

# Social Engineering

-

## das unterschätzte Risiko

Dr. René Hüsler, Leiter Institut für Sichere Softwaresysteme, HTA Luzern

Carlos Rieder, Leiter Competence Center IT-Security, HSW Luzern

Social Engineering / René Hüsler, Carlos Rieder  
2004 - 1

FACHHOCHSCHULE ZENTRALSCHWEIZ

**HTA**

ISIS → INSTITUT FÜR  
SICHERE SOFTWARESYSTEME

FACHHOCHSCHULE ZENTRALSCHWEIZ

**HSW**

IWI → INSTITUT FÜR  
WIRTSCHAFTSINFORMATIK LUZERN

## Agenda

- Einführung
- Vorgehen
- Praxiserfahrungen
- Abwehrmassnahmen

Social Engineering / René Hüsler, Carlos Rieder  
2004 - 2

FACHHOCHSCHULE ZENTRALSCHWEIZ FACHHOCHSCHULE ZENTRALSCHWEIZ

**HTA**

ISIS → INSTITUT FÜR  
SICHERE SOFTWARESYSTEME

**HSW**

IWI → INSTITUT FÜR  
WIRTSCHAFTSINFORMATIK LUZERN

# Einführung – Social Engineering (Quelle: Wikipedia)

- Begriff aus den frühen 70er Jahren
- Optimismus für Umgestaltung und Verbesserung der Gesellschaft durch:
  - rationale und
  - ingenieurmässige Methoden
- Beispiel:
  - Betonwüsten in Trabantenstädten



Social Engineering / René Hüsler, Carlos Rieder  
2004 - 3

FACHHOCHSCHULE ZENTRALSCHWEIZ FACHHOCHSCHULE ZENTRALSCHWEIZ

**HTA**

ISIS → INSTITUT FÜR  
SICHERE SOFTWARESYSTEME

**HSW**

IWI → INSTITUT FÜR  
WIRTSCHAFTSINFORMATIK LUZERN

## Social Engineering: Heute

Vorgehensweise zum

- nicht-technischen Ausspähen von Daten
  - Zugangsinformationen
  - Passwörter
  - Sicherheitsrelevante Informationen
  - Firmengeheimnisse

durch Kontakt zu Informationsträgern.

- Kunst und Wissenschaft Personen zum gewünschten Handeln zu bewegen – keine Hirnwäsche

Social Engineering / René Hüsler, Carlos Rieder  
2004 - 4

FACHHOCHSCHULE ZENTRALSCHWEIZ FACHHOCHSCHULE ZENTRALSCHWEIZ

**HTA**

ISIS → INSTITUT FÜR  
SICHERE SOFTWARESYSTEME

**HSW**

IWI → INSTITUT FÜR  
WIRTSCHAFTSINFORMATIK LUZERN

# Definition

- Umgehung von Sicherheitsvorkehrungen auf sozialer Ebene.
- Arten:
  - Mündlich (Telefon)
  - Persönlich
  - Auftreten etc.
- Verwenden von „Beziehungen“ zur Informations-Beschaffung



# Definition (cont'd)

- Funktioniert, durch
  - Gutgläubigkeit (bis Naivität)
  - Unwissenheit bezüglich Problematik
  - Unwissenheit bezüglich Sensitivität der Information
  - Unachtsamkeit
  - Vergesslichkeit
- Sicherheit beruht auf Vertrauen
- Angriffe durch SE passieren häufiger als man denkt
- Grösste Gefahr in heutiger Gesellschaft

# Ziele des Social Engineering

Grundsätzlich identisch mit Hacking im Allgemeinen

- Unerlaubter Zugriff auf Systeme oder Informationen
- Netzwerkeinbrüche
- Industriespionage
- Identitätsdiebstahl
- Stören des Systems allgemein
- etc.

**Vertrauen** in Social Engineer als Grundvoraussetzung

Social Engineering / René Hüsler, Carlos Rieder  
2004 - 7

FACHHOCHSCHULE ZENTRALSCHWEIZ FACHHOCHSCHULE ZENTRALSCHWEIZ

**HTA**

ISIS → INSTITUT FÜR  
SICHERE SOFTWARESYSTEME

**HSW**

IWI → INSTITUT FÜR  
WIRTSCHAFTSINFORMATIK LUZERN

# Vorgehensweise

- Auswahl eines geeigneten Ziels
- Informationsbeschaffung zur Zielfirma (Allg.)
  - Personen, Funktionen, Verantwortlichkeiten
  - Organigramm, Telefonnummern
  - Abwesenheiten, Hobby etc.
  - Bevorzugte Quelle: Internet
- Detailinformationen beschaffen
  - Physische Methode
  - Psychologische Methode

