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

Security by Culture

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

Security by Culture

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

- Angriffe auf die IT von westlichen Unternehmen sind quasi straffrei
- Hacking und Wirtschaftsspionage sind breit verfügbar und haben sich zur Dienstleistung entwickelt

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

Security by Culture

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

- Angriffe auf die IT von westlichen Unternehmen sind quasi straffrei
- Hacking und Wirtschaftsspionage sind breit verfügbar und haben sich zur Dienstleistung entwickelt

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
  - „Hacktivisten“ spähen Unternehmensdaten aus und veröffentlichen diese (Stratfor, HB Gary, etc.)
  - Produktfälschungen und Nachbauten (Mit falscher oder neuer Marke)
  - Angriffe auf RSA/Lockheed
  - Project Aurora (Angrffe 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

skype

facebook

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

Lieber Herr Stromberg,

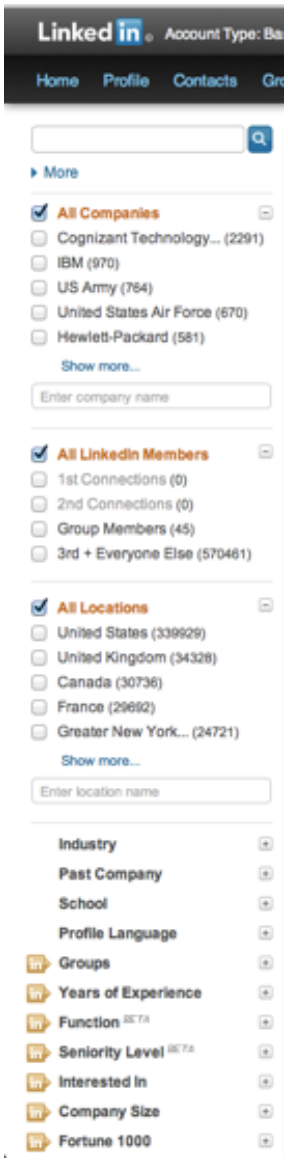
Alles Gute zum Geburtstag! Viel Spaß auf Mallorca! Danke dass Sie bei Facebook unserer Sozialaktion soviel Zeit schenken. Wir wollen uns bei Ihnen bedanken und schenken Ihnen zu Ihrem besonderen Tag einen 10 € iTunes Gutschein:

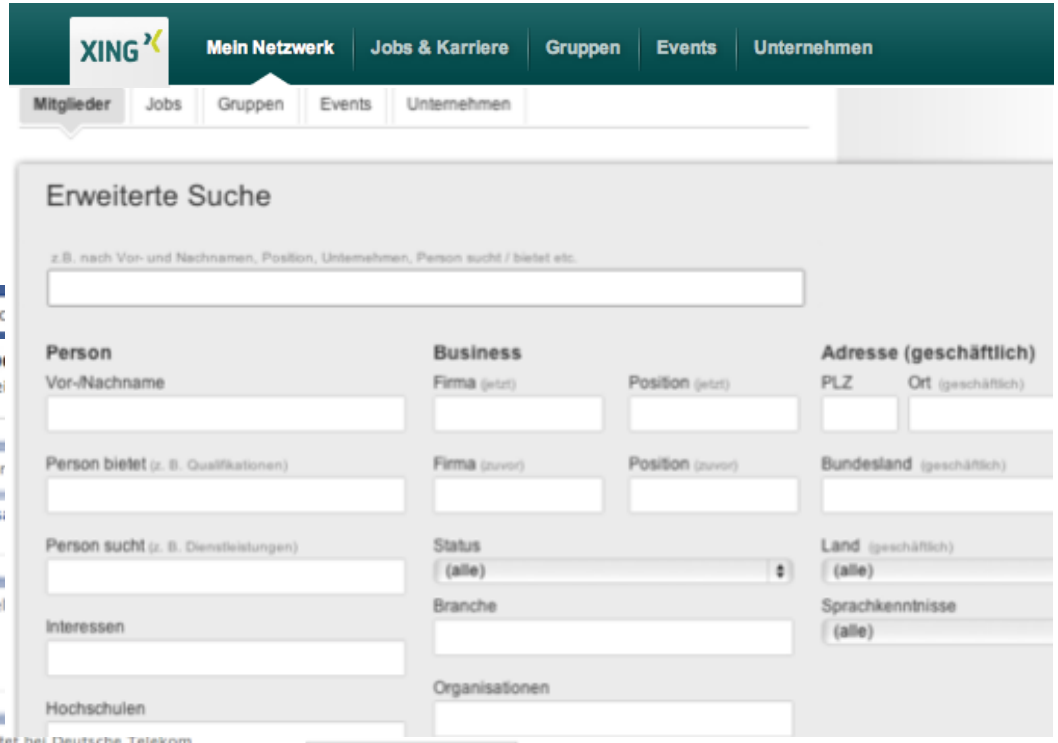
http://www.apple.com/iTunes_Birthday_Card_042J0345

