# Psychologische Aspekte des Social Engineerings

vorgetragen beim Stammtisch der IISA
http://iisa.at/

**Philipp Schaumann**
**Dipl. Physiker**
**Bull GmbH Wien**
**http://sicherheitskultur.at/**

**p.schaumann@bull.at**

# Agenda

- Definition
- Menschliche Schwächen und Stärken
- Die Techniken der Angreifer, psychologisch betrachtet
- Schutzmöglichkeiten auf psychologischer Basis

# Was ist „Social Engineering“

- Eine der gefährlichsten Angriffsmethoden, sie nutzt die Schwachstelle Mensch aus

- meine Definition:

  das Ausnutzen der menschlichen Psychologie um die Sicherheitsregeln des Unternehmens zu unterlaufen

DAS Buch zu Social Engineerings (must read!!):
Kevin Mitnick, The Art of Deception, Wiley Publishing 2002, ISBN 0-471-23712-4

# Menschen ....

- ... möchten anderen Menschen helfen
- ... haben das Bedürfnis, anderen Menschen zu vertrauen
- ... möchten gemocht/geliebt werden, beliebt sein
- ... vermeiden Ärger und Konflikte wo immer es geht

# Was sind die Methoden der Angreifer ? Menschliche Stärken und Schwächen (1)

- **Hilfsbereitschaft**
  „Ich bin ein Kollege aus xxx, muss nur schnell meine Emails abrufen.“
  „Könnten sie mir bitte kurz helfen, ich suche Informationen über ….“
- **Autoritätsgläubigkeit, Angst vor Schwierigkeiten**
  „Ich bin vom Helpdesk und brauche ihr Passwort ….“
  „Ich bin die Sekretärin des Big Boss und brauche heute Abend noch …..“
- **Geltungssucht, Eitelkeit, eigene Bedeutung**
  „Ich bin ein Journalist und mache einen Artikel über kreative Unternehmer.“
  „Ich habe ein Problem, nur Sie können mir helfen.“

# Was sind die Methoden der Angreifer ? Menschliche Stärken und Schwächen (2)

- **Gier, Bereicherungsabsicht**
  „Ich bin ein Prinz aus Nigeria und habe 1,2 Mio ….“
- **Neugier**
  Öffnen von Attachments, Klicken auf Links, fremde CDs oder USB-Sticks im Firmenrechner verwenden
- **Einsamkeit, Möglichkeit zum Flirt, Wunsch geliebt zu werden, Langeweile**
  I-Love-You-Virus, Flirt mit dem anderen Geschlecht
- **Einschüchterung** (hier nicht weiter behandelt)
  Phishing-Mails „wenn sie nicht sofort das Konto bestätigen …“
- **Erpressung** (hier nicht weiter behandelt)
- **Bestechung** (hier nicht weiter behandelt)
- **Spam-basierend, Web-basierend** (hier nicht weiter behandelt)

# Die Techniken im Detail: Hilfsbereitschaft (1)

- **Wichtigkeit des „Opfers“ betonen, Schmeicheln, Komplimente**
  „Nur Sie können mir hierbei helfen“

- **Plausibles, nachvollziehbares, ernstes Problem schildern**
  „Meine Mutter ist im Krankenhaus …..“
  „Ich bin neu hier in der Niederlassung, die anderen sind zum Essen und ein wichtiger Kunde ….“
  „Der Chef tobt schon, wann er endlich den Bericht bekommt.“

# Die Techniken im Detail: Hilfsbereitschaft (2)

- **Frustration darstellen**
  „Jetzt bin ich schon 3x weiterverbunden worden, ich hoffe, sie können mir helfen …..“
- **Überrumpeln** mit falschen Angaben, sich dann korrigieren lassen
  „Meine Kundennummer ist 08098098.“ - „Nein, wenn sie der Meier in der Kerngasse sind, dann ist es 4711“. - „OK, dann wird das ja stimmen, danke.“
- **Hilflosigkeit** darstellen, bis zum Weinen
  - Beim Portier am Wochenende: „Ich habe meinen Firmenschlüssel vergessen, muss wichtigen Bericht holen, mein Chef wirft mich raus wenn ich das schon wieder verpatze.“
  - „Ich bin von der Telekom, muss nur schnell die Verkabelung im Schaltraum überprüfen, sollte schon längst beim nächsten Kunden sein ....“ <schluchz>