Social Engineering / René Hüsler, Carlos Rieder  
2004 - 8

FACHHOCHSCHULE ZENTRALSCHWEIZ FACHHOCHSCHULE ZENTRALSCHWEIZ

**HTA**

ISIS → INSTITUT FÜR  
SICHERE SOFTWARESYSTEME

**HSW**

IWI → INSTITUT FÜR  
WIRTSCHAFTSINFORMATIK LUZERN

# Physische Methode

- Rundgang in Räumlichkeiten des Ziels
  - Username / Password
  - Offene Rechner (Installation, Datenklau)
  - Hardware / Pläne etc.
  - Telefonbücher
- Durchsuchen des Abfalls (intern/extern)
  - Firmeninformationen, Geschäftsbeziehungen
  - Adressen / Kunden / Aufträge / Umsatz / Prognosen
- Nutzen dieser Info für späteren Angriff

Social Engineering / René Hüsler, Carlos Rieder  
2004 - 9

FACHHOCHSCHULE ZENTRALSCHWEIZ FACHHOCHSCHULE ZENTRALSCHWEIZ

**HTA**  
ISIS → INSTITUT FÜR  
SICHERE SOFTWARESYSTEME

**HSW**  
IWI → INSTITUT FÜR  
WIRTSCHAFTSINFORMATIK LUZERN

# Psychologische Methode

- Telefonanfragen
  - Häufigste Methode
  - Direkte Interaktion/Reaktion
  - Vorgabe einer anderen Person
- On-line SE
  - Gleiches Passwort wird mehrfach eingesetzt
  - Yahoo, Bluewin, amazon etc.
- Helpdesks liefern Informationen sehr leicht



Social Engineering / René Hüsler, Carlos Rieder  
2004 - 10

FACHHOCHSCHULE ZENTRALSCHWEIZ FACHHOCHSCHULE ZENTRALSCHWEIZ

**HTA**  
ISIS → INSTITUT FÜR  
SICHERE SOFTWARESYSTEME

**HSW**  
IWI → INSTITUT FÜR  
WIRTSCHAFTSINFORMATIK LUZERN



# Kevin Mitnick

“You could spend a fortune purchasing technology and services...  
and your network infrastructure could still remain vulnerable to old-fashioned manipulation.”



(Quelle: „My first RSA Conference“, Security Focus, April 30, 2001)

Social Engineering / René Hüsler, Carlos Rieder  
2004 - 13

FACHHOCHSCHULE ZENTRALSCHWEIZ FACHHOCHSCHULE ZENTRALSCHWEIZ

**HTA**

ISIS → INSTITUT FÜR  
SICHERE SOFTWARESYSTEME

**HSW**

IWI → INSTITUT FÜR  
WIRTSCHAFTSINFORMATIK LUZERN

## Praxisbericht

- Vorgehensplan
- Informationsbeschaffung
- Angriff
- Resultate

Social Engineering / René Hüsler, Carlos Rieder  
2004 - 14

FACHHOCHSCHULE ZENTRALSCHWEIZ FACHHOCHSCHULE ZENTRALSCHWEIZ

**HTA**

ISIS → INSTITUT FÜR  
SICHERE SOFTWARESYSTEME

**HSW**

IWI → INSTITUT FÜR  
WIRTSCHAFTSINFORMATIK LUZERN

# Vorgehensplan

- Suchen nach einem interessierten Partner
- Absprachen der zu untersuchenden Inhalte
- Schriftliche Definition der Rahmenbedingungen
- Vertraulichkeitsvereinbarung

Social Engineering / René Hüsler, Carlos Rieder  
2004 - 15

# Informationsbeschaffung

- Beschaffen von Hintergrundinformationen mit der Absicht ein „Vertrauensverhältnis“ aufbauen zu können.
  - Namen
  - Tätigkeiten
  - Hobbies
  - Vereine

Social Engineering / René Hüsler, Carlos Rieder  
2004 - 16

# Informationsbeschaffung - GOOGLE

- Infos über URL ☞ Informatik-Verantwortlicher
- Namenssuche ☞ Persönliche Informationen
  - Vereine
  - Interessen
  - Aktivitäten
- Raster Mailadressen aa.bb@xy.ch
- Suche nach Namen der Mitarbeitenden
  - xy AG + Ort des Unternehmens + gängige Vornamen
- Weitere Suchbegriffe
  - Lehrlinge
  - Abteilungen
  - ....
- Sportanlässe / Ranglisten mit Firmenangaben

