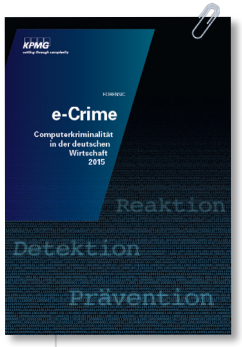
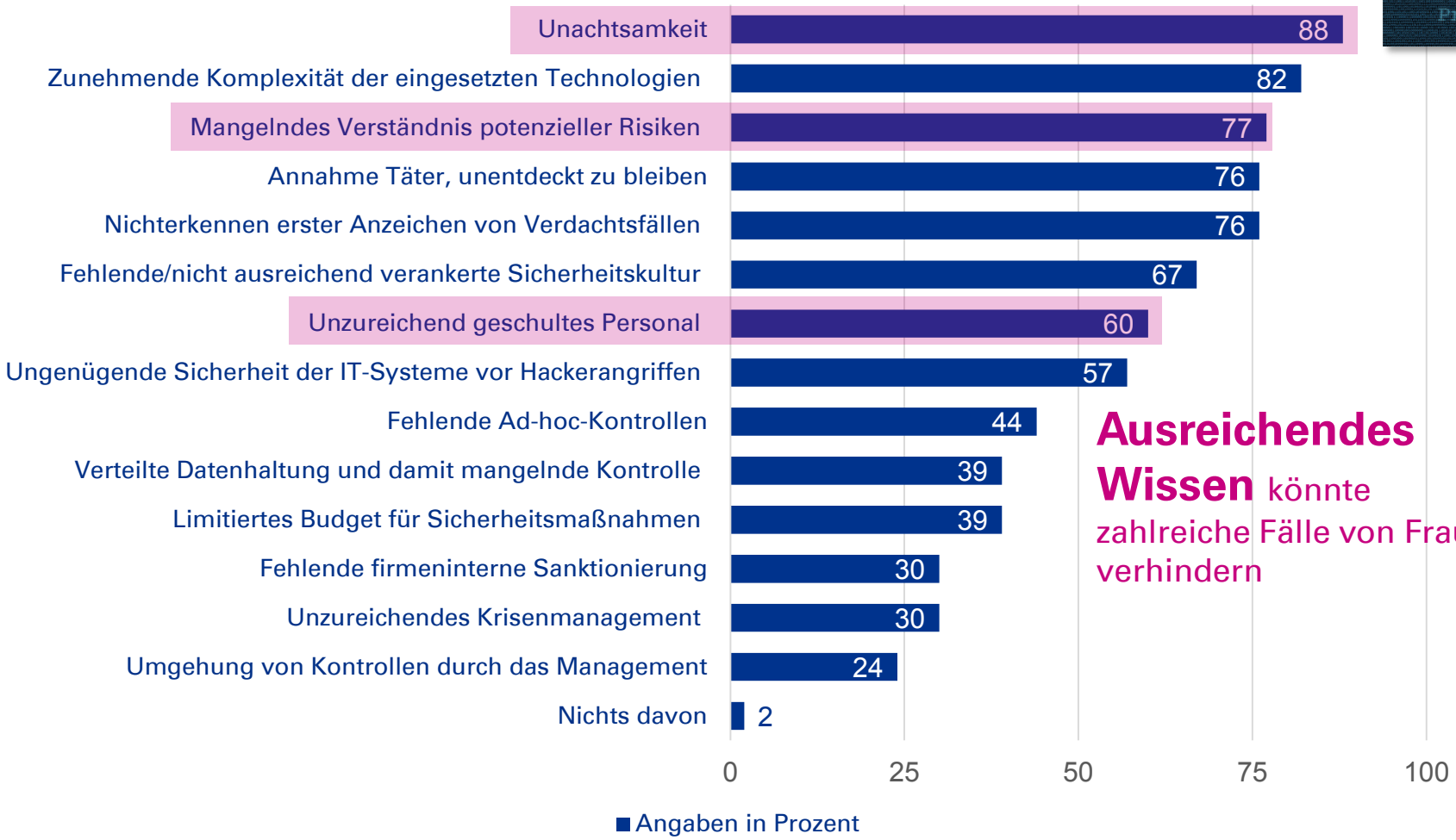
LKA NRW, Präventionstag CEO - Fraud

Alexander Geschonneck
Partner, Leiter Forensic Investigation
KPMG AG Wirtschaftsprüfungsgesellschaft

Düsseldorf, 6. Juli 2016

Begünstigtende Faktoren für Cybercrime





Ausreichendes Wissen könnte zahlreiche Fälle von Fraud verhindern

Wieso funktioniert Social Engineering?

