TeleTrusT
Pioneers in IT security.

TeleTrusT-Informationstag "Cyber Crime"

Berlin, 20.05.2011

Dr. Johannes Wiele
TÜV Rheinland i-sec GmbH
Competitive Intelligence und Social Engineering

Ausgangslage
Zwischen Informationsbeschaffung und Spionage

„Competitive Intelligence“:

- Informationsbeschaffung im Web
- Business Networking
- Einstellen/Abwerben von „erfahrenen Fachkräften mit Branchenkontakten“
- Informationsbeschaffung auf Messen
- Informationsbeschaffung auf Konferenzen

… und wo ist die Grenze?

Ausgangslage
An der Grenze zur Manipulation

„Social Engineering“:

- Gezielte Manipulation des menschlichen Verhaltens, um eigene Zwecke zu erreichen
- Sympathie und Autorität ausspielen
- Um Hilfe bitten
- Gute Stimmung nutzen
- Geben und nehmen (Reziprozität)

… und wo ist die Grenze?

Ausgangslage
Über die Grenze zur Manipulation hinweg

„Social Engineering“:

- Formell (ethisch/juristisch): Zur Überschreitung von Regeln bewegen
  - Gesetze (legitimiert)
  - Richtlinien (akzeptiert)
- Persönlich: Unter Druck setzen, außer Kontrolle bringen
  - Angst einjagen
  - Verunsichern
  - Alkohol etc.
- Identität fälschen, falsche Autorität anmaßen
- Bestechen
- Persönlicher / emotionaler Betrug

Gegenwehr
Die Problemkonstellation

Die Möglichkeiten der Technik sind begrenzt:

- „Wanzensuche“ ist ein Fall für Spezialisten
- Die Suche nach IT-gestützten Angriffen ist ein Fall für Spezialisten
- Psychologen scheitern an Technikern und Juristen

Was bleibt an Ansätzen?

- Regelungskompetenz der Führungskräfte – die Spezialisten müssen bestellt werden, Prozesse müssen modelliert werden

- Einbindung der Belegschaften als „Sensoren“

Gegenwehr
Die Problemkonstellation

Industriespionage findet im Rahmen von „Blended Threats“ statt.
Die Angreifer gehen Schritt für Schritt vor und …

- versuchen sich an der IT,
- rufen an,
- helfen oder machen Geschenke,
- durchforschen Mülltonnen,
- machen „Hausbesuche“,
- spielen mit dem Chef Golf … Führungskräfte suchen nach Kommunikationsgelegenheiten uns sind unter „Peers“ angreifbar .

- Die Einzelelemente bleiben unter dem Radar, bei schlechter Zusammenarbeit zwischen IT-, Konzern- und Personensicherheit so-wie Daten- und Objektschutz fallen die Einzelelemente kaum auf.
- Und leider sind die „Typen“ in den Sicherheitsabteilungen nicht immer kompatibel (Ausbildung Ausrichtung, Präferenzen))!

Social Engineering
Die Kunst der Manipulation

- Vortäuschung von Autorität:

  “Ich bin Niederlassungsleiter in X, Ihr Chef ist hier, er braucht für den Abschluss dringend die Präsentation Y…”

- Mitleid hervorrufen:

  “Sie sind doch auch noch neu hier, ich habe die Schlüssel vergessen, können Sie mir nicht den Raum aufschließen? Ich will doch nicht so früh schon Ärger…”

- Vortäuschung von Sympathie

Social Engineering
Die Kunst der Manipulation

Die Angreifer setzen auf Social Engineering. Sie…

- spielen Rollen (Hilfesuchender, Autoritätsperson, Dienstleister, Insider),
- recherchieren genau,
- helfen oder machen Geschenke…
- … und nutzen menschliche Heuristiken.

Was sind Heuristiken?

Gegenwehr
Heuristiken im Spiel

Heuristiken: Evolutionär gefestigte, im Menschen fest „verdrahtete“ Wege der Entscheidungsfindung.

