Social Media und Social Engineering

Von Patrick Helmig und Robert Reitze

INSIDERS KNOWLEDGE
Security by Culture

Gesellschaft für Informatik

15.06.2012
SECMGT Workshop
Digitale Identitäten / Identitätsmanagement

AGENDA

1 **Risikofaktoren Social Engineering und Social Media**
- Was ist Social Engineering?
- Soziale Netzwerke als Suchmaschinen
- Evolution von Social Engineering

2 Fallbeispiele
- Beispiel • Industriespionage im Mittelstand
- Beispiel • Kennen wir uns?

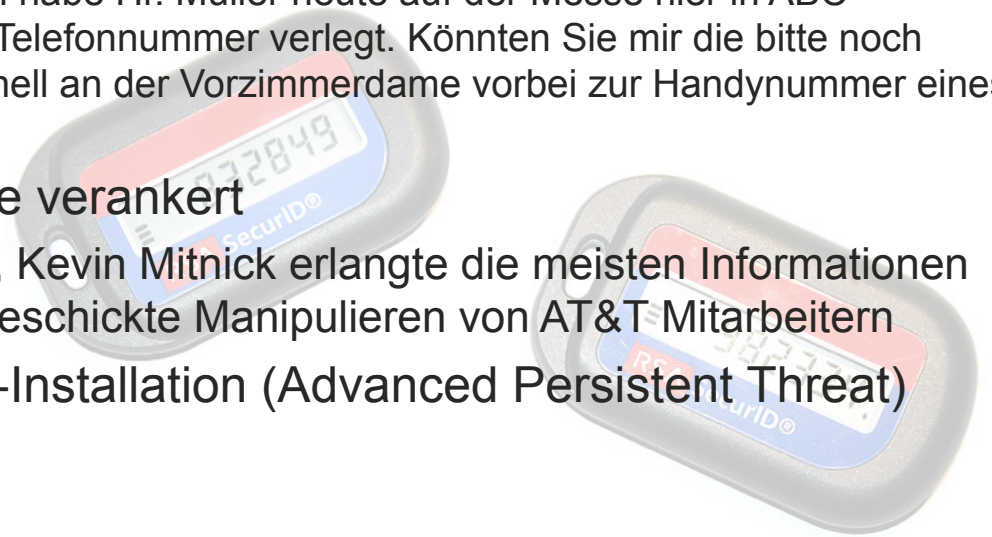
3 Abwehrmaßnahmen
- Social Media Leitfäden im Vergleich
- Mögliche weitere Maßnahmen