Social Engineering [ˈsəʊʃl ˌɛndʒɪˈnɪərɪŋ] (engl. eigentlich „angewandte Sozialwissenschaft“, auch „soziale Manipulation“) nennt man zwischenmenschliche Beeinflussungen mit dem Ziel, bei Personen bestimmte Verhaltensweisen hervorzurufen, sie zum Beispiel zur Preisgabe von vertraulichen Informationen, zum Kauf eines Produktes oder zur Freigabe von Finanzmitteln zu bewegen. Social Engineers spionieren das persönliche Umfeld ihres Opfers aus, täuschen Identitäten vor oder nutzen Verhaltensweisen wie Autoritätshörigkeit aus, um geheime Informationen oder unbezahlte Dienstleistungen zu erlangen. Meist dient Social Engineering dem Eindringen in ein fremdes Computersystem, um vertrauliche Daten einzusehen; man spricht dann auch von **Social Hacking** ['hækɪŋ] (vgl. Hacker). *(wikipedia.de)*

Funktioniert wegen

- **Neugierde**
- **Angst**
- **Sorglosigkeit**

Studie: Fast jeder zweite Nutzer verrät für Schokolade sein Passwort

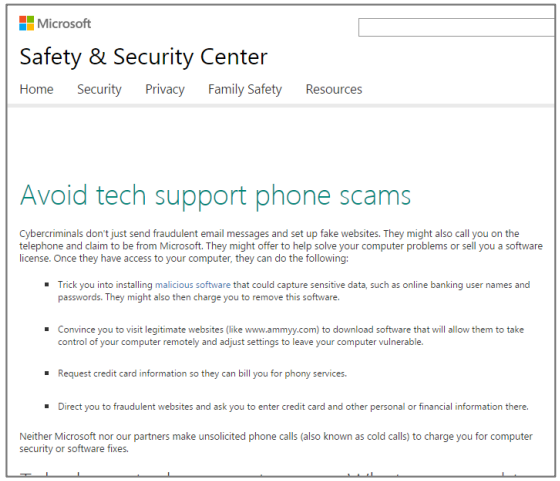
Technology Review 28.06.2016 08:03 Uhr – Sascha Mattke vorlesen

Users Really Do Plug in USB Drives They Find

Matthew Tischer[†] Zakir Durumeric[†,*] Sam Foster[†] Sunny Duan[†]
Alec Mori[†] Elie Bursztein[◇] Michael Bailey[†]

University of Illinois, Urbana Champaign [†] University of Michigan [*] Google, Inc.

Beliebte Social Engineering-Maschen



Von: CEO einer ausländischen Tochtergesellschaft

An: Führungskraft im mittleren Management

Inhalt: […] geheime Übernahme der Vorwand GmbH in China […] Vorsprung auf unseren stärksten Wettbewerber Plausibel AG […] Bitte um Unterstützung bei der Abwicklung […] Überweisung von EUR 1.341.200 auf das Konto 23432509 bei der Chinese Fraudster Bank (BIC CNFBCNSJ) […] Bestätigung über Herrn Müller (Telefonnummer +49 1805 764367) […]

„Hello, this is Microsoft“

Kriminelle kontaktieren Mitarbeiter per Telefon und geben sich als Mitarbeiter z.B. von Microsoft aus. Die Mitarbeiter werden z. B. zur Installation eines Updates aufgefordert.

Das „Update“ ist jedoch eine Schadsoftware, die Zugriff auf das System (und ggf. das Netzwerk des Unternehmens) verschafft.

Bitte durchstellen …

Ein Anrufer bittet, zu einem bestimmten Kollegen durchgestellt zu werden. Vorgeblich handelt es sich um ein Projekt, an welchem dieser beteiligt ist.

