KPMG
cutting through complexity

ÖGWT
IHR SERVICE-NETZWERK

FEEL FREE

A NEW APPROACH TO CYBER SECURITY

Cyber Crime Risiko „Fake President“ Angriff

Cyber Security Breakfast Vol. 1

Georg BEHAM

Diese Präsentation ist online unter
www.oegwt.at → Veranstaltungen → Oberösterreich
verfügbar.

Willkommen im ÖGWT CLUB OÖ!

Sehr geehrte Frau Kollegin! Sehr geehrter Herr Kollege!

Wir laden Sie sehr herzlich zum ÖGWT CLUB Oberösterreich ein.

THEMA — **Cyber Security**

Cyberangriffe erleben aktuell eine Hochkonjunktur, wie uns das Geschehen in der Wirtschaft und Medienberichte zeigen. Besonders Angriffe, die Gelddiebstahl von Unternehmen zum Ziel haben, steigen stetig an. Oft ist das Vorgehen dabei technisch sehr komplex, es wird Schadsoftware gezielt erzeugt und beim Opfer platziert.

Bei Angriffen, die den Mustern „Fake President“ und „Business Mail Compromisation“ entsprechen, wird die Technik oft nur zur Vorbereitung verwendet. Anschließend wird das Opfer, meist Mitarbeiter mit Zahlungsberechtigung im Rechnungswesen oder im Einkauf, unter Vortäuschung falscher Tatsachen zu einer Finanztransaktion geleitet. Der Schaden ist enorm und die Chance, die Täter zu fassen, geht gegen Null.

Im Rahmen unseres ÖGWT-Clubs zeigen wir Ihnen aktuelle Beispiele und stellen Ihnen praktische Schutzmaßnahmen vor. Wir laden Sie ein, gemeinsam mit einem Experten und Sachverständigen für IT-Sicherheit, zu diskutieren.

REFERENT — Georg Beham, MSc, KPMG

TERMIN und ORT

Zentralraum Linz — **8. März 2016**, 18:30 Uhr
Veranstaltungszentrum Sparkasse OÖ,
Taubenmarktarkade, Promenade 11-13, 4020 Linz
(während der Veranstaltung stehen die Parkplätze in der Tiefgarage der Sparkasse zur Verfügung)

SPARKASSE Oberösterreich

ANMELDUNG — Zur reibungslosen Vorbereitung bitten wir Sie, sich bis 3.3.2016 via E-Mail (akremminger@kpmg.at) oder Fax anzumelden.

FORTBILDUNG — Diese Veranstaltung ist auf die Fortbildungsverpflichtung für Steuerberater ab 2012 laut § 3 (5) WT-ARL und gem § 68 (3) BiBuG mit 2 Stunden anrechenbar.
Eine Teilnahmebestätigung wird aufgrund Ihrer Anmeldung ausgestellt und ist bei der Veranstaltung erhältlich.

Herzlichst Ihre ÖGWT – Ihr Servicenetzwerk

WP/StB Mag. Dr. Gerd-Dieter Mirtl
ÖGWT Landesleiter Oberösterreich

WP/StB Dr. Verena Trenkwalder
ÖGWT Vizepräsidentin

Breaking News

Gefälschte E-Mails: US-Manager überweist 17 Millionen Dollar an Betrüger

Mit gefälschten E-Mails haben Internetbetrüger einen amerikanischen Top-Manager dazu gebracht, umgerechnet 15 Millionen Euro auf ein Bankkonto in China zu überweisen. Das Opfer glaubte, auf Anweisung seines Chefs zu handeln.

Breaking News

FACC: Betrug mit Fake-President-Trick

Wie der Luftfahrt-Zulieferer um 50 Millionen Euro erleichtert wurde

© Bild: APA/Daniel Scharinger

Die Mail kam von ganz oben, vom Vorstandschef persönlich. Unter dem Siegel der strengsten Verschwiegenheit wurde eine Mitarbeiterin des österreichischen Luftfahrtzulieferers FACC während der Weihnachtstage angewiesen, 50 Millionen zu überweisen. Das Geld, so stand es in der Nachricht, sollte für eine geheime Firmenübernahme im Ausland verwendet werden. Also: geheime Kommandosache, kein Wort zu niemandem.

