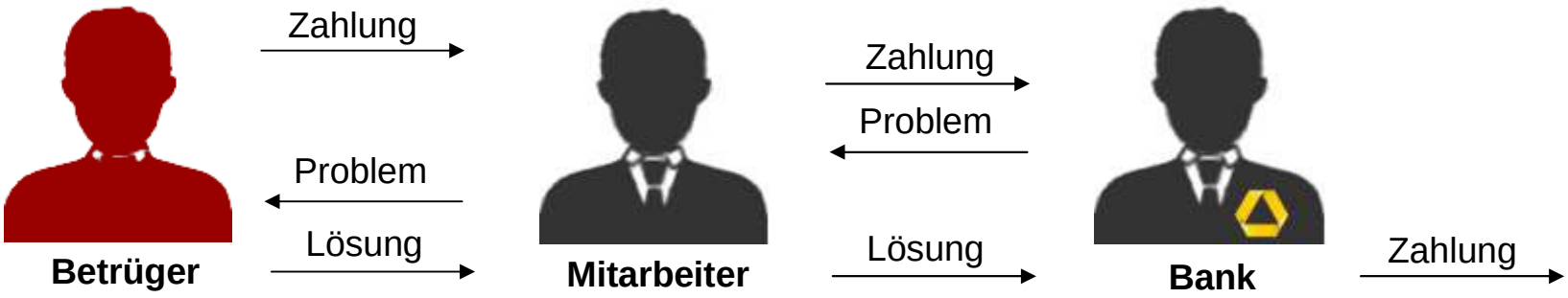
Geschäftsführer

- …zurzeit bereiten wir eine Transaktion vor … insbesondere die … 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.
- …weder persönlich noch telefonisch…kontaktieren.
- Jede Erörterung…ausnahmslos per E-Mail … um eine ausreichende Dokumentation gemäß den BAFin Richtlinien sicherzustellen.

Der Fraud setzt gezielt auf Ihre Hilfsbereitschaft und Ihre Beziehung zu Ihrer Hausbank.

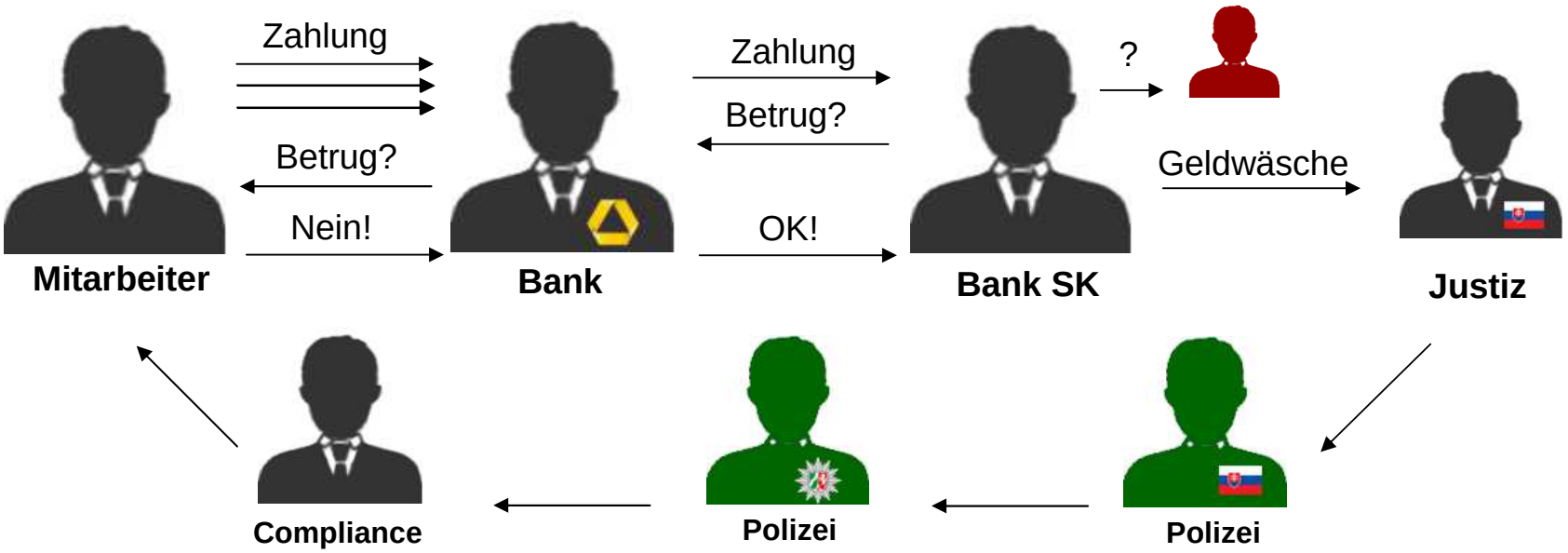
1. Der vermeintliche Chef betraut den Mitarbeiter unter absoluter Vertraulichkeit mit einer Aufgabe. Er soll einem Dritten (Anwalt, KPMG, PWC) alle notwendigen Informationen per Mail mitteilen.
2. Der Mitarbeiter wird danach von der dritten Person kontaktiert, geschickt beruhigt und manipuliert. Ziel ist die Erlangung weiterer Informationen (Limite, Autorisierungen, notwendige Unterschriften)
3. 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.
4. Der uns als Bank bekannte und vertraute Mitarbeiter beauftragt die Zahlung mit der gebotenen Dringlichkeit. Rückfragen werden meist aufgrund der Vertraulichkeit nicht beantwortet.

