

Die Psychologischen Grundlagen des Social Engineerings

Stefan Schumacher

www.kaishakunin.com

GUUG Frühjahrsfachgespräch
Karlsruhe
13.-14. März 2009

解
積
人

Über mich

- freier Unternehmensberater (Kaishakunin.com) mit Schwerpunkt auf Social Engineering, Security Awareness, Counter Intelligence und Security Management
- Student der Bildungswissenschaft und Psychologie an der Uni Magdeburg (Ex-Ingenieurinformatik/E-Technik)
- Chefororganisator des Magdeburger Open-Source-Tages
- NetBSD-Entwickler (Stefan@NetBSD.org)
Vorsitzender des NetBSD Deutschland e.V.
- Hobbies: Kryptographie, Sicherheit, angewandte Sozialpsychologie

解
积
人

Table of Contents

- 1 Grundlagen
- 2 Reziprozität
- 3 Commitment und Konsistenz
- 4 Soziale Bewährtheit
- 5 Obedience to Authority
- 6 Sympathie
- 7 Knappheit

Table of Contents

- 1 Grundlagen
- 2 Reziprozität
- 3 Commitment und Konsistenz
- 4 Soziale Bewährtheit
- 5 Obedience to Authority
- 6 Sympathie

解
积
人

Social Engineering

Was ist Social Engineering?

- Eine Theorie der Soziologie / Massen-/Sozialpsychologie
- Idee: Massen zu einem vorhersagbaren, festgelegten Verhalten zu bewegen
- Totalitäre Gesellschaften mögen das: Reichsparteitage, 1. Mai, Olympische Spiele, ...
- Romane: *Wir* (Jewgenij Samjatin), 1984, *Brave New World*

解
积
人

Social Engineering

Was ist Social Engineering?

- Hacking/IT-Security:
- »technische Sicherheitsmaßnahmen« werden durch menschliches Verhalten umgangen
- »Hacking People«
- Missbrauch der allgemeinen Psychologie
- Warum sollte ich `/etc/master.passwd` cracken, wenn ich doch einen Benutzer dazu bringen kann, mir sein Passwort zu geben.

解
釈
人

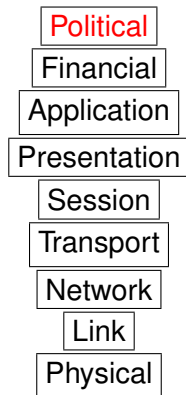
Social Engineering

Was ist Social Engineering?

- Hacking/IT-Security:
- »technische Sicherheitsmaßnahmen« werden durch menschliches Verhalten umgangen
- »Hacking People«
- Missbrauch der allgemeinen Psychologie
- Warum sollte ich `/etc/master.passwd` cracken, wenn ich doch einen Benutzer dazu bringen kann, mir sein Passwort zu geben.

解
釈
人

OSI-Layer 9



解
积
人

Grundlagen

Fixed Action Patterns

- Verhaltensbiologen entdeckten *Fixed Action Patterns*
- Konrad Lorenzens Graugänse
- Experiment nach M. W. Fox (1974)
 - ausgestopftes Wiesel mit Lautsprecher
 - Truthenne hat Wiesel attackiert (natürlicher Feind)
 - Lautsprecher spielte Trutküken-Tschiep-Tschiep
 - Truthenne akzeptierte Wiesel als Trutküken
 - in der Natur macht ein Wiesel nicht Tschiep-Tschiep
- Kuckuck, Knut, ...

解
釈
人

Grundlagen

stereotypes Verhalten

Wir sind auch nur Tiere

- fight-or-flight-Reaktion (Flucht oder Kampf)
- Teuer ist gut (Mercedes, Miele, Chivas Regal)
etwas *billigen*
- Experten wissen wovon sie reden ...
- eine gutaussehende Frau geht vorbei ...
- Frauen und Schuhläden ...
- Der erste Eindruck ist sehr wichtig
- Deshalb laufe ich nicht mehr im Metallica-Shirt rum ;-)

解
釈
人

Grundlagen

stereotypes Verhalten

Wir sind auch nur Tiere

- fight-or-flight-Reaktion (Flucht oder Kampf)
- Teuer ist gut (Mercedes, Miele, Chivas Regal)
etwas *billigen*
- Experten wissen wovon sie reden ...
- eine gutaussehende Frau geht vorbei ...
- Frauen und Schuhläden ...
- Der erste Eindruck ist sehr wichtig
- Deshalb laufe ich nicht mehr im Metallica-Shirt rum ;-)