© 2016 KPMG Advisory GmbH, österreichisches Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Printed in Austria. KPMG und das KPMG-Logo sind eingetragene Markenzeichen von KPMG International.

Breaking News

Baden-Württemberg

LANDESKRIMINALAMT

Warnmeldung für Firmen

PRESSESTELLE LKA BW
TELEFON 0711 5401-2012, -3012 ODER -3212, FAX 0711 5401-1012
E-MAIL PRESSESTELLE-LKA@POLIZEI.BWL.DE, INTERNET WWW.LKA-BW.DE

Stuttgart, 17. September 2015

E-Mails vom vermeintlichen Geschäftsführer: LKA warnt Firmen vor Betrugsmasche

Seit kurzem gehen vermehrt Hinweise auf eine seit längerem bekannte Betrugsmasche beim Landeskriminalamt Baden-Württemberg ein.
Dabei nutzen die Täter gezielt die Abwesenheit der Geschäftsführung aus, um mit gefälschten E-Mail-Absenderangaben an Firmengelder zu gelangen. Mit dieser Masche versuchen die Betrüger Firmen zu täuschen, teilweise kam es bereits zu Überweisungen und Schäden von mehreren Millionen Euro.

Breaking News

ONLINE SICHERHEIT.AT

Kinder & Jugendliche | Eltern | Lehrende | Konsument/innen | Generation 60plus | Mitarbeiter/innen | **Unternehmer/innen** | Öffentliche Verwaltung | Sicherh forschu

Home > Unternehmer/innen > News

- Sicherheitsmanagement
- Sicherheitshandbücher
- Sicherheitsnormen
- Weitere Normen und Standards
- Rechtliche Vorgaben
- Industrielle Sicherheit
- E-Government
- E-Business-Statistik
- Rat und Hilfe

04.12.2015

Neue Cyber-Betrugsmasche „fake president"

Eine neue Cyber-Betrugsmasche namens „fake president" hätte einem Grazer Unternehmen vor Kurzem fast 1,8 Millionen Euro gekostet. Die Buchhalterin des Betriebs überwies den Geldbetrag auf das Konto einer chinesischen Bank, nachdem eine vermeintlich vom Geschäftsführer stammende E-Mail mit der entsprechenden Anweisung bei ihr eingegangen war. Die gefälschte Nachricht wurde von einer E-Mail-Adresse des Firmennetzwerks abgeschickt und auch sonst als täuschend echt beschrieben.

Der Trick ist laut Polizei relativ neu: Cyberkriminelle hacken das E-Mail-Netz von Unternehmen, um daraufhin Namen und E-Mail-Konten der Geschäftsleitung für ihre Vorhaben nutzen zu können. Die Kriminellen geben zudem vor, das Anliegen sei dringend und geheim – beispielsweise im Zusammenhang mit einem neuen Forschungsprojekt oder einer Betriebsübernahme. So werden die Empfängerinnen und Empfänger der gefälschten Mails daran gehindert, lange zu überlegen oder gar nachzufragen. Zudem ist der Nachrichtentext plausibel und fehlerfrei. Im Falle des Grazer Unternehmens wurde der Betrugsversuch noch rechtzeitig entdeckt. Die Bank konnte die Überweisung stoppen; dem Betrieb entstand kein Schaden.

