Die psychologischen Grundlagen des Social Engineerings

— Mindfucking for Nerds —

Stefan Schumacher

Magdeburger Institut für Sicherheitsforschung

2011-08-11

Chaos Communication Camp 2011

Über mich

- Bildungswissenschaftler und Psychologe
- Direktor des Magdeburger Instituts für Sicherheitsforschung
- Herausgeber des Magdeburger Journals für Sicherheitsforschung (Open Access, zitierfähig)
- `www.Sicherheitsforschung-Magdeburg.de`
- Forschungsprogramm zu Social Engineering, Didaktik der Sicherheit/Kryptographie, u.v.a.m.

- **Psychologische Grundlagen des Social-Engineering**
  in: *Proceedings des GUUG Frühjahrsfachgespräches 2009*
  S. 77-98, 2009, Lehmanns Media Berlin, ISBN: 978-3-86541-322-2
- **Psychologische Grundlagen des Social-Engineering**
  in: *Die Datenschleuder. Das wissenschaftliche Fachblatt für den Datenreisenden*
  S. 52-59, 2010, Chaos Computer Club Hamburg, ISSN: 0930-1054 *(nicht zitierfähig)*
- **Die psychologischen Grundlagen des Social Engineerings**
  in: *Magdeburger Journal zur Sicherheitsforschung*, 01/2011, S. 1-26
  `http://www.wissens-werk.de/index.php/mjs/article/view/74`

Inhalt

Table of Contents

Social Engineering

Was ist Social Engineering? (ursprünglich)

- Karl Popper (1945) The Open Society and Its Enemies
- 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*

Social Engineering

Was ist Social Engineering? (Hacking)

- »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.

Social Engineering

Was ist Social Engineering? (Hacking)

- »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.

OSI-Layer 9

Political
Financial
Application
Presentation
Session
Transport
Network
Link
Physical

Grundlagen

Fixed Action Patterns

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

Grundlagen

stereotypes Verhalten

Wir sind auch nur Tiere

- fight-or-flight-Reaktion (Flucht oder Kampf)
- Teuer ist gut (Mercedes, Miele, Chivas Regal)
- Experten wissen wovon sie reden ...
- Frauen und Schuhläden ...
- Der erste Eindruck ...

Grundlagen

stereotypes Verhalten

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

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

Reziprozität

Grundlagen

- einen Gefallen zurückzahlen/eine Hand wäscht die andere
- Gesellschaften gewinnen durch Reziprozität
- Reziprozität existiert in *allen* Kulturen
- könnte biologistische Ursachen haben
- Leaky & Lewin (1978) behaupten das wir Menschen sind, weil wir Nahrung und Kompetenzen in einem respektierten Netz aus Verpflichtungen teilen

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, Geschäftsessen

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, Geschäftsessen

Reziprozität

etwas subtiler:

- ein Eingeständniss machen, das wird als Geschenk betrachtet $\rightsquigarrow$ Reziprozität
- Kannst du mir 100€ leihen? Nein? Vielleicht 10?
- Kontrast spielt auch mit

Table of Contents

Commitment und Konsistenz

Theorie des Commitment

- Konsistenz: sich erwartungsgemäß/wie angekündigt verhalten
- Der Wunsch nach Konsistenz wird als zentrale Verhaltensgrundlage betrachtet
- Konsistenz wird geschätzt und erwartet (vgl. Niklas Luhmann »Vertrauen als Mittel zur Reduktion sozialer Komplexität«)
- Inkonsistenz wird gewöhnlich als unerwünschte Verhaltensweise betrachtet
- Inkonsistenz wird häufig als geistige Störung betrachtet

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

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

Commitment und Konsistenz

Warum funktioniert Konsistenz?