Beste Grüße
Dr. Kristina Schröder

Ihr „Facebook für Familien“ Team

Hypothese 1 | Hypothese 2





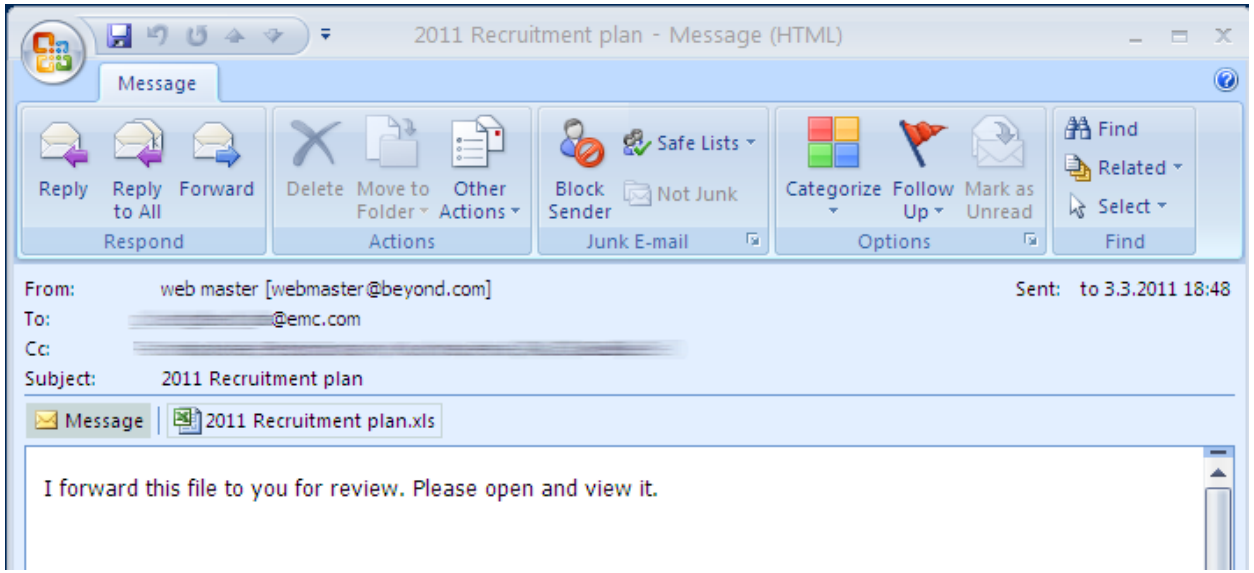
- Potentielle Ziele im Unternehmen sind dank Suchfunktion leicht recherchiert
  - HR Abteilung
  - Produktentwicklung
  - Geschäftsführung

Fallbeispiel 1 | Fallbeispiel 2

Angriff auf RSA

Identische Angriffe mit und ohne Nutzung von Daten aus sozialen Netzwerken

Fallbeispiel 1 | Fallbeispiel 2



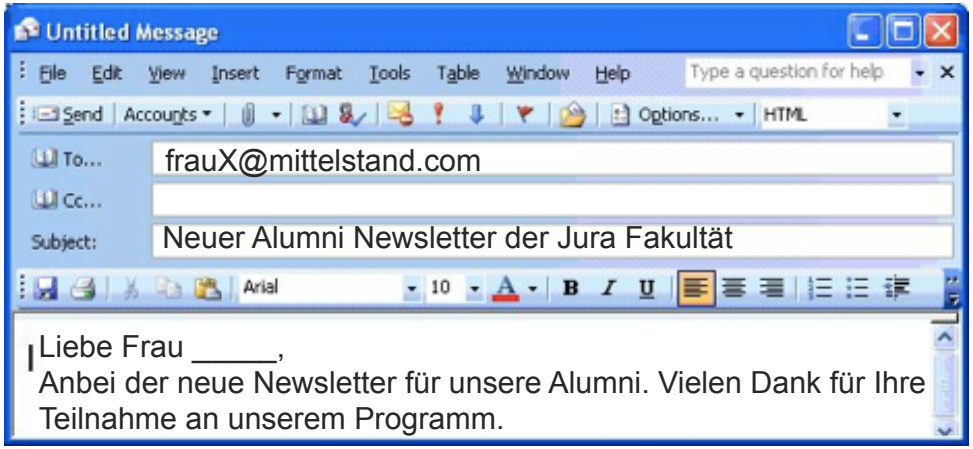
- Angriff auf die Personalabteilung des Mutterkonzerns EMC
- Adobe Flash Exploit, eingebettet in eine Microsoft Excel Datei
- Angriff auf weitere Rechner / Server im internen Netzwerk nach Infizierung eines Arbeitsplatzes bei EMC
- Erfolgreicher Diebstahl des Algorithmus zur Berechnung der Security Tokens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

Fallbeispiel 1 | Fallbeispiel 2

- 2 Angriffe auf ein mittelständisches Unternehmen, gleiche Zielperson

Rechts- und Staatswissenschaftliche Fakultät
Rechtswissenschaft

universitätbonn



24 Stunden = Erfolglos

8 Stunden = Erfolgreich

Nutzen – Kosten = Wert für den Angreifer

Security by Culture

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?