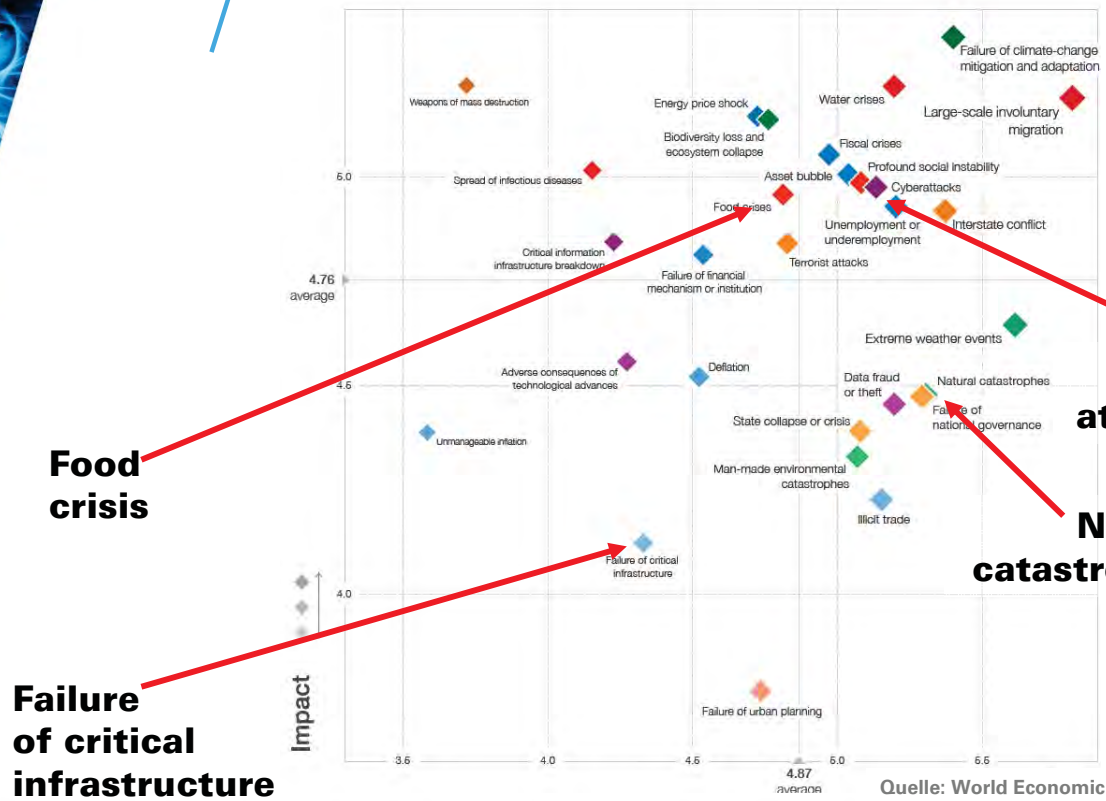
Weitere Informationen:

- zum Artikel auf kurier.at
- Information des Cyber Crime Competence Centers zur Betrugsmasche

Datum der Veröffentlichung: 04.12.2015

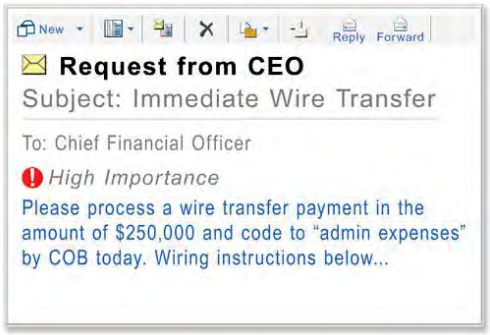
© 2016 KPMG Advisory GmbH, österreichisches Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Printed in Austria. KPMG und das KPMG-Logo sind eingetragene Markenzeichen von KPMG International.

Globale Risiken



Quelle: World Economic Forum Global Risk Report 2016

Cyber Crime Risiko „Fake President" Angriff



Fake-President Angriff

„Ein Betrugsfall, bei dem Täter unter einer falschen Identität versuchen, eine dringende Überweisung auf ein Bankkonto zu veranlassen. Als Grund für diese Überweisungsaufforderung wird meist eine ausstehende Zahlung, eine Anzahlung oder ein anderer wichtiger Grund genannt."

vermehrt „Fake President" und „Business E-Mail Compromise" Betrugsfälle!
Auch in Österreich!