- Was löst konsistentes Verhalten aus?
- Ein 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

Commitment und Konsistenz

Beispiele

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

Table of Contents

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
- funktioniert sehr gut, wenn die Referenzen uns ähnlich sind (Teenager)

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

Table of Contents

Obedience to Authority

- Stanley Milgram:
- 40 VPn, Lernexperiment mit Wortpaaren
- bei falscher Antwort: Stromstoß
- 15V, 30V, 45V ... 450V
- 40VPn bis 300V, 26VPn bis 450V (65%)
- UV: Autorität des VL, Distanz zwischen VPn
- aber: Nervenzusammenbrüche der VPn

Obedience to Authority

- Stanley Milgram:
- 40 VPn, Lernexperiment mit Wortpaaren
- bei falscher Antwort: Stromstoß
- 15V, 30V, 45V ... 450V
- 40VPn bis 300V, 26VPn bis 450V (65%)
- UV: Autorität des VL, Distanz zwischen VPn
- aber: Nervenzusammenbrüche der VPn
- Stanford Prison, Affenherden und Karamellbonbons
- Wir glauben an Autoritäten, Rollenmodelle, Überraschung hilft

Obedience to Authority

- Stanley Milgram:
- 40 VPn, Lernexperiment mit Wortpaaren
- bei falscher Antwort: Stromstoß
- 15V, 30V, 45V ... 450V
- 40VPn bis 300V, 26VPn bis 450V (65%)
- UV: Autorität des VL, Distanz zwischen VPn
- aber: Nervenzusammenbrüche der VPn
- Stanford Prison, Affenherden und Karamellbonbons
- Wir glauben an Autoritäten, Rollenmodelle, Überraschung hilft

Obedience to Authority

- Menschen reagieren auf *Symbole* der Authorität
  Forschung: Titel, Kleidung, Automobile
- Krankenschwestern (`r.ear`)

Table of Contents

Sympathie

Prinzip

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

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*?)

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 (Muzafer Sherif)

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 (Muzafer Sherif)

Table of Contents

Knappheit

- limitierte Ausgabe (special limited edition)
- begrenzte Angebote (Time Life)
- Zensur (Wolfenste1n, Doom)
- Ebay/Auktionen