Die so gewonnen Informationen werden von Kriminellen verkauft, oder zur Verfeinerung von anderen Angriffen genutzt (Fake President).

CEO an Mitarbeiter

Die momentan wohl beliebteste Masche: Täter geben sich als eine oder mehrere Personen im Unternehmen aus.

So können sei z. B. Zahlungen anweisen oder ebenfalls Informationen (inklusive vertraulichen Dokumenten) abgreifen.

http://www.heise.de/newsticker/meldung/Betrugsmasche-aufgewaermt-Falsche-Microsoft-Techniker-am-Telefon-2718299.html

Spear Phishing (targeted Phishing)

- Spear Phishing ist Phishing gegen ausgesuchte lohnende Ziele, beides fällt unter den Komplex „Social Engineeering“
- Höhere Erfolgsquote für Angreifer, da Zielpersonen sehr gezielt adressiert werden können (häufig geht Profiling der Opfer voraus)
- „Whaling“ ist Spear Phishing gegen besonders exponierte Ziele (bspw. CEO, CFO, höheres Management)

Weitere (auch analoge) Formen von Social Engineering:

- Pretexting (Betrug mittels eines erfundenen Szenarios)
- Diversion theft (Z.B. Abgreifen von Post-Lieferungen)
- Baiting (Betrug mittels eines Köders – z.B. interessanter USB-Stick)
- Quid pro quo (Informationen gegen vermeintlich echte Gegenleistungen)
- Tailgating (Problem der physischen Sicherheit)

Aktuelle Betrugsmaschen im Zahlungsverkehr

Fake President/CEO Fraud	Payment Diversion	Fake Identity Fraud
Zahlungsaufforderung durch als Vorstand getarnte Betrüger	Gefälschte Mitteilung über geänderte Kontoinformationen	Bestellung oder Betrug mit Hilfe falscher Identitäten

Österreichischer **Mittelständler** wurde im **Dezember 2015** Opfer mit einem Schaden von **50 Mio. €**

http://www.news.at/a/facc-betrug-fake-president-trick-millionen

Beispiel einer „Fake President" E-Mail

Authentischer Absender durch E-Mail-Spoofing, ähnlich aussehende Adresse oder Übernahme des E-Mail-Accounts

Bevollmächtigter Adressat für die Durchführung von Zahlungen wird vorher recherchiert (*Social Engineering*)

Geheimniskrämerei schmeichelt dem Empfänger (*Kreis der Eingeweihten*) und verhindert eigene Nachforschungen

Von: CEO einer ausländischen Muttergesellschaft

An: Führungskraft im mittleren Management

Inhalt: […] geheime Übernahme der Vorwand GmbH in China […] Vorsprung auf unseren stärksten Wettbewerber Plausibel AG […] Bitte um Unterstützung bei der Abwicklung […] Überweisung von EUR 1.341.200 auf das Konto 23432509 bei der Chinese Fraudster Bank (BIC CNFBCNSJ) […] Bestätigung über Herrn Müller (Telefonnummer +49 1805 764367) […]

Plausibilität wird durch die Recherche im Internet, Social Engineering oder auch über das Fälschen von Webseiten erreicht

Sozialer Druck durch die persönliche Adressierung des Vorstandes

Falscher Ansprechpartner (*externe Berater oder Treuhänder*) bestätigt bei Kontakt das Anliegen, ruft auch gern selbst an

KPMG

Ansatzpunkte zur Prävention

Schulung, Wachsamkeit und Meldung

Mitarbeiter (und Führungskräfte!) sollten regelmäßig in aufmerksamem Handeln geschult werden.

Mögliche Inhalte:

- Schutz von Zugangsdaten und Passwörtern
- Clean Desk Policy
- Sichere Entsorgung von vertraulichen Inhalten
- Gefahren von Diebstahl (Laptop in der Bahn)
- Social Engineering

Zudem:

Einrichtung eines adäquaten Meldesystems für Vorfälle dieser Art (Meldestrategie, Whistleblower-Hotline etc.)

Datenanalyseroutinen, um verdächtige Zahlungen zu erkennen und ggfls.. zu verhindern.