4 Kontaktinformationen

SOCIAL ENGINEERING & INDUSTRIESPIONAGE

Social Engineering als Unterstützung gezielter Angriffe

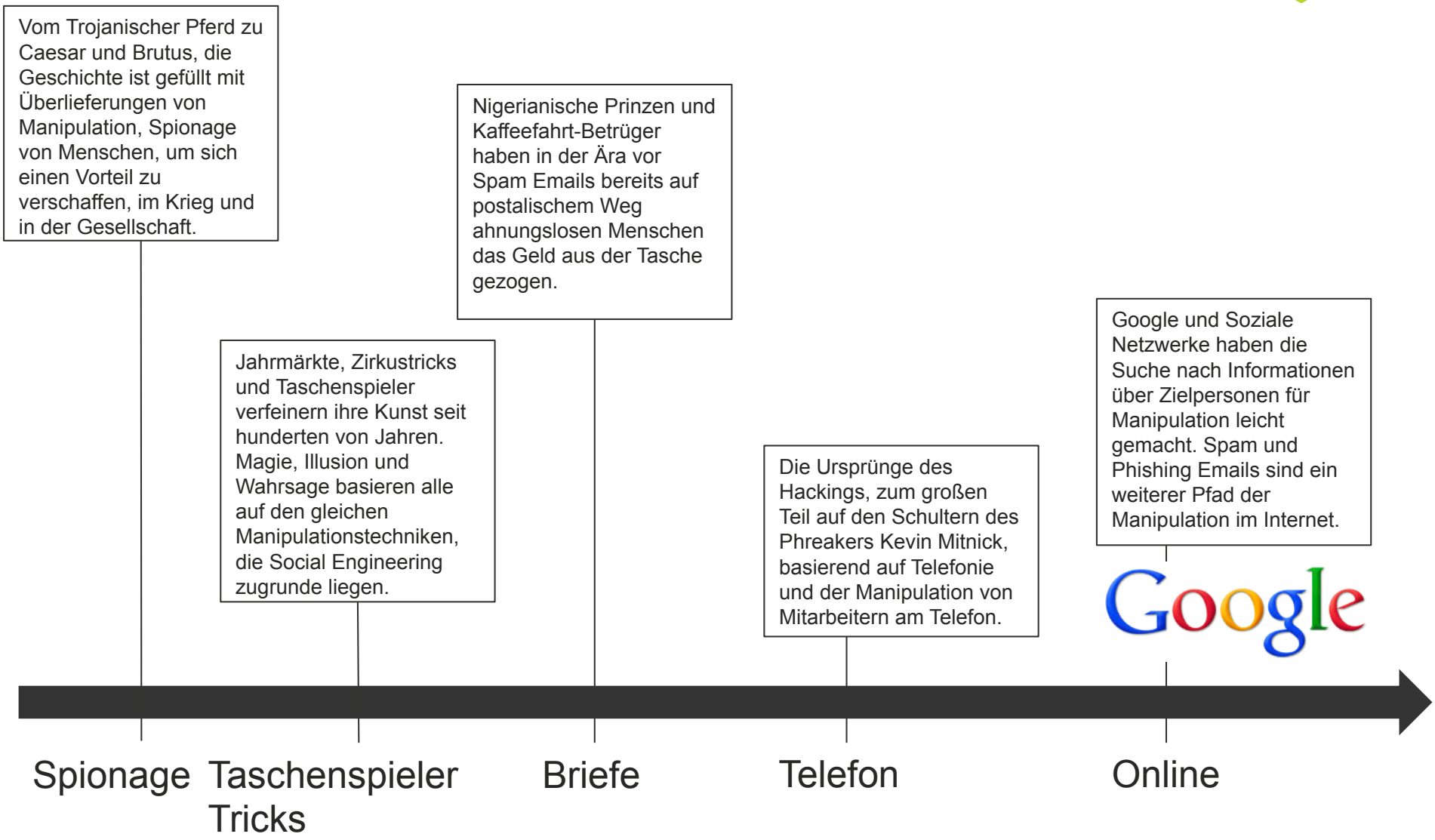
- Gezielte Manipulation anderer Menschen, im Dt. am ehesten angewandte Sozialwissenschaften
  - Informationen zum potentiellen Opfer können verwendet werden, um eine Vertrauenssituation herzustellen
    - z.B.: Wissen über Freunde und Kollegen (Hr. Mayer hat mir gesagt sie sind der Datenbanken Experte des Unternehmens)
    - Wissen über den Arbeitsplatz und die Position
    - Wissen über den Aufenthaltsort (!) „Ich habe Hr. Müller heute auf der Messe hier in ABC kennengelernt. Leider habe ich seine Telefonnummer verlegt. Könnten Sie mir die bitte noch einmal zukommen lassen?“, führt schnell an der Vorzimmerdame vorbei zur Handynummer eines CEOs
- In der Hackerkultur schon sehr lange verankert
  - Einer der ersten „bekannten“ Hacker, Kevin Mitnick erlangte die meisten Informationen über das US Telefonnetz durch das geschickte Manipulieren von AT&T Mitarbeitern
- Kann als Türöffner für eine Trojaner-Installation (Advanced Persistent Threat) dienen
  - z.B.: RSA
- Kann auch ohne technische Unterstützung dienen
  - Bsp. Spione, Trickbetrüger, Journalisten, etc.