Sie kommen zum Einsatz …

- wenn eine Situation für eine rational-logische Entscheidung zu wenige oder zu viele Informationen liefert, also „unübersichtlich“ ist (trifft auf jede vierspurige Kreuzung zu, die Sie heute mit dem Auto überqueren mussten – Roboter schaffen das bisher kaum),
- bei Zeitmangel,
- unter Stressbedingungen.

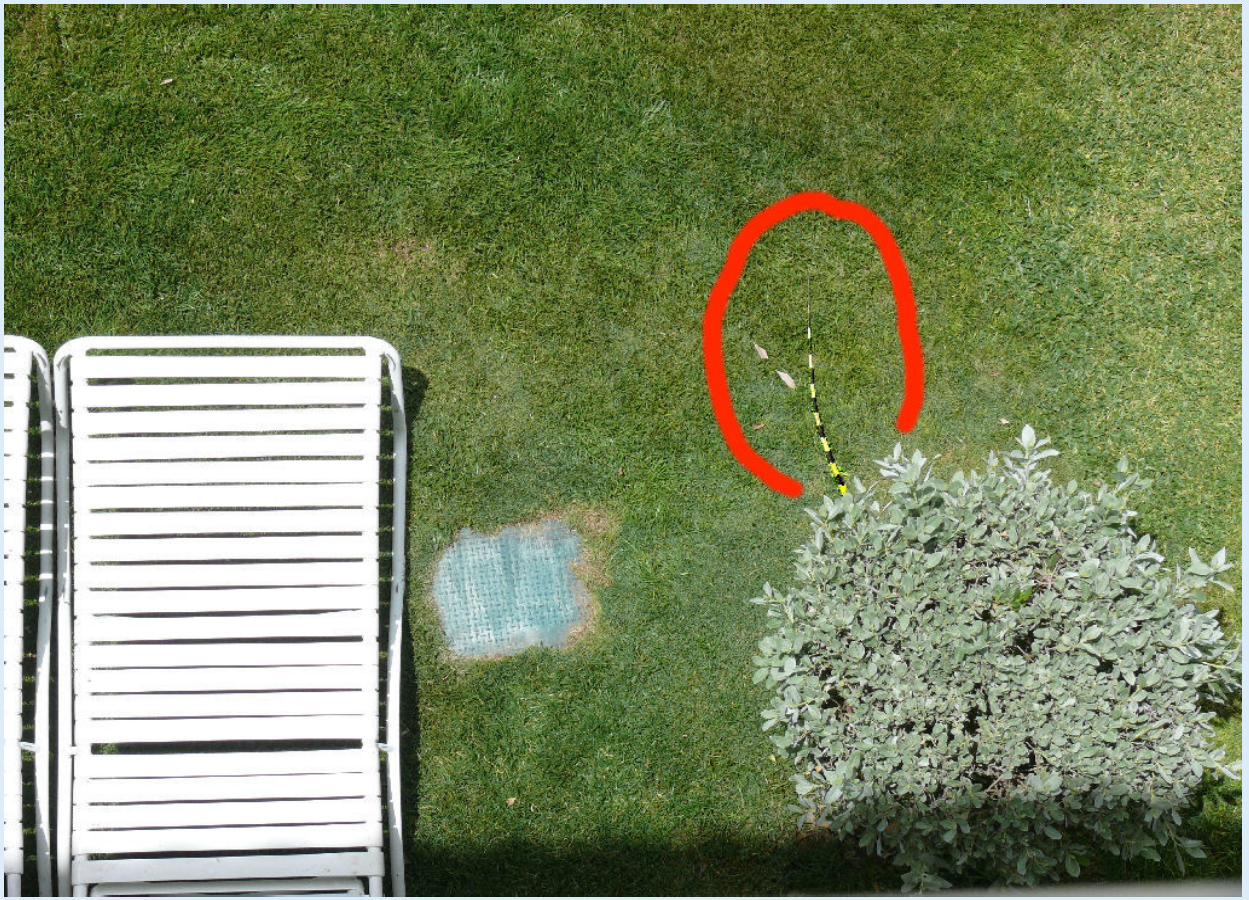
- Social-Engineering-Aspekt: Es erleichtert die Manipulation, Menschen in heuristische Entscheidungswege zu zwingen.