Empfehlungen beim Umgang mit E-Mail

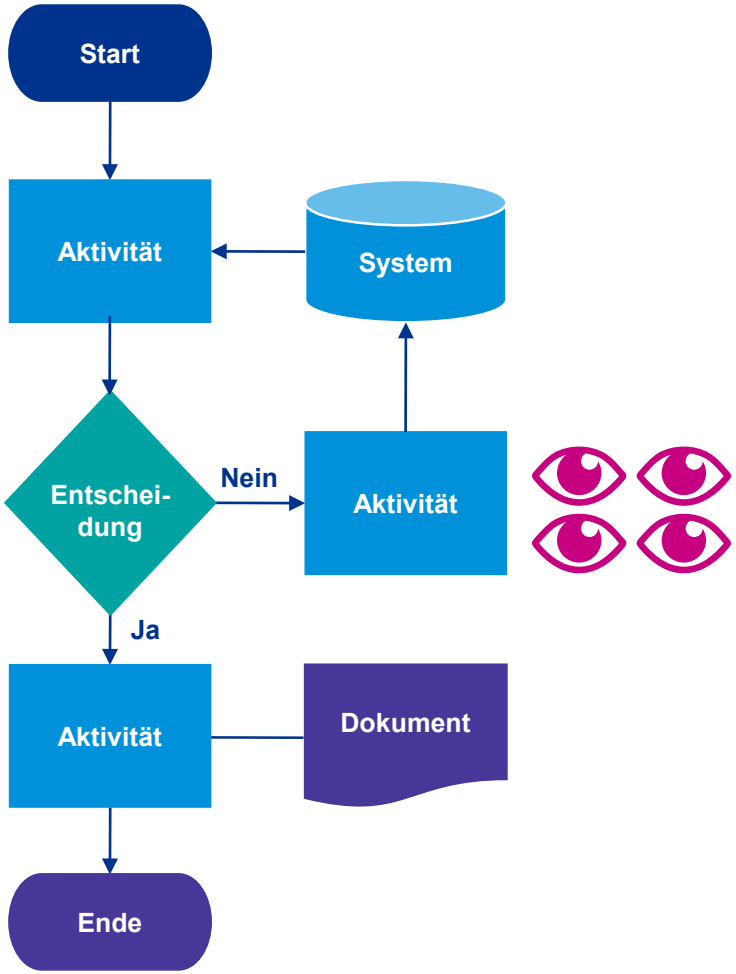
- Ist die Identität des Absenders einer E-Mail nicht sichergestellt, sollte man stets misstrauisch sein.
- Bei Anrufen sollten auch scheinbar unwichtige Daten nicht sorglos an Unbekannte weitergegeben werden, da diese die so erhaltenen Informationen für weitere Angriffe und Betrugsdelikte nutzen können.
- Bei Antworten auf eine E-Mail-Anfrage sollten unter keinen Umständen persönliche oder finanzielle Daten preisgegeben werden, egal von wem die Nachricht zu kommen scheint.
- Keine Links aus E-Mails verwenden, die persönliche Daten als Eingabe verlangen. Stattdessen die URL selbst im Browser eingeben. URL auf Sinnhaftigkeit prüfen.
- Bei Unklarheit über die Echtheit des Absenders diesen nochmals telefonisch kontaktieren, um die Authentizität der E-Mail zu überprüfen. Die Telefonnummer sollte nicht aus der E-Mail stammen.

Sichere Unternehmensprozesse

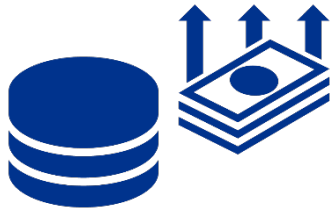
Sichere Prozesse – „by design“ – bieten den besten Schutz gegen Schäden durch Social Engineering & Co.

