

Soziale Netzwerke machen Industriespionage wirtschaftlich

Von Patrick Helmig und Robert Reitze

INSIDERS
KNOWLEDGE
Security by Culture

25.09.2012

**D-A-C-H Security Konferenz
Konstanz**



Nutzen – Kosten = Wert für den Angreifer


Anmerkung: Modell geht von einem risikofreien Szenario aus bei dem der Angreifer nicht das Risiko straf- oder zivilrechtlicher Konsequenzen zu befürchten hat.
Beispiel: Industriespionage aus China oder gute Anonymisierung des Angriffs




Nutzen – Kosten = Wert für den Angreifer

ANREIZE FÜR ANGREIFER

- Zunehmende digitale Verfügbarkeit von unternehmenskritischen Informationen (Baupläne, Rezepte, etc.)
- Produktionskapazitäten und -Know-How sind in Ländern wie z.B. China und Russland vorhanden
- Für viele Produkte sind die Produktionsgrundkosten kleiner als die Entwicklungs- und Qualitätskosten



Der **Wert** von gestohlenen Informationen steigt



Nutzen – **Kosten** = Wert für den Angreifer

ANREIZE FÜR ANGREIFER

- Zunehmende digitale Verfügbarkeit von unternehmenskritischen Informationen (Baupläne, Rezepte, etc.)
- Produktionskapazitäten und -Know-How sind in Ländern wie z.B. China und Russland vorhanden
- Für viele Produkte sind die Produktionsgrundkosten kleiner als die Entwicklungs- und Qualitätskosten
- Angriffe auf die IT von westlichen Unternehmen sind quasi straffrei
- Hacking und Wirtschaftsspionage sind breit verfügbar und haben sich zur Dienstleistung entwickelt

Der **Wert** von gestohlenen Informationen steigt



Das **Risiko** und die **Kosten** für Angreifer sinken



Nutzen – Kosten = Wert für den Angreifer

ANREIZE FÜR ANGREIFER

- Zunehmende digitale Verfügbarkeit von unternehmenskritischen Informationen (Baupläne, Rezepte, etc.)
- Produktionskapazitäten und -Know-How sind in Ländern wie z.B. China und Russland vorhanden
- Für viele Produkte sind die Produktionsgrundkosten kleiner als die Entwicklungs- und Qualitätskosten
- Angriffe auf die IT von westlichen Unternehmen sind quasi straffrei
- Hacking und Wirtschaftsspionage sind breit verfügbar und haben sich zur Dienstleistung entwickelt

Der **Wert** von gestohlenen Informationen steigt

Das **Risiko** und die **Kosten** für Angreifer sinken

FOLGEN

- Staatlich subventionierte Angriffe
 - Stuxnet
 - RSA
 - Spionage schon bei Zollkontrollen und Messen
- Markt für Datenhehlerei
 - Für die Daten gestohlener Notebooks, Smartphones und Datenträger kann es in Zukunft einen Schwarzmarkt geben
- Privat organisierte Angriffe
 - Murdoch engagiert Hacker, um anderen Pay-TV Anbietern zu schaden
 - „Hacktivist“ spähen Unternehmensdaten aus und veröffentlichen diese (Stratfor, HB Gary, etc.)
 - Produktfälschungen und Nachbauten (Mit falscher oder neuer Marke)
 - Angriffe auf RSA/Lockheed
 - Project Aurora (Angriffe auf Google und andere große US Unternehmen)
 - Wikileaks, Cryptome

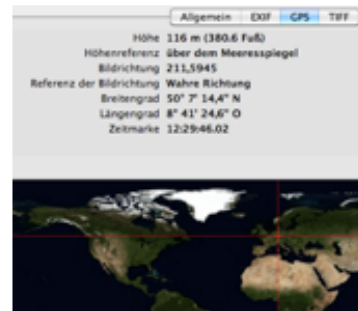


Hypothese 1 | Hypothese 2

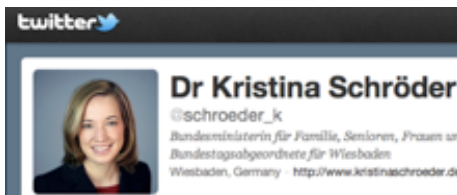
Öffentlich zugängliche Unternehmens- und Mitarbeiterprofile in sozialen Netzwerken beeinflussen die Kosten für gezielte Angriffe auf sensible Unternehmensdaten.