Zahlen des FBI (Oktober 2013 bis August 2015)	
Gesamtanzahl der US-Opfer:	7.066
Gesamtverlust USA:	$ 747.659.840
Gesamtanzahl der Nicht-US-Opfer:	1.113
Gesamtverlust der Nicht-US-Opfer:	$ 51.238.118
Gesamtopfer:	8.179
Gesamtverlust:	**$ 798.897.959**

Die BEDROHUNGS-Akteure

Fake President Akteure

MINOR LEAGUE

HACKTIVISM
HACKING INSPIRIERT DURCH DIE TECHNOLOGIE

MOTIVATION: VERÄNDERNDE LOYALITÄT, NICHT VORHERSEHBAR
AUSWIRKUNG: REPUTATIONSVERLUST, INFORMATIONSVERLUST

DIE INSIDER
MIT VORSATZ ODER UNABSICHTLICH

MOTIVATION: NEID, FINANZIELLE BEREICHERUNG
AUSWIRKUNG: VERTEILUNG ODER ZERSTÖRUNG, INFORMATIONS-DIEBSTAHL, REPUTATIONSVERLUST

ORGANISIERTE KRIMINALITÄT
GLOBAL, KAUM IDENTIFIZIERBAR UND VERFOLGBAR

MOTIVATION: FINANZIELLE BEREICHERUNG
AUSWIRKUNG: INFORMATIONSDIEBSTAHL UND -ABFLUSS

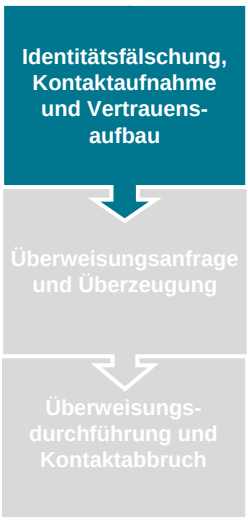
STAATLICHE INTERESSEN
SPIONAGE UND SABOTAGE

MOTIVATION: POLITISCHE, WIRTSCHAFTLICHE UND MILITÄRISCHE INTERESSEN
AUSWIRKUNG: UNTERBRECHUNG ODER ZERSTÖRUNG VON INFORMATIONEN UND INFRASTRUKTUREN, INFORMATIONS-DIEBSTAHL, REPUTATIONSVERLUST

MAJOR LEAGUE

Angriffsszenario „Fake President" Angriff im Detail

- **Wissensaneignung** über den Markt, die Struktur und Kunden des Zielunternehmens via Insider, öffentlich verfügbare Kanäle (Webseiten, Soziale Netzwerke wie Xing, Facebook, LinkedIn) oder die Platzierung von Malware meist durch kriminelle Organisationen.
- Wissen wird zur **Identitätsfälschung** verwendet (Ausgabe als Vorstand, CEO oder vertrauenswürdiger Partner wie Rechtsanwalt, Notar oder Wirtschaftsprüfer).
- Telefonische oder E-Mail **Kontaktaufnahme** mit Mitarbeitern mit Zahlungsbefugnissen (Manager, Buchhalter).



typischer Ablauf einer „Fake President" Attacke

Angriffsszenario „Fake President“ Angriff im Detail

- Die Betrüger verlangen eine **dringende Banküberweisung** einer hohen Summe auf ein Bankkonto im Ausland.
- Verwendung einer Kombination an vertraulichen Informationen, erfundenen Tatsachen und Überzeugungselementen, wie

hohe **D**ringlichkeit

autoritäres Auftreten des vermeintlichen Vorgesetzten

erhöhte **G**eheimhaltung der Transaktion

typischer Ablauf einer „Fake President“ Attacke

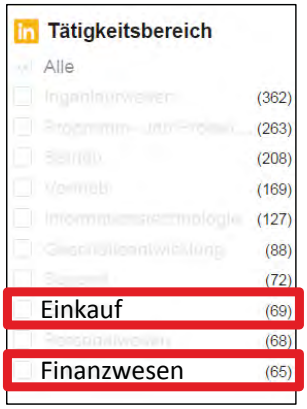
Angriffsszenario „Fake President“ Angriff im Detail

- Veranlassung der Durchführung der **Überweisung** vom getäuschten Mitarbeiter.
- **Bezug des Gelds** von den verwendeten Konten, Kontaktabbruch und Verwischung der Spuren durch den Täter.
- Die **Chance den Täter zu fassen** bzw das Geld zurückzuerhalten, tendiert zu diesem Zeitpunkt **gegen Null**.