Der Fraud setzt gezielt auf Ihre Hilfsbereitschaft und Ihre Beziehung zu Ihrer Hausbank.



5. Probleme werden mit dem vermeintlichen Chef geklärt. Nicht autorisierte Unterschriften sollen nun z. B. auf der Basis des Handelsregisters autorisiert werden.
6. 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.
7. Verlangte Absicherungen und Bestätigungen werden geliefert.
8. 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.

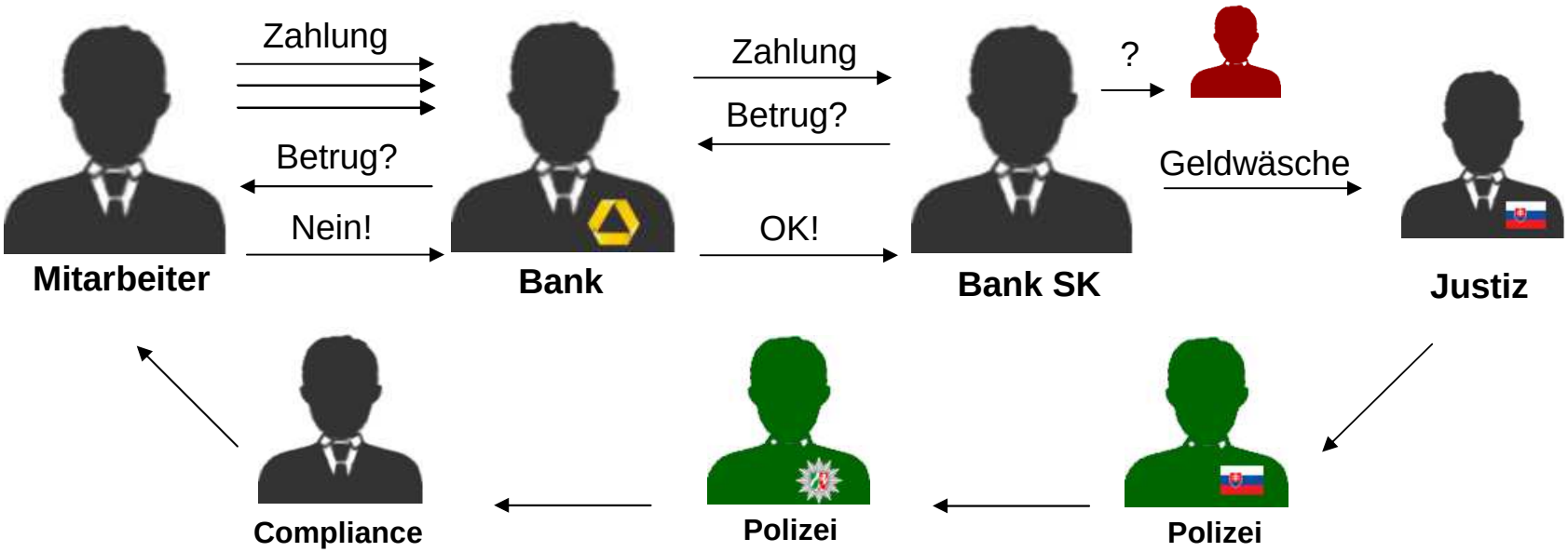
Der Fraud setzt gezielt auf Ihre Hilfsbereitschaft und Ihre Beziehung zu Ihrer Hausbank.



9. 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.

Der Fraud setzt gezielt auf Ihre Hilfsbereitschaft und Ihre Beziehung zu Ihrer Hausbank.



9. 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.

COMMERZBANK

Der Fraud setzt gezielt auf Ihre Hilfsbereitschaft und Ihre Beziehung zu Ihrer Hausbank.