解
釈
人

Grundlagen

stereotypes Verhalten

- automatisiertes, stereotypes Verhalten ist die effizienteste Verhaltensform
- Unsere Welt ist zu schnell und zu komplex um jede Entscheidung zu analysieren
- *Urteilsheuristiken* als Entscheidungsmakros werden durch *Auslösemerkmale* ausgelöst
- Auslösemerkmale sind tlw. kulturabhängig (ehre die Alten, Frauen sind wertlos)
- *kontrolliertes Verhalten* aufgrund sorgfältiger Analyse nur, wenn die Entscheidung als wichtig empfunden wird
- Wir erwarten von unseren Beratern kontrolliertes Verhalten

解
釈
人

stereotypes Verhalten

Wahrnehmungskontraste

- Wir reagieren auf Unterschiede/Kontraste
- Experiment: 3 Wassereimer: kalt, warm, heiß
- linke Hand in kaltes, rechte Hand in heißes Wasser
- dann beide Hände in warmes Wasser

Table of Contents

1 Grundlagen

2 Reziprozität

3 Commitment und Konsistenz

4 Soziale Bewährtheit

5 Obedience to Authority

6 Sympathie

Reziprozität

Grundlagen

- einen Gefallen zurückzahlen
- Reziprozität existiert in *allen* Kulturen
- Leaky & Lewin (1978) behaupten das wie Menschen sind, weil wir Nahrung und Kompetenzen in einem respektierten Netz aus Verpflichtungen teilen
- Gesellschaften gewinnen durch Reziprozität
- Reziprozität soll uns beim durchbrechen der »grauen Barriere« geholfen haben
- könnte biologistische Ursachen haben

解
积
人

Reziprozität

Beispiel

- 1985 erschütterte ein Erdbeben Mexiko, Äthiopien hungerte (Band Aid)
- Das Äthiopische Rote Kreuz hat Mexiko 5,000\$ gespendet
- 1935 hat Mexiko Äthiopien geholfen, als es von Italien angegriffen wurde
- Das ÄRK spürte den Drang zu helfen
- Ebenso: freie Kostproben im Supermarkt, 5\$-Scheck im Voraus bei Fragebögen

解
积
人

Reziprozität

Beispiel

- 1985 erschütterte ein Erdbeben Mexiko, Äthiopien hungerte (Band Aid)
- Das Äthiopische Rote Kreuz hat Mexiko 5,000\$ gespendet
- 1935 hat Mexiko Äthiopien geholfen, als es von Italien angegriffen wurde
- Das ÄRK spürte den Drang zu helfen
- Ebenso: freie Kostproben im Supermarkt, 5\$-Scheck im Voraus bei Fragebögen

解
积
人

Reziprozität

Macht

- Reziprozität kann Antipathie überladen: Gastgeschenke
- Reziprozität kann zu ungleichem Ausgleich führen
- *jede* Gesellschaft erzwingt Reziprozität durch sozialen Druck
- mit Ausnahmen: wenn die »Beschenkten« nichts zurückgeben können (Kinder)

解
积
人

Reziprozität

etwas subtiler:

- ein Eingeständnis machen, das wird als Geschenk betrachtet \rightsquigarrow Reziprozität
- Kannst du mir 100€ leihen? Nein? Vielleicht 10?
- Sie müssen alle 14 Tage ihr Passwort wechseln, es muss 30 Zeichen lang sein!
OK, und wenn sie monatlich wechseln und 12 Zeichen nehmen?
- Kontrast spielt auch mit

解
釈
人

Reziprozität

Abwehr

- Geschenke ablehnen ist schwer (Japan)
- Es gibt immer großzügige Menschen (Wir sind kein Homo Öconomicus!)
- Gefallen akzeptieren, *aber* wenn er sich als Trick herausstellt, sollte man die Reziprozität ignorieren

解
积
人

Table of Contents

1 Grundlagen

2 Reziprozität

3 Commitment und Konsistenz

4 Soziale Bewährtheit

5 Obedience to Authority

6 Sympathie

Commitment und Konsistenz

Theorie des Commitment

- Der Wunsch nach Konsistenz wird als zentrale Verhaltensgrundlage betrachtet
- Konsistenz wird geschätzt und erwartet (vgl. Luhmanns »Vertrauen«)
- Inkonsistenz wird gewöhnlich als unerwünschte Verhaltensweise betrachtet
- Inkonsistenz wird häufig als geistige Störung betrachtet

解
积
人

Commitment und Konsistenz

Example

- Ein Assistent ging zum Strand um sich zu sonnen und nahm ein Kofferradio mit
- nach 10min holte er sich etwas zu trinken
- ein anderer Assistent griff sich das Radio und verschwand damit
- 4/10 VPn hielten den Dieb auf
- im 2. Durchlauf bat der 1. Assistent seine Nachbarn auf das Radio zu achten
- 19/20 VPn stoppten den Dieb
- einige sogar mit Gewalt