Bilder: WikiMedia

EVOLUTION DES SOCIAL ENGINEERING

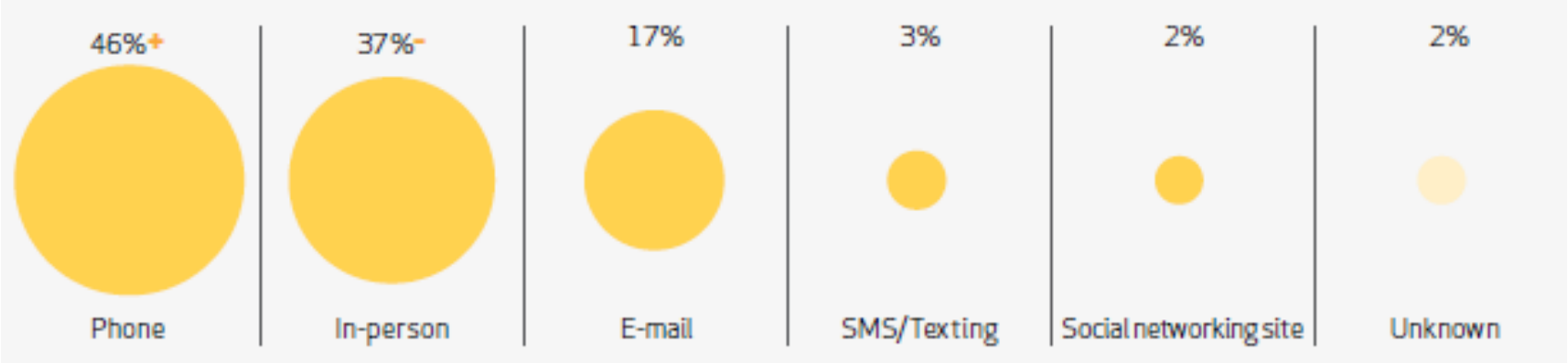
Die Manipulation von Menschen ist nichts Neues



SOCIAL ENGINEERING HEUTE

Der persönliche Kontakt zu Mitarbeitern ist die häufigste Variante

Prozentuale Verteilung von Social Engineering Methoden bei Angriffen. (Laut Verizon Data Breach Report 2012)



- Die meisten Versuche, Mitarbeiter dazu zu bringen, Geschäftsgeheimnisse heraus zu geben finden über das Telefon oder persönlich statt
- Soziale Netzwerke werden zwar sehr selten zur Kontaktaufnahme genutzt, dienen aber als wichtige Informationsquelle
- E-Mails und soziale Netzwerke stellen die unterstützenden Medien für klassische Angriffe dar

http://www.troyhunt.com/2012/04/5-interesting-security-trends-from.html
http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