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

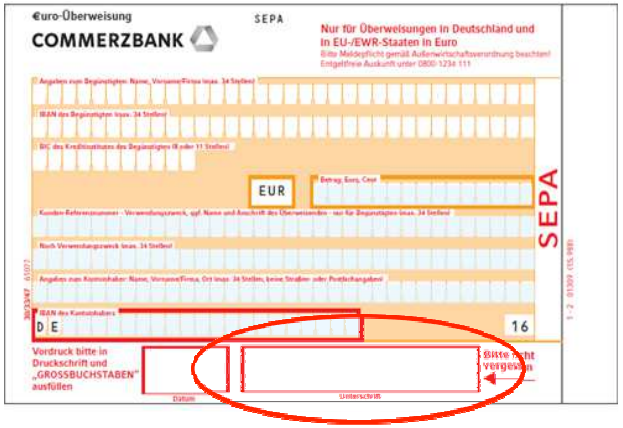
Selbst die Rückfrage der eigenen Compliance-Abteilung im Unternehmen wird mit dem Verweis auf die gebotene Vertraulichkeit abgewiesen.

COMMERZBANK

Fraud-Szenarien in der Praxis: Unsere Kenntnisse zum CFO-Fraud/CEO-Fraud

- Auf die erste E-Mail folgt der avisierte Anruf.
- Auch das Vortäuschen ganzer Telefon- und Videokonferenzen ist uns bekannt.
- Die eventuell angezeigte Rufnummer in Ihrem Telefon-Display ist über „Spoofing“ fälschbar.
- Von Ihnen oder der Bank verlangte Dokumente werden in der Regel auch gefälscht geliefert (Ausweiskopien, Fusionsverträge etc.)
- Der Betrug wird aus sicherer Entfernung per Anruf so oft wiederholt, bis die Täuschung durch Sie entdeckt wird.
- Überweisungen finden meist im ersten oder spätestens zweiten Schritt in den asiatischen Raum statt. Die Anweisungen werden oft kurz vor 12 Uhr MEZ initiiert und es wird meist eine gleichtägige Valuta verlangt.
- Auch Stimmen sind imitierbar, teils mit elektronischer Unterstützung.
- Praxisfall 1: Es rief laut Aussage des Mitarbeiters der CFO der eigenen Holding persönlich an und der Mitarbeiter meinte, ihn an der Stimme erkannt zu haben. Die eingeschaltete Revision war vor Ort, als weitere Anrufe des Betrügers folgten und man konnte die Ähnlichkeit der Stimme bestätigen.
- Praxisfall 2: Der Treasurer in einer gerade aufgekauften Firma erhielt den Anruf vom vermeintlichen Vorstand. Er glaubte ebenfalls, ihn an der Stimme erkannt zu haben, da dieser ihn vor drei Wochen erst angerufen und zum Firmenjubiläum gratuliert hatte. Beide Anrufe waren vorgetäuscht.

CEO-/CFO-Fraud ist keine Frage der Sicherheit im Online Banking! Der Betrüger bedient sich meist des Faxauftrags.



- Eine Unterschrift ist leicht nachzumachen. Eine gute Fälschung hält im Tagesgeschäft vielleicht einer Sichtprüfung stand.
- Beim Betrug im beleghaften Zahlungsverkehr täuscht der Täter die Identität des Kunden vor.

Die digitale Signatur:

```
30460221009e0339f72c793a89e664a8a932
df073962a3f84eda0bd9e02084a6a9567f75
aa022100bd9cbaca2e5ec195751efdfac164
b76250b1e21302e51ca86dd7ebd7020cdc06
01
```

- Eine digitale Signatur ist mit technischen Mitteln nicht „imitierbar".
- Die Täter versuchen, den Kunden den betrügerischen Zahlungsvorgang selbst auslösen zu lassen, oder lassen sich vom Kunden Zugang zu seinem System gewähren.

COMMERZBANK

Wie können sich Unternehmen schützen?

- Schulen Sie Ihre Mitarbeiter im Umgang mit Social Media.
- Führen Sie in Ihrer Firma Maßnahmen zur Prävention und Aufklärung gegen Betrugsversuche durch.
- Identifizieren Sie risikobehaftete Prozesse und stellen Sie Kontrollen sicher. Halten Sie diese immer ein.
- Prüfen Sie jeden überraschenden Sachverhalt mit dem gesunden Menschenverstand.
- Rückversicherung bei Unsicherheit: Eine telefonische Rückversicherung bei einem bekannten Ansprechpartner oder Vorgesetzten im Unternehmen, bei der Bank oder beim Geschäftspartner kann den Betrug verhindern. Nutzen Sie dafür nicht den gleichen Kanal (z.B. Anruf statt E-Mail).

Bankfachliche Fragen:

- Haben Mitarbeiter in Ihrer Firma Einzelunterschriftsvollmachten?
- Dürfen Mitarbeiter in Ihrer Firma unlimitiert unterschreiben?
- Haben Sie bei der Bank ein Fax-/E-Mail-Revers für Aufträge hinterlegt?
- Haben Sie bei Ihrer Bank die Sperrung beleghafter Zahlungsaufträge beauftragt?
- Sind öffentlich bekannte Unterschriften auch für die Autorisierung bei der Bank hinterlegt?