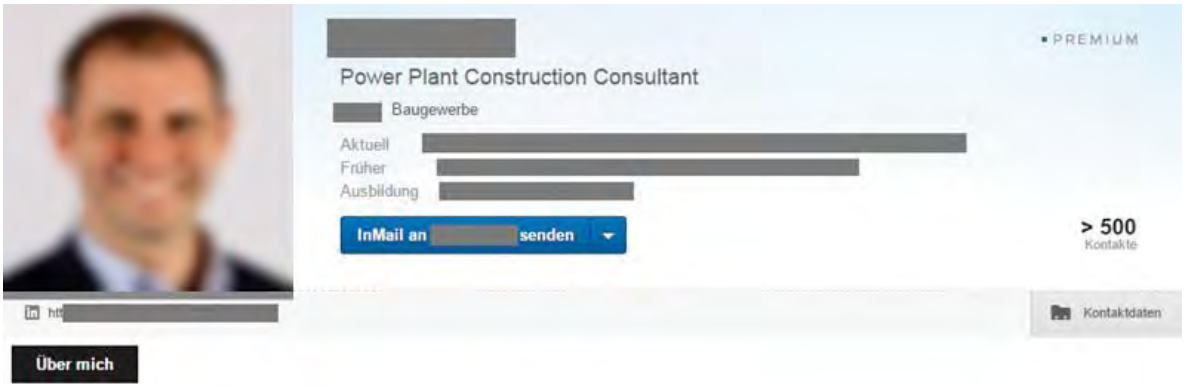
typischer Ablauf einer „Fake President“ Attacke

It´s quite easy!
Abruf öffentlicher Informationen

- Viele **Informationen**, die ein Angreifer für einen Fake President Angriff benötigt, sind **öffentlich** im Internet abrufbar, zB durch Durchsuchen von:
  - Homepage des Zielunternehmens
  - Sozialen Netzwerken
    - bieten oftmals eine Vielzahl an Filtermöglichkeiten
      → Ideal für Angreifer



Beispiel
Abruf öffentlicher Informationen



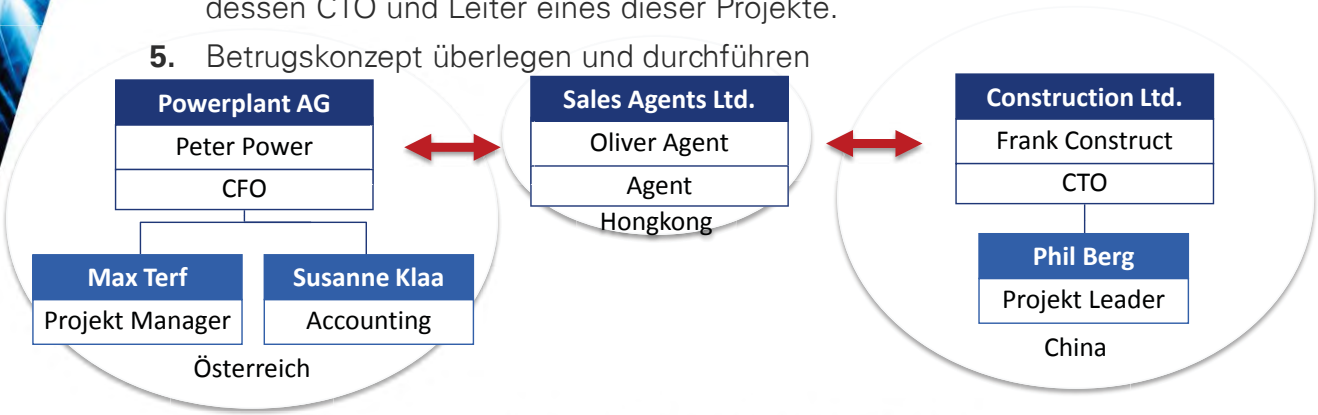
Über mich

Zusammenfassung

Expert with more than fifty years' experience planning and supervising construction projects and shut downs in the Power, & Gas and Nuclear industries.