Die Nutzung von sozialen Netzwerken senken die Kosten für mögliche Angreifer und erhöhen so den Wert und die Effizienz eines Angriffs.

Hypothese 1 | Hypothese 2



**Explizite / Implizite
Informationen**



An: BStromberg@capitol.de
 Von: kschöder@gmail.com
 Betreff: Geburtstags-Gutschein

Lieber Herr Stromberg,

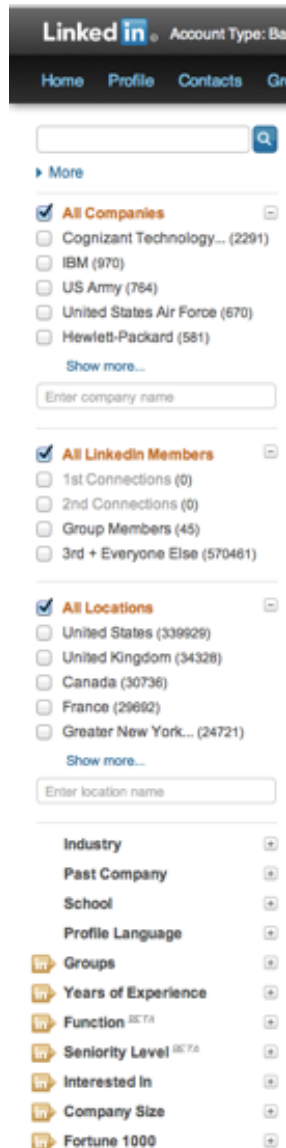
Alles Gute zum Geburtstag! Viel Spaß auf Mallorca! Danke dass Sie bei Facebook unserer Sozialaktion soviel Zeit schenken. Wir wollen uns bei Ihnen bedanken und schenken Ihnen zu Ihrem besonderen Tag einen 10 € iTunes Gutschein:

[http://www.apple.com/
iTunes Birthday Card 042J0345](http://www.apple.com/iTunes_Birthday_Card_042J0345)

Beste Grüße
 Dr. Kristina Schröder

Ihr „Facebook für Familien“ Team

Hypothese 1 | Hypothese 2



LinkedIn Account Type: Ba

Home Profile Contacts Gr

Search bar

More

All Companies (2291)

- Cognizant Technology... (2291)
- IBM (970)
- US Army (764)
- United States Air Force (670)
- Hewlett-Packard (581)

Show more...

Enter company name

All LinkedIn Members

- 1st Connections (0)
- 2nd Connections (0)
- Group Members (45)
- 3rd + Everyone Else (570461)

All Locations

- United States (339929)
- United Kingdom (34328)
- Canada (30736)
- France (29692)
- Greater New York... (24721)

Show more...

Enter location name

Industry

Past Company

School

Profile Language

Groups

Years of Experience

Function

Seniority Level

Interested In

Company Size

Fortune 1000



Google

facebook Suche nach etwas auf Fac

Finde Freunde aus verschiedenen Lebensb

Benutze die Felder unten, um Nutzer zu entdecken, die du aus de

Heimatstadt

Gib eine andere Stadt ein

Derzeitiger Wohnort

- Frankfurt am Main
- Frankfurt am Main (Frankfurt, Germany)