# Die Techniken im Detail: Hilfsbereitschaft (3)

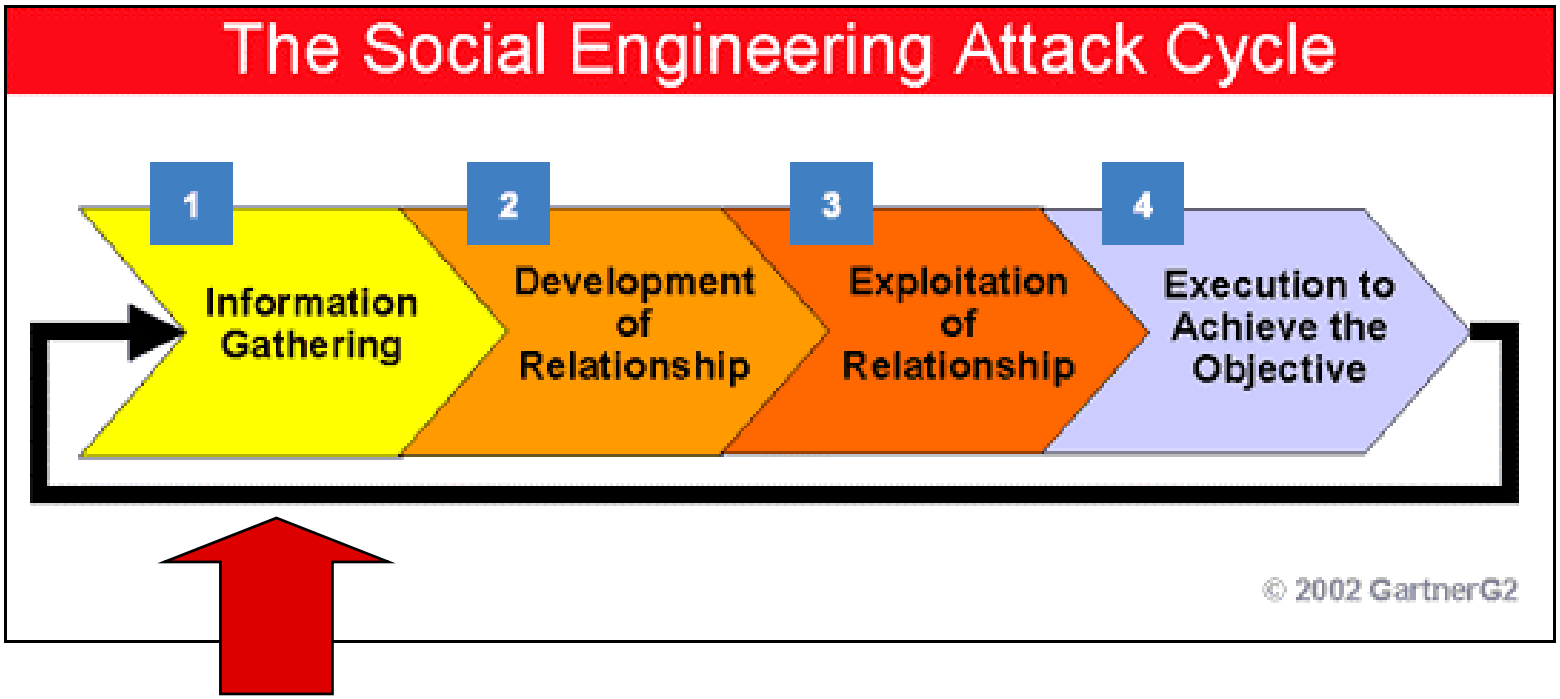
- **Legitimierung erzeugen**

  „Ich habe schon mit ihrer Kollegin Frau Maier gesprochen und die hat gesagt, sie würden mir gern helfen“
  (Referenz ausnutzen)

  „Ich habe ihren Chef, Herrn Schmidt auf einem Seminar getroffen. Ich weiß, dass er jetzt in Urlaub ist, aber er hat mir versprochen, sie würden mir helfen …..“
  (an Autorität appellieren)

  „Ja ich weiß, Regel 4711 sagt, dass sie mir das nicht sagen dürfen, aber sie werden einen Kollegen doch nicht im Regen stehen lassen“
  (Insiderwissen)

# Wo kommt das Insiderwissen her? Der Ablauf nach Gartner




- Ein Profi-Angriff ist mehrstufig. Jedes Telefonat fragt nur eine kleine, „fast öffentliche“ Zusatzinformation ab. Nach einigen Anrufen entsteht Insider-Wissen, das „legitimiert“