Social Engineering / René Hüsler, Carlos Rieder  
2004 - 17

FACHHOCHSCHULE ZENTRALSCHWEIZ FACHHOCHSCHULE ZENTRALSCHWEIZ

**HTA**  
ISIS → INSTITUT FÜR  
SICHERE SOFTWARESYSTEME

**HSW**  
IWI → INSTITUT FÜR  
WIRTSCHAFTSINFORMATIK LUZERN

# Entwickeln eines Vorgehensplanes

- „Plausibles Geschehtli“ erfinden
- Gründe vorbereiten
  - Wieso brauchen wir die Information?
  - Wieso sind wir berechtigt diese Information zu bekommen?
- „Günstige“ Rahmenbedingungen schaffen
  - Mittagszeit
  - Kurz nach Arbeitsende
  - Ferienzeit
- Spuren verwischen / verschleiern
  - Unregistriertes Natel
  - Anonyme WebSite

Social Engineering / René Hüsler, Carlos Rieder  
2004 - 18

FACHHOCHSCHULE ZENTRALSCHWEIZ FACHHOCHSCHULE ZENTRALSCHWEIZ

**HTA**  
ISIS → INSTITUT FÜR  
SICHERE SOFTWARESYSTEME

**HSW**  
IWI → INSTITUT FÜR  
WIRTSCHAFTSINFORMATIK LUZERN

# Angriff – per Telefon

- Direktwahl
- Umfrage zu den „IT-Dienstleistungen“ im Auftrag der IT, Herr xy
  - Verfügbarkeit
  - Applikationen alle die nötig sind
  - Helpdesk effizient
  - SPAM Problematik gut gelöst, Mails verloren?
  - Virenschutz ausreichend
  - Informiert vorgehen Virenbefall
  - Allgemeines Wissen zur Sicherheit
  - Passwort Stärke, gute Passwörter sind ....
  - Wissen die IT-Leute Ihr Passwort
  - Was ist das PW?
  - Hardware genügend schnell, neue Maschine nötig
  - Weitere Geräte nötig Palm, Drucker, ...
- Oder
  - Ist Ihre Maschine auf dem neusten Sicherheitsstand?
  - Für die Einspielung aktuellster Sicherheits-Updates benötigen wir Usernamen und Passwort

Social Engineering / René Hüsler, Carlos Rieder  
2004 - 19

FACHHOCHSCHULE ZENTRALSCHWEIZ FACHHOCHSCHULE ZENTRALSCHWEIZ

**HTA**  
ISIS → INSTITUT FÜR  
SICHERE SOFTWARESYSTEME

**HSW**  
IWI → INSTITUT FÜR  
WIRTSCHAFTSINFORMATIK LUZERN

# Angriff – per Internet

- Web-Server-Umfrage
  - Anmelden der Umfrage per Mail mit [www.xy.ch](http://www.xy.ch) mit gefälschter Absenderadresse ([hans\\_muster@xy.ch](mailto:hans_muster@xy.ch)), als neuer Mitarbeiter der IT zuständig für Security.
  - Gleiches Look and Feel wie FirmenWebSite
  - Einbau Login Prozedur (evt. wie für den geschützten Bereich)
  - 5 Security Fragen stellen
  - Absenden

Social Engineering / René Hüsler, Carlos Rieder  
2004 - 20

FACHHOCHSCHULE ZENTRALSCHWEIZ FACHHOCHSCHULE ZENTRALSCHWEIZ

**HTA**  
ISIS → INSTITUT FÜR  
SICHERE SOFTWARESYSTEME

**HSW**  
IWI → INSTITUT FÜR  
WIRTSCHAFTSINFORMATIK LUZERN

## Angriff – per Internet

- Umfrage-Unternehmen  
„Schweizerisches Institut für Umfragen“
- Anfrage per Mail im Auftrag von xy (IT-Leiter im Unternehmen)
- Einfache Webseite gebaut
- Fünf Fragen zur Security
- „Passwort-Checker“ integriert

Social Engineering / René Hüsler, Carlos Rieder  
2004 - 21

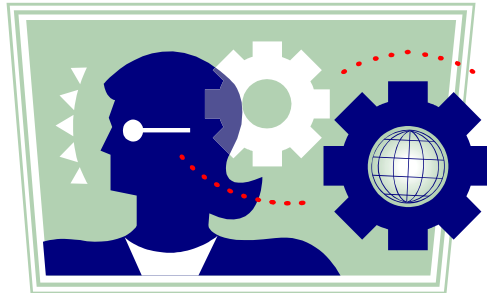
## Resultate

- Neun persönliche Anfragen an eine willkürliche Auswahl von Mitarbeitenden
- Eine Antwort mit Passwort
- Feedback, dass das Passwort besser gewechselt werden sollte
- URL wurde im Auftrag der IT des Unternehmens gesperrt