Gib eine andere Stadt ein

Schule

Gib eine Schule ein

Gemeinsame/r FreundIn

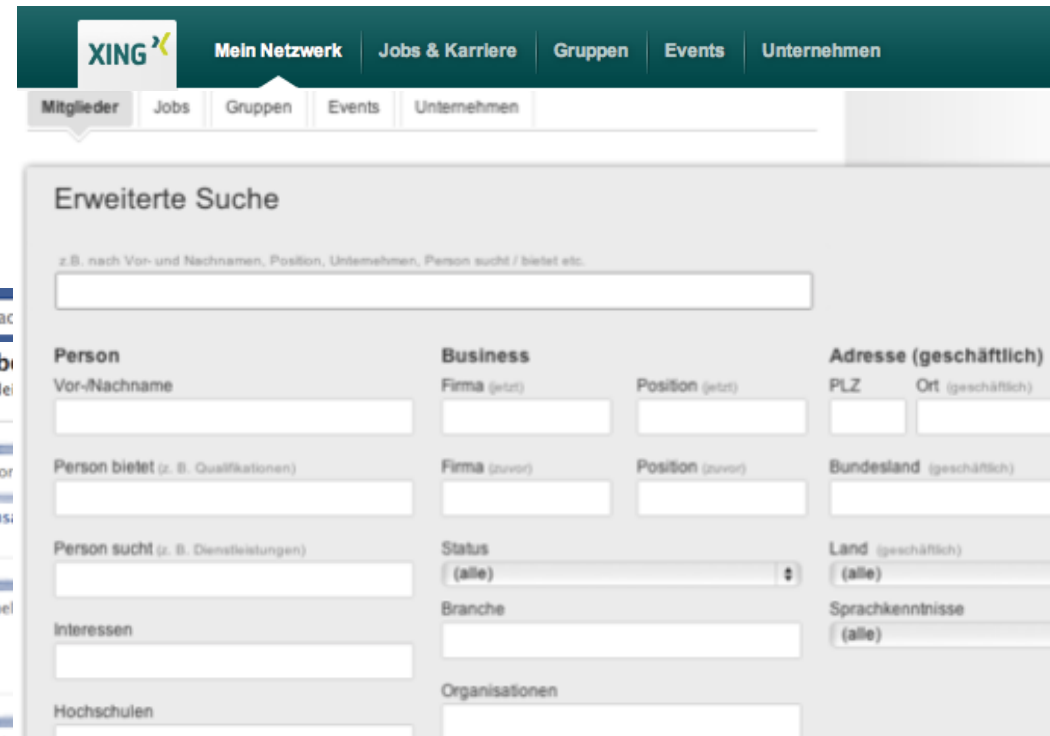
Gib einen anderen Namen ein

Hochschule oder Universität

Gib eine Hochschule ein

Arbeitgeber

- Deutsche Telekom (Deutsche



XING Mein Netzwerk Jobs & Karriere Gruppen Events Unternehmen

Mitglieder Jobs Gruppen Events Unternehmen

Erweiterte Suche

z.B. nach Vor- und Nachnamen, Position, Unternehmen, Person sucht / bietet etc.

Person

Vor-Nachname

Person bietet (z. B. Qualifikationen)

Person sucht (z. B. Dienstleistungen)

Interessen

Hochschulen

Business

Firma (jetzt)

Firma (zuvor)

Status (alle)

Branche

Organisationen

Adresse (geschäftlich)

PLZ Ort (geschäftlich)

Bundesland (geschäftlich)

Land (geschäftlich)

Sprachkenntnisse (alle)