# Internes Wissen als Weg zum Vertrauen

- Internet-Recherchen, Presse (Namen von Angestellten, Struktur, Niederlassungen, Außenstellen, …)
- Urlaubsabwesenheitsnotizen („…bis zum xx.Aug. außer Haus“)
- Mehrere harmlose Telefonate, z.B. mit der Telefon-zentrale („wer ist bei Ihnen für xxx zuständig“ - „Ich bin zufriedener Kunde und möchte mich beim Chef bedanken.“)
- Wissen aus dem vorigen Interview dient beim nächsten als Legitimierung – Namen von Mitarbeitern führen zu Kostenstellen-Bezeichnungen, diese führen zu ….)

# Beispiel: der Legitimierungskette führt zum Vertrauensverhältnis

- 1. Telefonat → „Ich bin von einem Bonitätsdienst, welchen Bonitätsdienst benutzen sie derzeit?“
- 2. Telefonat → „Ich bin von Trust-Kredit, wir machen einen Zufriedensheitsumfrage….. Darf ich fragen, mit welchem von ihren Accounts bei uns Sie eigentlich arbeiten?“
- 3. Telefonat → „Ich bin Administrator von Trust-Kredit, es geht um ihren Account xxxx, ich brauche ihr Passwort für eine Account-Verifizierung“.

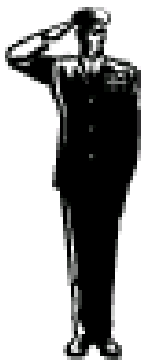
2002: Kriminelle spiegeln gegenüber Experian vor, Ford Motor Company zu sein und bekommen Kreditreports und Bankinformationen von 13 000 Menschen

# Weitere Wege zu Legitimierungen – Respekt vor Autoritäten ausnutzen

- **Äußerlichkeiten**
  Uniformen, Dienstkleidung (Polizei, Rettung, UPS, DHL,Monteur von Telekom, ….)
  „ich bin von EDS und muss ihre Rechner reparieren“ - Zoll Australien Sept. 2003

- **„Wichtige Person“ mit inhärenter Legitimierung**
  - Manager einer Auslandsniederlassung im sehr guten Anzug
  - Behördenvertreter, irgendeine Kontrollbehörde
  - Journalist vom xxx
  - IT-Administrator (der eigenen Firma oder eines Kunden oder Partners)
  - Consultant eines wichtigen Kundens