It´s quite easy!
Abruf öffentlicher Informationen

1. Profil des CFO eines Kraftwerkerrichtungs-Unternehmen auf LinkedIn identifiziert
2. Projektmanager und Buchhalter des gleichen Unternehmens ebenfalls öffentlich einsehbar
3. Informationen über aktuelle Kraftwerksprojekte in China auf der Homepage des Unternehmens auffindbar. Dort werden auch Angaben über einen Handelsagenten gemacht.
4. Nach einer Recherche findet man einen chinesischen Baukonzern inklusive dessen CTO und Leiter eines dieser Projekte.
5. Betrugskonzept überlegen und durchführen



37 Mrd EUR: Estimated cost of Cyber Crime in the UK.[1]

Whereas the illegal drug trade is worth just 13 Mrd EUR a year.[2]

1) The Cost of Cyber Crime. Cabinet Office. UK. 2014

2) http://www.nationalcrimeagency.gov.uk/crime-threats/drugs am 28.10.2015

Beispiele für „Fake President" Angriffe

#1: Produktionsunternehmen Variante „Business E-Mail Compromise"

- österreichisches Unternehmen („Verkäufer") verkaufte und lieferte ein Technologieprodukt an ein Unternehmen im Ausland („Käufer").
- **Angreifer registrierte** sich Domain-Adressen, welche den originalen Domains des Verkäufers sehr ähnlich waren (sogenannte "**Fake-Domains**", zB "KMPG.at" statt "KPMG.at") sowie dazugehörige E-Mail Adressen zu Personen, welche für Projektabwicklung und -bezahlung verantwortlich waren (zB payment@kmpg.at).
- **Angreifer sendete** eine projektbezogene **E-Mail** bzw eine E-Mail aus einem kompromittierten E-Mail-Account **ein zweites Mal** an den Käufer.
- Käufer erkannten die falsche E-Mail-Adresse nicht als solche und verwendeten die "Antworten"-Funktion aus ihrem E-Mail Client.
  → **Erfolgreiches Einschleusen in die Kommunikation** zwischen Verkäufer und Käufer.
- **Angreifer verlangte** die **Bezahlung** auf ein **anderes Bankkonto** (**Begründung** „**Sanktionen**" für Zahlungsverkehr).

Schadensausmaß

- falsch überwiesener Geldbetrag: ca. 800.000,- €
- Kosten für die Aufarbeitung: ca. 200.000,- €

Beispiele für „Fake President“ Angriffe
#1: Produktionsunternehmen

Variante „Business E-Mail Compromise“

Beispiel E-Mail

- richtig: max.mustermann@company.com
- gefälscht: max.mustermann@compamy.com

From: Max Mustermann [mailto:max.mustermann@compamy.com]
Sent: Thursday, 1 October, 2015 3:15 AM
To: frank@company-austria.com
Subject: Payment for machine no. 23739

Dear Frank!

Our acct have been suspended due to auditing and we can not receive any payment on it for now, based on this till we resolved that, we use our Turkey investment company account; MOUA CONSULTING LTD for our all pending payments.

Please instruct the client to make payment to to the bellow bank details and send me swift copy of payment asap

ACCOUNT NAME:.....MOUA CONSULTING LTD.
ACCOUNT NUMBER:....123-123-12
SWIFT CODE:.....HXXXX
IBAN NUMBER:.....TR-123123-123
BANK ADDRESS:.....Turkey
BANK NAME.....HSBC Bank