解
釈
人

Commitment und Konsistenz

Example

- Ein Assistent ging zum Strand um sich zu sonnen und nahm ein Kofferradio mit
- nach 10min holte er sich etwas zu trinken
- ein anderer Assistent griff sich das Radio und verschwand damit
- 4/10 VPn hielten den Dieb auf
- im 2. Durchlauf bat der 1. Assistent seine Nachbarn auf das Radio zu achten
- 19/20 VPn stoppten den Dieb
- einige sogar mit Gewalt

解
釈
人

Commitment und Konsistenz

Warum funktioniert Konsistenz?

- Wie kann man konsistentes Verhalten missbrauchen? Was löst konsistentes Verhalten aus?
- Ein sog. Commitment löst konsistentes Verhalten aus (bspw. Versprechen, auf Treu und Glauben)
- Das Commitment muss freiwillig, ohne Druck oder Belohnung gemacht werden
- aktives Opt-In ist das beste Commitment
- ein Commitment kann das Selbstbild einer Person verändern
- »win the hearts and minds« of your workforce

解
釈
人

Commitment und Konsistenz

Beispiele

- Initiationsriten (Armee, Burschenschaften, ...)
- initiierte Personen unterstützen die Gruppe besser und finden die Gruppe auch besser

Commitment und Konsistenz

Abwehr

- Commitment und Konsistenz können nicht einfach ignoriert werden
- höre auf deine Bauchsignale, wir haben immer noch unsere Instinkte
- höre auf dein Herz, das ist etwas sensibler als der Bauch
- Würde ich mich wieder so verhalten, wie ich es gerade tue?

解
积
人

Commitment und Konsistenz

Zusammenfassung

- persönliche Konsistenz wird von der Gesellschaft erwartet und wertgeschätzt
- Konsistenz vereinfacht das komplexe tägliche Leben
- Nach einem Commitment sind Menschen gewillter, Anfragen zu erfüllen, wenn diese in ihr Commitment passen
- sogar falsche Commitments können selbst-erfüllend werden

解
积
人

Table of Contents

- 1 Grundlagen
- 2 Reziprozität
- 3 Commitment und Konsistenz
- 4 Soziale Bewährtheit**
- 5 Obedience to Authority
- 6 Sympathie

解
积
人

Soziale Bewährtheit

Prinzip

- wir entscheiden was korrekt ist, indem wir herausfinden, was andere Menschen für korrekt halten
- eine Handlung gilt als korrekt, wenn andere sie auch vollziehen
- wenn alle von der Brücke springen würden ...
- funktioniert sehr gut, wenn Menschen unsicher sind (Luxemburg)
- funktioniert sehr gut, wenn die Referenzen uns ähnlich sind (Teenager)

解
积
人

Soziale Bewährtheit

Beispiele

- Gelächter vom Band in TV-Sendungen
- Jemand der den Kirchturm anstarrt
- Jeder kauft/nutzt/tut X
- Banken crashen (Malaysia 1999)
- Stampedes
- affektive Desensibilisierung mittels Video möglich (Kinder/Hunde)
- Passive Bystander

解
积
人

Soziale Bewährtheit

Anwendung

- Wenn die Mehrheit die Sicherheitsrichtlinie ignoriert, haben Sie verloren
- Wenn die Mehrheit die Sicherheitsrichtlinie beachtet, haben Sie gewonnen
- kritische Masse erreichen und ausnutzen

解
积
人

Table of Contents

- 1 Grundlagen
- 2 Reziprozität
- 3 Commitment und Konsistenz
- 4 Soziale Bewährtheit
- 5 Obedience to Authority**
- 6 Sympathie

解
积
人

Obedience to Authority

- Stanley Milgram
- Stanford Prison
- Wir glauben an Autoritäten, Rollenmodelle
- Überraschung hilft

解
积
人

Obedience to Authority

- When reacting to authority in an automatic fashion, there is a tendency to do so in response to the mere symbols of authority rather than to its substance.
Forschung: Titel, Kleidung, Automobile
- Krankenschwestern

Table of Contents

- 1 Grundlagen
- 2 Reziprozität
- 3 Commitment und Konsistenz
- 4 Soziale Bewährtheit
- 5 Obedience to Authority
- 6 Sympathie**

解
积
人

Sympathie

Prinzip

- wir werden eher von Menschen beeinflusst, die wir mögen
- Ein Rat unter Freunden ...
- Marketingmasche (Dove, Shampoo)
- Susanne Klatten

解
积
人

Sympathie

Warum finden wir Menschen sympathisch?