Potentielle Ziele im Unternehmen sind dank Suchfunktion leicht recherchiert

- HR Abteilung
- Produktentwicklung
- Geschäftsführung

Modell

Hypothesen

Fallbeispiele

Fazit



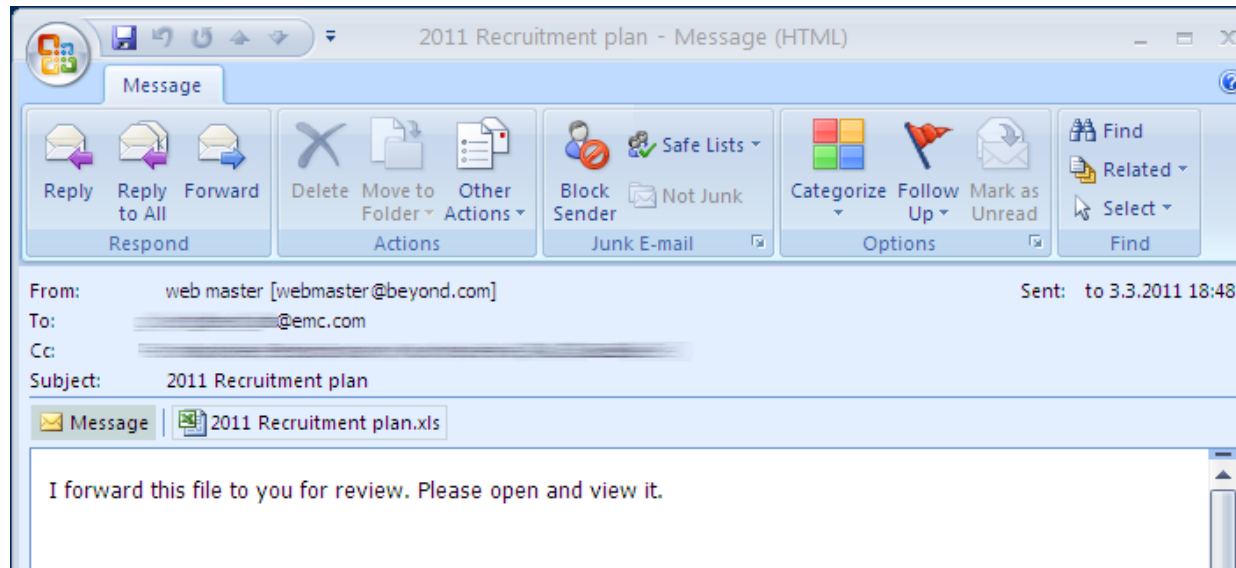
Security by Culture

Fallbeispiel 1 | Fallbeispiel 2

Angriff auf RSA

Identische Angriffe mit und ohne Nutzung
von Daten aus sozialen Netzwerken

Fallbeispiel 1 | Fallbeispiel 2



RSA
SECURITY®



- Angriff auf die Personalabteilung des Mutterkonzerns EMC
- Adobe Flash Exploit, eingebettet in eine Microsoft Excel Datei
- Angriff auf weitere Rechner / Server im internen Netzwerk nach Infizierung eines Arbeitsplatzes bei EMC
- Erfolgreicher Diebstahl des Algorithmus zur Berechnung der Security Tokens
- Informationen aus diesem Angriff wurden genutzt um bei Lookhead Martin einzubrechen

Fallbeispiel 1 | Fallbeispiel 2

- 2 Angriffe auf ein mittelständisches Unternehmen, gleiche Zielperson



24 Stunden = Erfolglos



8 Stunden = Erfolgreich

Modell

Hypothesen

Fallbeispiele

Fazit



Security by Culture

Nutzen – Kosten = Wert für den Angreifer



Nutzen – Kosten = Wert für den Angreifer

- Option 1 - Reduzierung des Nutzens für den Angreifer
 - Reduzierung der digitalen Verfügbarkeit von sensiblen Informationen
 - → Schwierig oder nicht umsetzbar
 - Option 2 - Erhöhung der **Kosten** für den Angreifer
 - IT Sicherheit
 - Informationssicherheitsmanagement
 - Reduzierung der in sozialen Netzwerken verfügbaren Informationen über Mitarbeiter (nicht nur rechtlich schwierig)
 - Option 3 – Reduzierung der **Effizienz** von Angriffen
 - Verbesserung der internen Kommunikation
 - Mitarbeitersensibilisierung
- Lösung – Kombination?