Thanks for your understanding

Best regards

Mit freundlichen Grüssen / Cordialement

Max Mustermann
Project Manager

Direct: (+43) 12 3 45 67

Company
Street 18, 1234 Vienna, Austria
WEB: <http://www.company.com/>

Beispiele für „Fake President“ Angriffe
#2: Unternehmen + Anwaltskanzlei

- Ein Rechnungswesen-Mitarbeiter erhält einen Anruf von einem Angreifer, der **vorgibt der Vorstand zu sein**.
- Der Mitarbeiter wird über eine wichtige Transaktion informiert, die aus „Compliance Gründen“ **sehr vertraulich behandelt** werden muss. Es geht um eine **„Provisionszahlung“** an einen Agenten in Übersee. Diese sei dringend nötig, um einen Kundenauftrag zu erhalten.
- Der vermeintliche **Angreifer überzeugt** den **Mitarbeiter**, der auf eine Schmiergeld-Zahlung schließt, dass die Transaktion von einer Anwaltskanzlei durchgeführt wird.
- Der Mitarbeiter kennt die Kanzlei nicht, findet deren Homepage aber im Internet. Auch der vom Vorstand genannte Rechtsanwalt ist auf der Seite abgebildet.
- Nach einem Gespräch mit dem Anwalt, **initiiert der Mitarbeiter** die **Zahlung**.
- Die Rechtsanwaltskanzlei war erfunden und wurde anschließend wieder vom Netz genommen.

Schadensausmaß
- falsch überwiesener Geldbetrag: ca. 700.000,- €

Beispiele für „Fake President“ Angriffe
#3: Unternehmen mit Handelsvertreter

Variante „Business E-Mail Compromise“

- Ein Buchhalter bemerkte **offene Forderungen** bei diversen Kunden in Übersee. Die Kunden werden von einem Handelsvertreter betreut.
- Der Buchhalter urgierte diese Forderungen per E-Mail beim Handelsvertreter.
- Der Buchhalter erhielt daraufhin **Überweisungsbestätigungen**, welche **Widersprüche** enthalten.
- Die **forensische Aufarbeitung** durch KPMG ergab, dass:
  - das **E-Mail System** des Handelsvertreters **kompromittiert** wurde,
  - Kunden durch gefälschte E-Mails aufgefordert wurden, ein anderes Bankkonto zur Begleichung der offenen Forderungen zu verwenden und dadurch
  - Überweisungen auf falsche Konten getätigt wurden.

Schadensausmaß
- falsch überwiesener Geldbetrag: ca. 500.000,- €

Maßnahmen gegen „Fake President“ Angriffe

Was kann das Unternehmen tun?

Organisationale Maßnahmen

Technische Maßnahmen

Maßnahmen gegen „Fake President“ Angriffe

Was kann das Unternehmen tun?

Organisationale Maßnahmen

Awareness schaffen

- **Information an** alle **Mitarbeiter mit Zahlungsbefugnissen** mittels einer Aussendung über den Betrugstyp „Fake President“.
- Durchführung von **Schulungen** mit Verweis auf Datenschutz in sozialen Netzwerken (Xing, LinkedIn, Facebook, etc).
- Regelmäßige unangekündigte **Überprüfungen**

Analyse kritischer Prozesse

- **Erhebung und Dokumentation** aller **Zahlungsprozesse** im Unternehmen
- **Identifikation** von **Einzelzahlungsberechtigungen**
- Statistik über vergangene Zahlungsvorgänge
  → Identifikation von Zahlungen bei denen der Standardprozess nicht eingehalten wurde

Maßnahmen gegen „Fake President“ Angriffe

Was kann das Unternehmen tun?

Organisationale Maßnahmen

Einführung sicherer Prozesse / IKS

- Etablierung und Überwachung **standardisierter Arbeitsprozesse**, gerade für Überweisungen.
- Einführung und Überwachung des **4-Augen-Prinzips** sowie Sicherstellung, dass es zu keinen Ausnahmen kommen kann.
- Sicherstellung, dass Änderungen von Zahlungsmodalitäten **verpflichtend** mit einer **Rückfrage** über einen anderen Kommunikationskanal (zB Telefon) an eine definierte Person **ausnahmslos** erfolgen müssen.
- Einführung eines „**internen Kontrollsystems**“ und Berücksichtigung dessen Prinzipien:
  - Transparenz
  - 4-Augen-Prinzip
  - Funktionstrennung
  - Mindestinformation

Maßnahmen gegen „Fake President“ Angriffe

Was kann das Unternehmen tun?