# Die Techniken im Detail: Angst vor Ärger ausnutzen, Einschüchtern



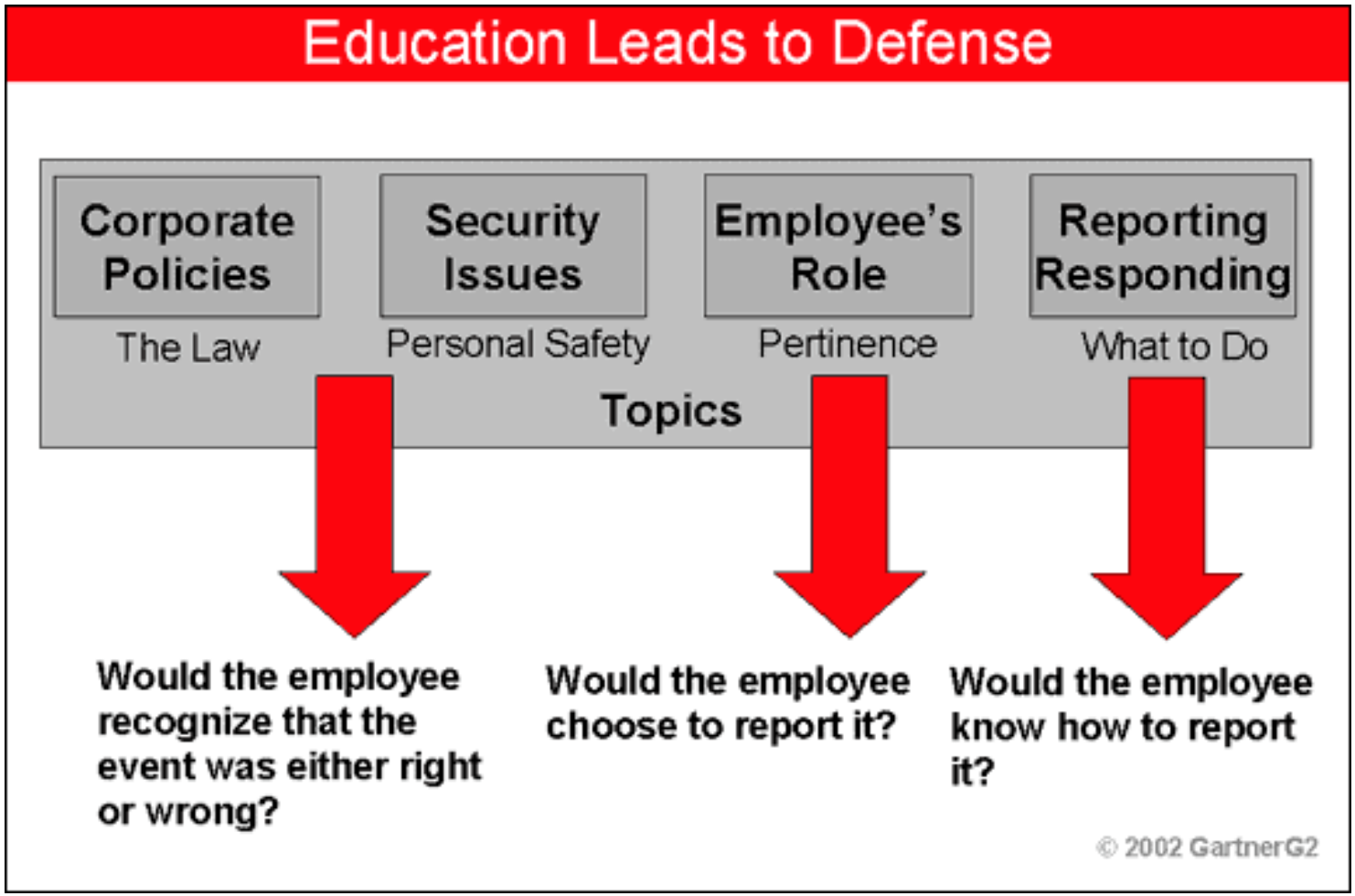
- **Großen Boss spielen, sich auf den großen Boss berufen** („wissen sie nicht, wer ich bin ?!?“)
- **Wichtigen Kunden spielen** (wütend, „bei uns steht die ganz IT, ich brauche dringend das Admin-Passwort“)
- **Wichtigen Geschäftspartner spielen** („wissen Sie eigentlich, wie viel Umsatz wir bei Ihnen machen?“)
- **Neue Mitarbeiter als Opfer aussuchen**

# Traditionelle Schutzversuche

- Strikte, aber abstrakte Regeln, notfalls mit Strafandrohung bei Übertretung durch die Mitarbeiter ….
- …. und dann den Mitarbeiter mit dem wütenden Kunden allein lassen
- Kundenfreundlichkeit als Leitziel, aber schlechte Abgrenzung zu Sicherheitsverletzungen

- Fehlendes Training,
  - wie Social Engineering Versuche erkannt werden,
  - keine Regelungen wie mit “harmlosen” Anfragen, z.B. nach Mitarbeiternamen und Verantwortlichkeiten umgegangen werden soll
  - kein Training, wie weit Hilfsbereitschaft und Kundenfreundlichkeit noch gehen soll

# Etwas bessere Schutzversuche



# Ansätze zum Schutz - Flexible, aber konsistente und sichere Regeln

- die Stärken und Schwächen der Mitarbeiter als Tatsache akzeptieren (wie z.B. starke Hilfsbereitschaft = Kundenfreundlichkeit)
- Im Service-Bereich: Durchführung einer Risikoanalyse um zu klären, welche Legitimierungsmechanismen leicht angreifbar sind (z.B. weil sie auf öffentlichen Daten beruhen, z.B. ZMR)
- Entwicklung von sicheren Legitimierungs-mechanismen, die doch benutzerfreundlich sind

Aktuelle Negativbeispiele: „Pretexting“-Diskussion rund um die Telefonrechnungen des HP-Aufsichtsrats, US-Telefongesellschaften erlauben den Abruf des Gesprächsnachweises gegen Angabe der Sozialversicherungssnummer.
http://derstandard.at/?url=/?id=2579821