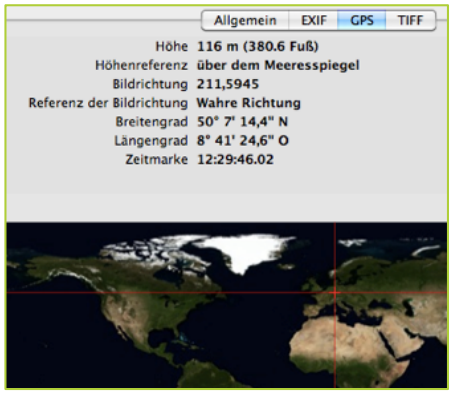
Bilder: Verizon

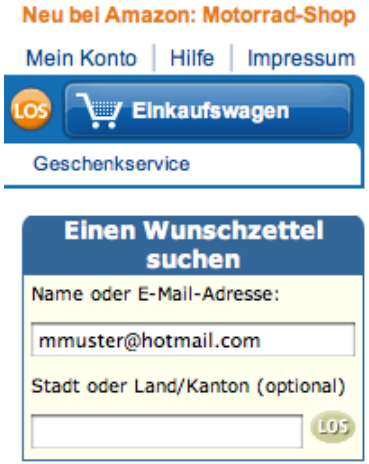
INFORMATIONEN IN SOCIAL MEDIA

Öffentlich zugängliche Daten in Social Media

facebook

Explizite / Implizite Informationen





skype™

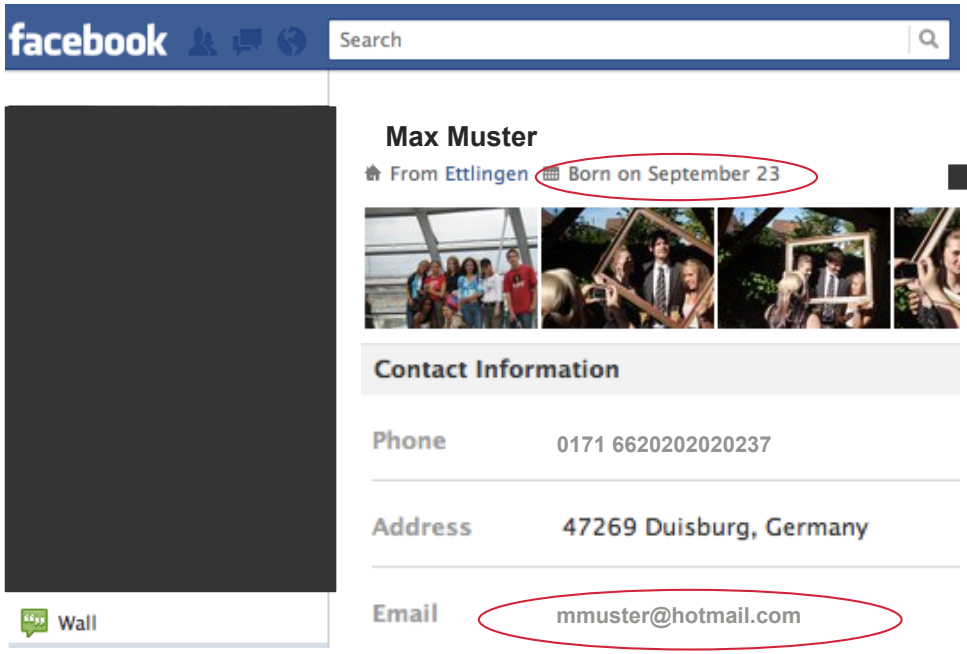
SOZIALE NETZWERKE ALS SUCHMASCHINEN

Komplexe Filter erlauben eine präzise Suche nach Personengruppen

- Soziale Netzwerke wie XING, Facebook und LinkedIN stellen nicht nur Informationen und Verbindungen einzelner Personen bereit, sie erlaub auch das Dursuchen der Mitglieder nach Attributen
- Anhand einer zunehmender Anzahl von Eigenschaften können Mitglieder gefunden werden:
  - Arbeitgeber
  - Ausbildung
  - Wohnort
  - Schule
  - Etc
- Diese Suchfunktion macht es leicht, Mitglieder einer Organisation sehr präzise zu identifizieren (z.B. alle Mitarbeiter eines bestimmten Standorts oder alle Mitarbeiter die Jura studiert haben)

RISIKOFAKTOR SOCIAL ENGINEERING

Missbrauch von öffentlich zugänglichen Informationen



Gezielte-Phishing Email:

An: Mmuster@hotmail.com
Von: support@apple.con
Betreff: Geburtstags-Gutschein

Hi Max,

Alles Gute zum Geburtstag! Wir schenken dir einen 10 € iTunes Gutschein:

http://www.apple.com/iTunes_Birthday_Card_042J0345

Beste Grüße
Ihr iTunes Support Team

- Bei Facebook und XING öffentlich zugängliche Informationen erleichtern es Angreifern, personalisierte Phishing-Attacken zu starten. Die Email Adresse und der Geburtstag oder persönliche Interessen sind häufig schon ausreichend.

AGENDA

1 Risikofaktoren Social Engineering und Social Media
- Was ist Social Engineering?
- Soziale Netzwerke als Suchmaschinen
- Evolution von Social Engineering