Technische Maßnahmen

Absicherung Zahlungsverkehr

- **Freigabeworkflows technisch absichern** (Umgehen des 4- oder mehr-Augen-Prinzips technisch verhindern)
- Implementierung zusätzlicher Authentifizierungsmaßnahmen

Brand Tracking

- Maßnahmen zur **Überwachung der** eigenen „**Unternehmensmarke**“ (Domain-Watching, Social Network Tracking“), um falsche Informationen identifizieren zu können

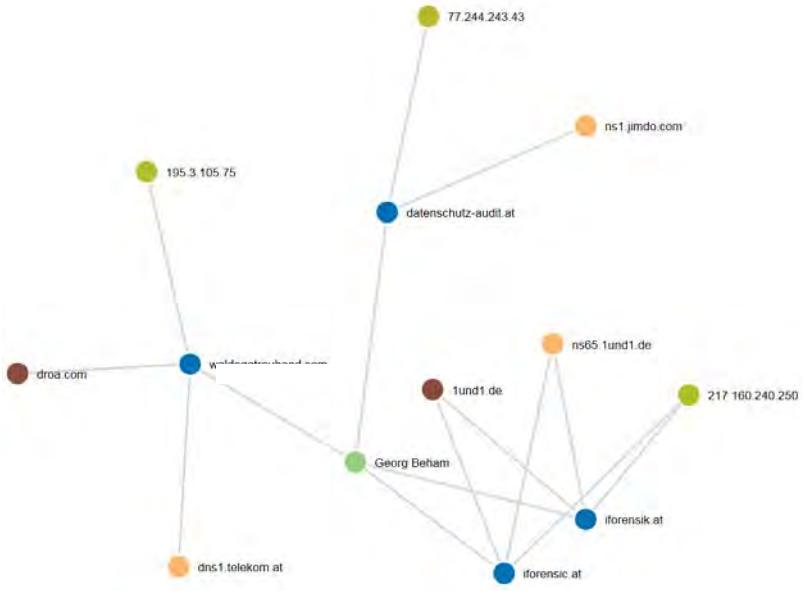
Anti-Malware

- Maßnahmen zur **Erkennung** und **Abwehr von Schadsoftware**, welche Informationen ausspähen und an Angreifer senden kann

Maßnahmen gegen „Fake President“ Angriffe

Was kann das Unternehmen tun?

Technische Maßnahmen



© 2016 KPMG Advisory GmbH, österreichisches Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International“), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Printed in Austria. KPMG und das KPMG-Logo sind eingetragene Markenzeichen von KPMG International.

Maßnahmen gegen „Fake President“ Angriffe

Was kann das Unternehmen tun?

Technische Maßnahmen

Erkennung von Cyber Angriffen

- Anpassung **Logging** und **Monitoring**
- Inventur aller Logdaten-Quellen
- Einführung eines **Log-Management** Prozesses mit Vorgaben zur Aufbewahrung, Übertragung und Analyse
- Anschaffung von speziellen **IT-Systemen** zur **Erkennung von Cyber Angriffen** (Intrusion Detection Systeme) oder Zukauf eines dementsprechenden Services von Dienstleistern

E-Mail-Absicherung

- Berechtigungsprüfung E-Mail Server
- **E-Mail-Verschlüsselung** einführen
- Ermöglichen des **Erkennens** von **Phishing E-Mails** und **E-Mail-Spoofing** im eigenen Netzwerk

© 2016 KPMG Advisory GmbH, österreichisches Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International“), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Printed in Austria. KPMG und das KPMG-Logo sind eingetragene Markenzeichen von KPMG International.

FIGURE 2 Forrester Wave™: Information Security Consulting Service Providers, Q1 '16

KPMG

ÖGWT
IHR SERVICE-NETZWERK

www.kpmg.at/cyber

Georg Beham, MSc
Director, Advisory
Tel: 0664 816 11 71
Email: gbeham@kpmg.at

Notfall-Hotline: 0800 07 10 30

Diese Präsentation ist online unter
www.oegwt.at → Veranstaltungen → Oberösterreich
verfügbar.