Knappheit

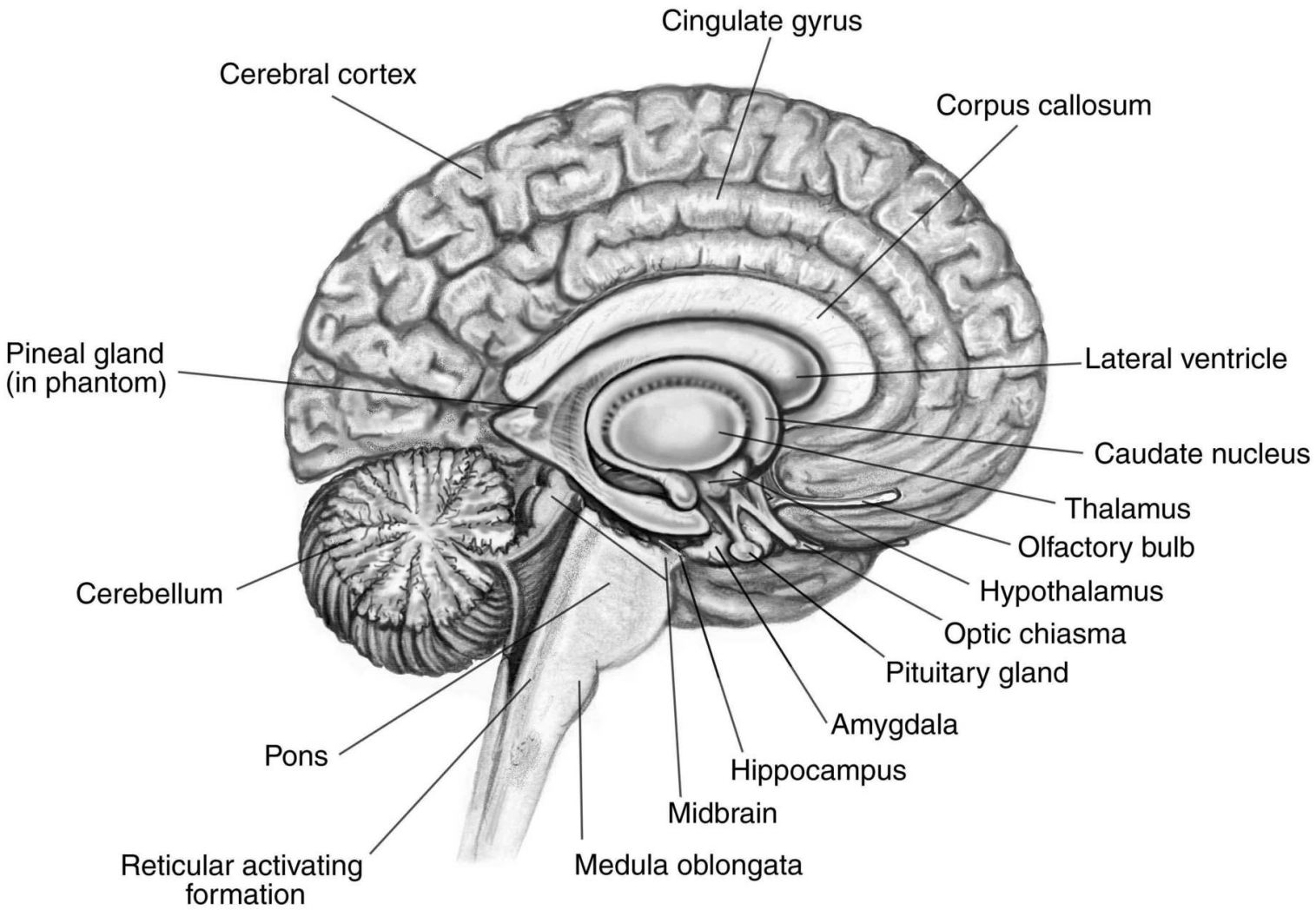
- Entscheidungsmöglichkeiten gelten als wertvoller, wenn sie weniger verfügbar sind
- Dinge an die man schwerer rannkommt sind in der Regel wertvoller
- Wenn Dinge weniger verfügbar werden, verlieren wir Freiheitsgrade
- Wenn man Informationen einschränkt, wollen Menschen diese umso mehr bekommen und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

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

Biologische Psychologie

- endogenes Neuropeptid Oxytozin, generiert im Nucleus paraventricularis und Nucleus supraopticus
- Zwischenspeicherung in der Hypophyse
- senkt Blutdruck und Cortisol, wirkt sedierend, verringert Stress
- Bindungsverhalten, z.B. zwischen Mutter und Säugling
- Ditzena et. al. (2006) Effects of social support and oxytocin on psychological and physiological stress responses during marital conflict
- ggw. Forschung: Sozialphobien, Schizophrenie, Autismus/Asperger


Cingulate gyrus
Cerebral cortex
Corpus callosum
Pineal gland
(in phantom)
Lateral ventricle
Caudate nucleus
Thalamus
Olfactory bulb
Cerebellum
Hypothalamus
Optic chiasma
Pituitary gland
Amygdala
Pons
Hippocampus
Midbrain
Reticular activating
formation
Medula oblongata

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

Fazit

- Es gibt keine 100%ige Sicherheit und damit auch keinen 100%igen Schutz vor Social Engineering
- Resiliente Systeme entwerfen, die Social Engineering beachten
- psychische und soziale Systeme beachten
- Häufiger Schwachpunkt: Authentifikationsmechanismen

Literatur

- (Bibliographie im Artikel)
- Robert Cialdini: Die Psychologie des Überzeugens
- Kevin Mitnick: Die Kunst der Täuschung; Die Kunst des Einbruchs
- Niklas Luhmann: Vertrauen; Die Gesellschaft der Gesellschaft, Soziologie des Risikos
- Ulrich Beck: Die Risikogesellschaft; Weltrisikogesellschaft

Fragen?

Stefan.Schumacher@
Sicherheitsforschung-Magdeburg.de