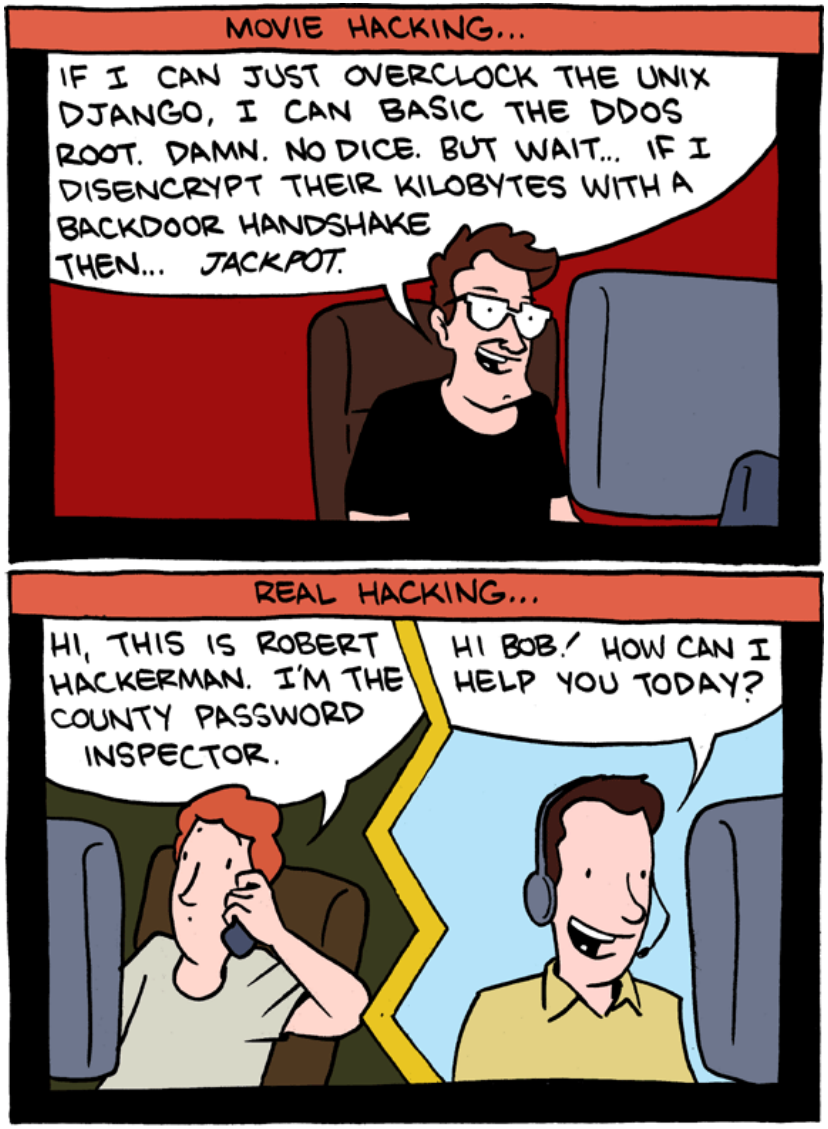
2 Fallbeispiele
- Beispiel • Industriespionage im Mittelstand
- Beispiel • Kennen wir uns?

3 Abwehrmaßnahmen
- Social Media Leitfäden im Vergleich
- Mögliche weitere Maßnahmen

4 Kontaktinformationen

BEISPIEL • INDUSTRIESPIONAGE IM MITTELSTAND

Ein kompletter Angriff, ohne das Ausnutzen einer technischen Sicherheitslücke



http://www.smbc-comics.com/index.php?db=comics&id=2526

Ziel: Mittelständisches Technologie Unternehmen (~400 Mitarbeiter)

Einschränkung: Keine „teuren“ Mittel (0-Days, physischer Einbruch)

Umsetzung:

- Gezielte Recherche zu Mitgliedern der Geschäftsführung via XING, Facebook, LinkedIn und Google
- Einladung zu einem „Alumni Treffen“ der Uni Heidelberg mit angehängtem Word Dokument + Macro (Kein Exploit, o.Ä.)
- Folge: Fernzugriff auf einen Arbeitsplatz und das E-Mail System
- Innerhalb von 24h Zugriff auf alle Zieldaten

AGENDA

1 Risikofaktoren Social Engineering und Social Media
- Was ist Social Engineering?
- Soziale Netzwerke als Suchmaschinen
- Evolution von Social Engineering

2 Fallbeispiele
- Beispiel • Industriespionage im Mittelstand
- Beispiel • Kennen wir uns?

3 Abwehrmaßnahmen
- Social Media Leitfäden im Vergleich
- Mögliche weitere Maßnahmen

4 Kontaktinformationen

SOCIAL MEDIA LEITFÄDEN IM VERGLEICH

Maßnahmen verschiedener Unternehmen

hr.2020

Richtlinien für hr-Mitarbeiter zum Umgang mit Sozialen Netzen

Daimler AG

Social Media Leitfaden

Das Internet ist aus unserer Gesellschaft nicht mehr wegzudenken. Zurzeit gewinnt vor allem die Nutzung von Social Media Angeboten mehr und mehr an Bedeutung. Unter dem Begriff „Social Media" werden Plattformen und Netzwerke zusammengefasst, bei denen die Nutzer die Möglichkeit haben beispielsweise Fotos, Videos, aber auch Erfahrungsberichte oder Meinungen auszutauschen. Dazu zählen unter anderem Blogs, Wikipedia, YouTube, Facebook oder auch Twitter.