Heuristiken
Kognitive Heuristiken

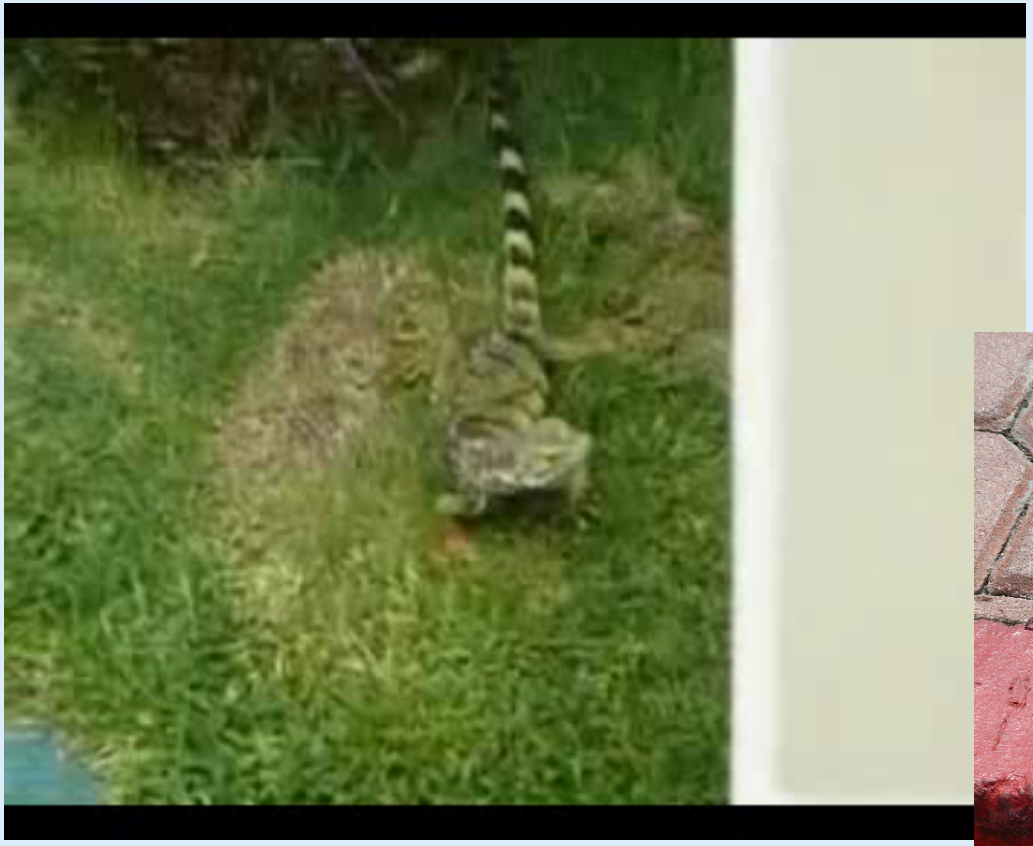
Muster-
erkennung

Schlange,
Wespe,
Tiger…

www.
stadtsporkasse.
de



Heuristiken
Kognitive Heuristiken



Heuristiken
Kognitive Heuristiken

- Sure-Gain-Heuristik
- Optimismus
- Kontroll-Heuristik
- Häufigkeitserfahrung
- Konfirmationspräferenz

Ohne diese Heuristiken könnte der Mensch nicht bestehen!

Heuristiken
Soziale Heuristiken

- Autorität (bzw. deren Anerkennung)
- Sympathie
- Hilfsbereitschaft
- Reziprozität
- Soziale Bewährtheit
- Kommitment/Konsistenz
- Knappheit

(Nach Robert Cialdini)

Heuristiken
Probleme?

- Mustererkennung unterwandert den „guten Sensor“ Mensch
- Die Anweisung, gegen soziale Heuristiken zu verstoßen, stößt auf extreme Widerstände
- Auf den „Rationalmodus“ umzuschalten und dies zu trainieren (Vorschlag Kevin Mitnick) wäre eine Lösung, würden Social Engineers nicht immer wieder Situationen heraufbeschwören, die genau dies erschweren

Heuristiken
Probleme?