Social Engineering / René Hüsler, Carlos Rieder  
2004 - 22

# Schutzmassnahmen

- **SENSIBILISIERUNG**
- **GMV aktivieren**



Social Engineering / René Hüsler, Carlos Rieder  
2004 - 23

FACHHOCHSCHULE ZENTRALSCHWEIZ FACHHOCHSCHULE ZENTRALSCHWEIZ

**HTA**  
ISIS → INSTITUT FÜR  
SICHERE SOFTWARESYSTEME

**HSW**  
IWI → INSTITUT FÜR  
WIRTSCHAFTSINFORMATIK LUZERN

# Schutzmassnahmen

- Aufklärung
- Awareness fördern
- Ausbildung



Social Engineering / René Hüsler, Carlos Rieder  
2004 - 24

FACHHOCHSCHULE ZENTRALSCHWEIZ FACHHOCHSCHULE ZENTRALSCHWEIZ

**HTA**  
ISIS → INSTITUT FÜR  
SICHERE SOFTWARESYSTEME

**HSW**  
IWI → INSTITUT FÜR  
WIRTSCHAFTSINFORMATIK LUZERN

# Schutzmassnahmen



- Aufmerksam sein!
- Ungewöhnliche Anliegen hinterfragen!
- Sich nicht unter Druck setzen lassen!
- Bei Zweifel nicht zuerst helfen, sondern Abklärungen machen und zurückrufen!
- Informationen nur an berechtigte Personen weiterleiten!
- E-Mails an Mitarbeiter nur an die Firmen E-Mail Adresse senden und nicht an private E-Mail Adressen!
- Bei Hilfe von Unbekannten skeptisch ein!
- Keine Software von „Unbekannten“ entgegennehmen und installieren!
- Vorsicht beim Öffnen von E-Mail-Anhängen!
- Keine Firmen-Passwörter und Usernamen im Internet verwenden!

Social Engineering / René Hüsler, Carlos Rieder  
2004 - 25

FACHHOCHSCHULE ZENTRALSCHWEIZ FACHHOCHSCHULE ZENTRALSCHWEIZ

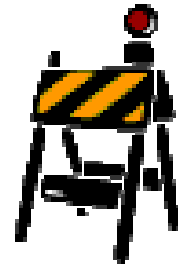
**HTA**

ISIS → INSTITUT FÜR  
SICHERE SOFTWARESYSTEME

**HSW**

IWI → INSTITUT FÜR  
WIRTSCHAFTSINFORMATIK LUZERN

# Schutzmassnahmen



- Gefahrenbewusstsein ist auszubauen
- Bewusstes Hinterfragen der Tätigkeiten
- Reduktion der frei verfügbaren Informationen
  - Namenslisten
  - Ansprechpartner

Social Engineering / René Hüsler, Carlos Rieder  
2004 - 26

FACHHOCHSCHULE ZENTRALSCHWEIZ FACHHOCHSCHULE ZENTRALSCHWEIZ

**HTA**

ISIS → INSTITUT FÜR  
SICHERE SOFTWARESYSTEME

**HSW**

IWI → INSTITUT FÜR  
WIRTSCHAFTSINFORMATIK LUZERN

# Social Engineering – Alter Wein in neuen Schläuchen

**“... still remain vulnerable to old-  
fashioned manipulation.”**

(Quelle: Kevin Mitnick „My first RSA Conference“, Security Focus, April 30, 2001)

Social Engineering / René Hüsler, Carlos Rieder  
2004 - 27

FACHHOCHSCHULE ZENTRALSCHWEIZ

**HTA**

ISIS → INSTITUT FÜR  
SICHERE SOFTWARESYSTEME

FACHHOCHSCHULE ZENTRALSCHWEIZ

**HSW**

IWI → INSTITUT FÜR  
WIRTSCHAFTSINFORMATIK LUZERN



[rhuesler@hta.fhz.ch](mailto:rhuesler@hta.fhz.ch)

[crieder@hsw.fhz.ch](mailto:crieder@hsw.fhz.ch)

Social Engineering / René Hüsler, Carlos Rieder  
2004 - 28

FACHHOCHSCHULE ZENTRALSCHWEIZ

**HTA**

ISIS → INSTITUT FÜR  
SICHERE SOFTWARESYSTEME

FACHHOCHSCHULE ZENTRALSCHWEIZ

**HSW**

IWI → INSTITUT FÜR  
WIRTSCHAFTSINFORMATIK LUZERN