Social Media-Guidelines für DATEV-Mitarbeiter

Kunden wie auch Geschäftspartner machen verstärkt Gebrauch von den neuen Möglichkeiten des Internets, um sich auszutauschen und nach für sie passenden Lösungen zu suchen. Hier will DATEV dabei sein und den Dialog auch im Internet aufnehmen. Social Media kann DATEV also auf dem Markt, aber auch Ihnen bei Ihrer täglichen Arbeit helfen.

Machen Sie sich ruhig vertraut mit den Plattformen, seien Sie neugierig, lernen Sie diese zu gebrauchen und Ihren persönlichen Nutzen aus ihnen zu ziehen.

Intel Social Media Guidelines

Tagged As Policy

- Hinweise zu Privatsphäre und Nutzersicherheit eher selten.
- DATEV als herausragendes Beispiel

SOCIAL MEDIA LEITFÄDEN IM VERGLEICH

Maßnahmen verschiedener Unternehmen

Analyse der Social Media Leitfäden von Daimler, Intel, dem Hessischen Rundfunk, Datev und Cisco

- Was bereits in allen Leitfäden vorhanden ist:
  - Hinweis auf die Trennung von privaten und geschäftlichen Inhalten
  - Kennzeichnung von privaten Beiträgen
  - Einschränkung von Aktivitäten in sozialen Netzwerken während der Arbeitszeit
  - Hinweis auf die Verpflichtung zum Schutz von vertraulichen und geheimen Informationen
- Was weitgehend* fehlt:
  - Risiko des indirekten Preisgebens von vertraulichen Informationen
  - Hacking und Phishing Attacken in sozialen Netzwerken
  - Privatsphäreneinstellungen und der Umgang mit Fake-Profilen etc.
  - Social Engineering im Allgemeinen und unter Verwendung von sozialen Netzwerken

* Cisco ist eine Ausnahme und stellt sogar einen eigenen Leitfaden zum Umgang mit Social Engineering bereit

MÖGLICHE MAßNAHMEN

Kompetenz und Aufmerksamkeit verbessern die Sicherheit

- Leitfaden für den Umgang mit sozialen Medien und Netzwerken
- Kompetenz und Aufmerksamkeit der Mitarbeiter durch Trainings erhöhen
- Ansprechpartner schaffen und kommunizieren
- Klassifizierung von Informationen erhöht die Sensibilität der Mitarbeiter im Umgang mit diesen Informationen
- Selbstbewusste Mitarbeiter gehen bewusster und sicherer mit sensiblen Daten und Angriffen um
- Eine Sicherheitskultur im Unternehmen verankert das Bewusstsein für Risiken bei den Mitarbeitern

INSIDERS**KNOWLEDGE**

Security by Culture

Wir unterstützen kleine und mittelständische Unternehmen bei der Entwicklung von Informations-Sicherheitsbewusstsein in der Unternehmenskultur. Die Mitarbeiter unserer Klienten sind die erste Verteidigungslinie zum Schutz von Geschäftsgeheimnissen und vertraulichen Daten.

Wir bieten umfassende Sicherheitskonzepte an, die wir individuell an Ihr Unternehmen anpassen. Wir unterstützen Sie gerne bei:

- Managementstrategien zur Stärkung des Sicherheitsbewusstseins im Unternehmen
- Mitarbeitertrainings zur Identifikation von Angriffen und Wirtschaftsspionage
- Trainings für Ihre IT-Mitarbeiter zur Identifikation und Abwehr aktueller Angriffsmethoden
- Analyse und Beratung zur Sicherung bestehender IT-Infrastruktur
- Und allen anderen Fragen zum Thema Informationssicherheit

Für eine kostenlose Vorstellung unserer Beratungsleistungen können uns gerne über info@InsidersKnowledge.com kontaktieren.

Oder besuchen Sie uns auf www.INSIDERS**KNOWLEDGE**.com

© 2012 INSIDERSKNOWLEDGE