Was, wenn es doch passiert ist?

Was tun, wenn man Opfer geworden ist?

› Kontaktieren Sie **sofort** Ihre Bank, insbesondere wenn die Zahlung noch „frisch“ ist.

– Zahlungen werden nur dann garantiert zurückgegeben, wenn sie dem Empfängerkonto noch nicht gutgeschrieben sind.

– Zahlungen werden unter Umständen auch dann noch zurückgegeben, wenn über das Geld noch nicht verfügt wurde (good will).

– Ein erfolgreicher Überweisungsrückruf ist nur möglich, wenn er zeitnah erfolgt.

– Auch bei abgewendeten Betrugsversuchen teilen Sie uns bitte die Empfängerbankverbindung mit

– Klären Sie im Betrugsfall und im Fall des Betrugsversuchs mit Ihrem Management, ob Sie - wie von uns empfohlen - eine Anzeige bei der Polizei stellen möchten.

Was kann die Commerzbank im Fall des Falles für Sie tun?

› Unmittelbarer Überweisungsrückruf

› Inanspruchnahme der weltweit guten Vernetzung mit internationalen Banken

› Vermittlung von Kontakten zu Ermittlungs-behörden im ganzen Bundesgebiet, die auf Cybercrime bzw. Wirtschaftskriminalität spezialisiert sind.

› Empfehlungen für die weitere Vorgehensweise je nach Betrag, Land und Sachverhalt.

Fazit

- Cybercrime im Firmenkundengeschäft ist nicht „industrialisiert“ wie im browserbasierten Banking. Hohe Diversität macht das Schreiben von Malware zu „teuer“. Daher wird der Mitarbeiter manipuliert.
- Die Attacken erfolgen meist über Social Engineering.
- Die Schulung von Mitarbeitern, gesicherte Prozessschritte, die Prüfung eines merkwürdigen Sachverhalts mit dem gesunden Menschenverstand und die Rückversicherung bei bekannten Ansprechpartnern helfen, einen Betrug zu verhindern.
- Der Schaden durch einen zu spät bemerkten Betrug kann unter Umständen auch nach Geldabgang noch abgewendet werden, wenn Sie nicht zögern und sofort Ihre Bank informieren. Dann kann ein Überweisungsrückruf eingeleitet werden.

Commerzbank AG

GS-OS IS Security Consulting & Research

MSB CTS & FI, Product Management Cash Services, Fraud Prevention

E-Mail: msb.sicherheit@commerzbank.com
(Informieren Sie uns im Betrugsfall zusätzlich zu Ihrem Berater)

Geschäftsräume:
Kaiserstraße 16
60311 Frankfurt/Main
www.commerzbank.de

Postanschrift:
60261 Frankfurt/Main
Tel.: +49 69 1362-0

Disclaimer

Diese Präsentation wurde von der Commerzbank AG vorbereitet und erstellt. Die Veröffentlichung richtet sich an professionelle und institutionelle Kunden.

Alle Informationen in dieser Präsentation beruhen auf als verlässlich erachteten Quellen. Die Commerzbank AG und/oder ihre Tochtergesellschaften und/oder Filialen (hier als Commerzbank Gruppe bezeichnet) übernehmen jedoch keine Gewähr-leistungen oder Garantien im Hinblick auf die Genauigkeit der Daten.

Die darin enthaltenen Annahmen und Bewertungen geben unsere beste Beurteilung zum jetzigen Zeitpunkt wieder. Sie können jederzeit ohne Ankündigung geändert werden. Die Präsentation dient ausschließlich Informationszwecken. Sie zielt nicht darauf ab und ist auch nicht als Angebot oder Verpflichtung, Aktien oder Anleihen zu kaufen oder zu verkaufen, die in dieser Präsentation erwähnt sind, wahrzunehmen.

Die Commerzbank Gruppe kann die Informationen aus der Präsentation auch vor Veröffentlichung gegenüber ihren Kunden benutzen. Die Commerzbank Gruppe oder ihre Mitarbeiter können ebenso Aktien, Anleihen und dementsprechende Derivate besitzen, kaufen oder jederzeit verkaufen, wenn sie es für angemessen halten. Die Commerzbank Gruppe bietet interessierten Parteien Bankdienstleistungen an. Die Commerzbank Gruppe übernimmt keine Verantwortung oder Haftung jedweder Art für Aufwendungen, Verluste oder Schäden, die aus dieser Präsentation entstehen oder in irgendeiner Art und Weise im Zusammenhang mit der Nutzung eines Teils dieser Präsentation stehen.