# Ansätze zum Schutz - Regeln, die dem Mitarbeiter helfen, nicht behindern

- Klare Regelungen, was in der Kompetenz des Mitarbeiters liegt und was nicht
- Welche Hinweise deuten auf „Fischiges“?
- Erstellung von Regeln, die Hilfsbereitschaft ohne Sicherheitsverletzung erlauben, z.B.
  - Mehrere Mechanismen zur Legitimierung anbieten (die Mitarbeiter fragen, welche der Hilfsanfragen ihnen am meisten Probleme bereiten)
  - Alle diese Mechanismen durch geeignete Prozesse unterstützen
  - Eine zentrale Stelle anbieten, bei der Spezialanfragen „abgeladen“ werden können, oder nachträglich Anomalien berichtet werden können

# Ansätze zum Schutz – Training im Nein-Sagen Rollenspiele sind notwendig

- Wenn mit diesen Mitteln eine Legitimierung nicht hergestellt werden dem Mitarbeiter einen Katalog von freundlichen Optionen für Hilfsangebote zur Verfügung stellen

- “Nein” – aber dann ein Gegenangebot
  - “Können wir Sie später zurückrufen?”
  - „Leider nein, aber ich werde mich erkundigen und sie morgen zurückrufen“
- Rückzug hinter die Firmenrichtlinie („Sie haben bestimmt Verständnis, dass wir zum Schutz unserer Kunden …. – ich werde mit meinem Chef sprechen, ob in ihrem Fall …..“
- Keine Angst vor „großen Tieren“

# Trainingsvorschlag

- **Alle Mitarbeiter:**
  Was ist bei uns „vertraulich“?
  Was ist zwar nicht „vertraulich“, wird aber trotzdem nicht (am Telefon) ohne Legitimierung öffentlich bekannt gemacht (z.B. Handynummern, Zuständigkeiten)
- Telefonzentrale, Sekretärinnen:
  Rollenspiele, wie gehe ich mit wissbegierlichen Anrufern um:
  - „Diese Informationen können bei uns grundsätzlich nicht über Telefon weitergegeben werden.“
  - „Dürfen wir Sie zurückrufen?“
  - „Ich leite ihre Kontaktdaten gern an die Zuständigen weiter.“

# Notizen eines „hell-wachen“ IT-Mitarbeiters/Portiers/Rezeptionist/...

- Darf ICH diese Informationen weitergeben?
- Weiß ich, welche Legiti-mierungen notwendig sind?
- Wie kann ich die genannten Legitimierungen überprüfen?
- Wie sicher bin ich, dass er/sie ist, was er vorgibt?
- Warum fragt er gerade mich danach?
- warum kann ich nicht zurückrufen?

- Was könnte mit diesen Informationen in falschen Händen passieren?
- Was wären die Folgen?
- Wen kann ich (um diese Uhrzeit) um Hilfe bitten?
- Passiert etwas schlimmes, wenn ich zum “Kunden” erst mal Nein sage?
- Sollte ich diese Anfrage an jemanden berichten, an wen?

Habe ich ein sicheres Gefühl bei diesem Anrufer?

# Die „traditionellen“ Regeln behalten ihre Gültigkeit

- Hintergrundchecks für Mitarbeiter, aber auch Teilzeitkräfte
- Sicherheitsbestätigung für Fremdkräfte (Vertraulichkeitserklärung)
- Schneller Berichtsweg in Verdachtsfällen
- Routionemäßige Auswertung von Sicherheitslogs
- Mitarbeiter und Gäste brauchen sichtbare Ausweise auf dem Werksgelände
- Mitarbeiterzufriedenheit messen und verbessern
- Unternehmenskultur/Unternehmensethik als Schutzmechanismus
- Regelmäßige (wöchentliche) Kommunikation zu Sicherheitsfragen, spannend gemacht
- Belohnung für vorbildliches Verhalten

# Umfrage von Infosecurity Europe - 2004

http://www.infosec.co.uk/

- 34 Prozent der befragten Personen verrieten ihre Passwörter vollkommen freiwillig
- 79 Prozent der Befragten gaben unwissentlich Informationen bekannt, die zum digitalen Identitätsdiebstahl verwendet werden können
- Auf die Frage, ob das Passwort etwas mit dem Haustier oder eigenem Kind zu tun haben, verrieten 34 Prozent der befragten Personen ihr Codewort
- 71 Prozent der befragten Personen würden für ein Stück Schokolade das Passwort verraten
- Das ist ein Fortschritt, in 2003 wollten 90 Prozent der Befragten ihr Passwort für einen billigen Kugelschreiber verraten

# Fragen bitte

Skripten zu Sicherheitsthemen auf meiner Website:
http://sicherheitskultur.at/Eisbergprinzip.htm