Insbesondere:

- Vier-Augen-Prinzip
- Verpflichtende Genehmigungsschritte
- Effektives Berechtigungsmanagement
- Automatische Überwachung auf Prozessabweichungen

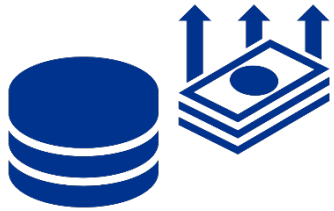


Schwachstellen



Schwachstellen	Auswirkungen
Dezentrale Stammdatenpflege	Sensible Stammdatenfelder wie Bankkonten von Lieferanten werden ohne Verifikation geändert
Fehlende Transparenz über Bankkonten	Keine Möglichkeit der Kontrolle über Zugriffsrechte und Kontobewegungen
Dezentraler Zahlungsverkehr	Systemimmanente Schwachstellen wie Know-How und lokale Electronic Banking-Systeme
Heterogene Formate & Prozesse	Prohibitiv hoher Aufwand für standardisierte und automatisierte Kontrollen
Ungeklärte Zuständigkeiten (End-to-End)	Treasury vs. Buchhaltung vs. IT mit entsprechenden Regelungslücken
Manuelle Zahlungen	i.d.R. außerhalb des Regelprozesses; Einfallstor für eine Reihe von Betrugsmaschen (häufig eilig)
Manuelle Kontoauszugsverarbeitung	Deutlich verringerte Wirksamkeit der ex-post Kontrolle

mögliche Lösungen



Schwachstellen	Lösungen
Dezentrale Stammdatenpflege	Zentrale Stammdatenpflege (2-Faktor Authentifizierung)
Fehlende Transparenz über Bankkonten	Bank Account Management System – zentrale Verwaltung der Bankkonten
Dezentraler Zahlungsverkehr	Zentralisierung des Zahlungsverkehrs (Payment Hub, Payment Factory, Inhouse Bank); zentrale Datenbank f. Fraud-Versuche
Heterogene Formate & Prozesse	Format- & Kommunikationskanalstandardisierung, Einheitliche Prozesse (Stammdaten-Pflege, externes Zahlen)
Ungeklärte Zuständigkeiten (End-to-End)	Treasury*: strategisch*, IT: *Sicherheit*, Buchhaltung / SSC: *operativ; 4-Augen Prinzip für ALLE Zahlungen und Definition der durchzuführenden Checks*
Manuelle Zahlungen	Begrenzung auf vordefinierte, kritische Einzeltransaktionen mit gesonderten Kontrollen
Manuelle Kontoauszugsverarbeitung	Automatische Kontoauszugsverarbeitung und Nutzung von Near Real-Time Statusnachrichten

Reaktion bei einem Fake CEO-Betrugsvorfall

Auch wenn die Identifikation von Tätern schwierig ist, sollte eine Untersuchung durchgeführt werden um aus dem Vorfall zu lernen

Bei Verdacht auf Manipulation von IT-Systemen müssen Daten für eine Untersuchung rechtzeitig gesichert werden.

Was kann man tun :

- Sofortiger Kontakt zur Bank und Anzeige bei der Polizei
- Untersuchung des Vorfalls und Sachverhaltsdarstellung für die juristische Weiterverfolgung
- Forensische Datensicherung und -analyse der relevanten IT-Systeme (auch Buchhaltung)
- Kreditoren- und Zahlungsstromanalyse zur Identifikation weiterer, auffälliger Transaktionen
- Vermittlung psychologischer Expertise zur Nachbetreuung involvierter Mitarbeiter.

Fazit

- Schulung und Sensibilisierung der Mitarbeiter
- Bewertung der eigenen Unternehmenskultur
- Angemessene Richtlinien
- Regelmäßige Audits
- Angemessene technische Schutzmaßnahmen
- Streamlining der Zahlungsprozesse
- Regelmäßige Kontrolle der Zahlungsströme

Alexander Geschonneck
Partner, Head of Forensic Deutschland
T +49 30 2068 1520
ageschonneck@kpmg.com

KPMG AG
Wirtschaftsprüfungsgesellschaft
Klingelhöferstraße 18
10785 Berlin

www.kpmg.de/forensic

Über unsere KPMG Notruf-Hotline bei Verdacht auf Wirtschaftskriminalität und Cybercrime erreichen Sie unsere Forensic-Experten rund um die Uhr telefonisch:

0180 KPMG FOR*
(+49 1805 764367*)

*Telefonkosten: Festnetz 14ct/min; Mobilfunknetze 42ct/min

kpmg.com/socialmedia

Download on the App Store

kpmg.com/app