- Angreifer geben sich auf der Basis von Recherchen als Insider aus
- Menschen unterschätzen, wie viele Informationen über sie im Web frei verfügbar sind

Beispiel:

- Unternehmen (High-Tech-Zulieferer) behauptet, dank restriktiver Web-2.0-Strategie und „Vorsicht“ kaum im Web präsent zu sein
  - Ergebnis einer Überprüfung:

    Das Web kennt die Golfclubs der Manager und Familienmitglieder, Teilnahme an Turnieren, Soziales Engagement, familiäre Verbandlung von Führungskräften

    Ungewöhnlicher Firmenjet vorhanden, wird auf Luftschauen vorgeführt – aber auch von „Planespottern“ verfolgt: Landungen auf Werksflughäfen (Kunden, Partner, potenzielle Kunden…) sind im Web penibel nachgeführt

Heuristiken
Was also tun?

- Bestimmen und dokumentieren, welche Informationen übers Unternehmen/Einzelpersonen im Umlauf sind, um gefälschte Vertrauensbeweise zu erschweren und zu sensibilisieren
- Anweisung, gegen soziale Heuristiken zu verstoßen, stößt auf extreme Widerstände

Heuristiken
Was also tun?

Einzelpersonen:

- Autorität hinterfragen, Kommitment hinterfragen
- Bei unerbetenen Leistungen/Geschenken die Gegenleistung selbst bestimmen – und die Reaktion beobachten
- In Kommunikationssituationen ein „ungutes Gefühl“ ernst nehmen: Verlangt das Gegenüber „zuviel“, ist irgendetwas „verdächtig??
- Die Schwelle für Rückrufe und Nachfragen senken, das schwierige „Nein-Sagen“ dabei trainieren und nicht nur verlangen
- Allzu große „Liebe“ oder „Seelenverwandschaft“ aus dem Nichts hinterfragen – etwa unwahrscheinliche Schicksalsübereinstimmungen
- Bei all dem nicht paranoid werden…

Heuristiken
Was also tun?

Organisationen:

- Mitarbeiter für ihre Angreifbarkeit sensibilisieren
- Rückfragen und Verzögerungen aus Sicherheitsgründen positiv bewerten (-> Führungskräfte!)
- Kommunikationskanäle zwischen den Sicherheitsverantwortlichen schaffen (-> Chefetage!)
- Mit der Belegschaft kritische Situationen und Zielkonflikte ermitteln (-> Zusammenarbeit oben/unten, „Critical Incidents Technique“ (Flanagan))

- **HILFE IN UNSICHEREN SITUATIONEN BIETEN!!!**
  (Notfallknopf, Telefonnummer, definierter Eskalationsweg)

Maßnahmen
Empowerment versus Awareness

Empowerment:

Prozess, der eine Person befähigt, das nötige Wissen und Können und die Haltung anzunehmen, um souverän mit einer sich wandelnden Welt und den Umständen umzugehen, in denen sie lebt und arbeitet.

Awareness:

- Traditionelle Awareness-Kampagnen schaffen Bewusstsein, aber noch nicht automatisch auch die Fähigkeit, die Sicherheitsanforderungen zu bewältigen!

Vielen Dank!

Dr. Johannes Wiele
Senior Consultant ISMC
TÜV Rheinland i-sec GmbH
Am Grauen Stein
51105 Köln

Tel. 0221/806-3004
johannes.wiele@i-sec.tuv.com

Bettina Weßelmann und Johannes Wiele, Digital Natives und Informations-Sicherheit, in: kes 5/2009, S. 6 ff.

Bettina Weßelmann und Johannes Wiele, Awareness - Warum Informationssicherheit nicht ohne Anwender funktioniert, in: ix special 03/2010

Bettina Weßelmann, „Interne Spionageabwehr", in: kes 1/2011, S. 66-69. Online abrufbar unter http://www.kes.info/archiv/online/11-1-066.htm

TÜVRheinland®
Genau. Richtig.