- physische Attraktivität (Halos)
- Ähnlichkeit (gespiegelte Fotos)
- Komplimente/Sympathie/Liebe (Romeo-Agenten)
- Konditionierung und Assoziation
(Klingelt es beim Namen *Pawlow*?)

解
积
人

Sympathie

Warum finden wir Menschen sympathisch?

- physische Attraktivität (Halos)
- Ähnlichkeit (gespiegelte Fotos)
- Komplimente/Sympathie/Liebe (Romeo-Agenten)
- Konditionierung und Assoziation
(Klingelt es beim Namen *Pawlow*?)
- zusammenarbeiten und erfolgreich sein (Sherif)

解
积
人

Sympathie

Warum finden wir Menschen sympathisch?

- physische Attraktivität (Halos)
- Ähnlichkeit (gespiegelte Fotos)
- Komplimente/Sympathie/Liebe (Romeo-Agenten)
- Konditionierung und Assoziation
(Klingelt es beim Namen *Pawlow*?)
- zusammenarbeiten und erfolgreich sein (Sherif)

解
积
人

Sympathie

Abwehr

- Hören Sie auf Ihre Gefühle
- Versucht jemand von mir gemocht zu werden?
- Betont jemand Ähnlichkeit? (Verkaufsmasche)

解
釈
人

Table of Contents

- 1 Grundlagen
- 2 Reziprozität
- 3 Commitment und Konsistenz
- 4 Soziale Bewährtheit
- 5 Obedience to Authority
- 6 Sympathie

解
积
人

Knappheit

- Less is best and loss is worst
- limitierte Ausgabe (special limited edition)
- begrenzte Angebote (Time Life)
- Zensur (W0lfenste1n, D00m)
- Ebay/Auktionen
- Terrible Two

解
积
人

Knappheit

- Entscheidungsmöglichkeiten gelten als wertvoller, wenn sie weniger verfügbar sind
- Dinge an die man schwerer rannkommt sind in der Regel wertvoller
- Wenn Dinge weniger verfügbar werden, verlieren wir Freiheitsgrade
- Wenn man Informationen einschränkt, wollen Menschen diese umso mehr bekommen und schätzen sie auch wertvoller ein (Beraterparadoxon)
- niemals einer einzelnen Informationsquelle vertrauen

解
釈
人

Knappheit

- Entscheidungsmöglichkeiten gelten als wertvoller, wenn sie weniger verfügbar sind
- Dinge an die man schwerer rannkommt sind in der Regel wertvoller
- Wenn Dinge weniger verfügbar werden, verlieren wir Freiheitsgrade
- Wenn man Informationen einschränkt, wollen Menschen diese umso mehr bekommen und schätzen sie auch wertvoller ein (Beraterparadoxon)
- niemals einer einzelnen Informationsquelle vertrauen

解
釈
人

Biologische Psychologie

- Neuropeptid Oxytozin beeinflusst Bindungsverhalten
- Gibt es überhaupt einen freien Willen? (Aktionspotentiale)
- Ratio vs. Emotio
- Neuroökonomie

解
积
人

Fazit

- Social Engineering nutzt grundlegendes menschliches Verhalten aus
- Kognitive Prozesse werden durch emotionale Reaktionen unterdrückt
- Security-Awareness-Kampagnen können das Sicherheitsbewusstsein erhöhen
- menschliches Verhalten ist weder deterministisch noch determinierend

解
积
人

Fazit

- Es gibt keinen Schutz vor Social Engineering
- Es gibt keine 100%ige Sicherheit
- »Sicherheit« ist ein latentes soziales Konstrukt und keine Naturkonstante
- Resiliente Systeme entwerfen, die Social Engineering beachten
- Häufiger Schwachpunkt: Authentifikation, aber: Computer können keinen Sinn stiften
- Verteidigung in der Tiefe mit überlappenden Mechanismen (Clausewitz: Vom Kriege)

解
釈
人

Literatur

- Robert Cialdini: Die Psychologie des Überzeugens
- Kevin Mitnick: Die Kunst der Täuschung; Die Kunst des Einbruchs
- Niklas Luhmann: Vertrauen; Die Gesellschaft der Gesellschaft
- Ulrich Beck: Die Risikogesellschaft; Weltrisikogesellschaft
- Richard Sennet: Der flexible Mensch

解
积
人

TERMINATOR:

THE SARAH CONNOR CHRONICLES

解
积
人

Fragen?
Stefan.Schumacher@Kaishakunin.com

Folien: www.Kaishakunin.com

解
积
人