Social Engineering und Security Awareness für Systemadministratoren

Stefan Schumacher

Magdeburger Institut für Sicherheitsforschung
stefan.schumacher@sicherheitsforschung-magdeburg.de

SLAC2016

Über Mich

Über Mich

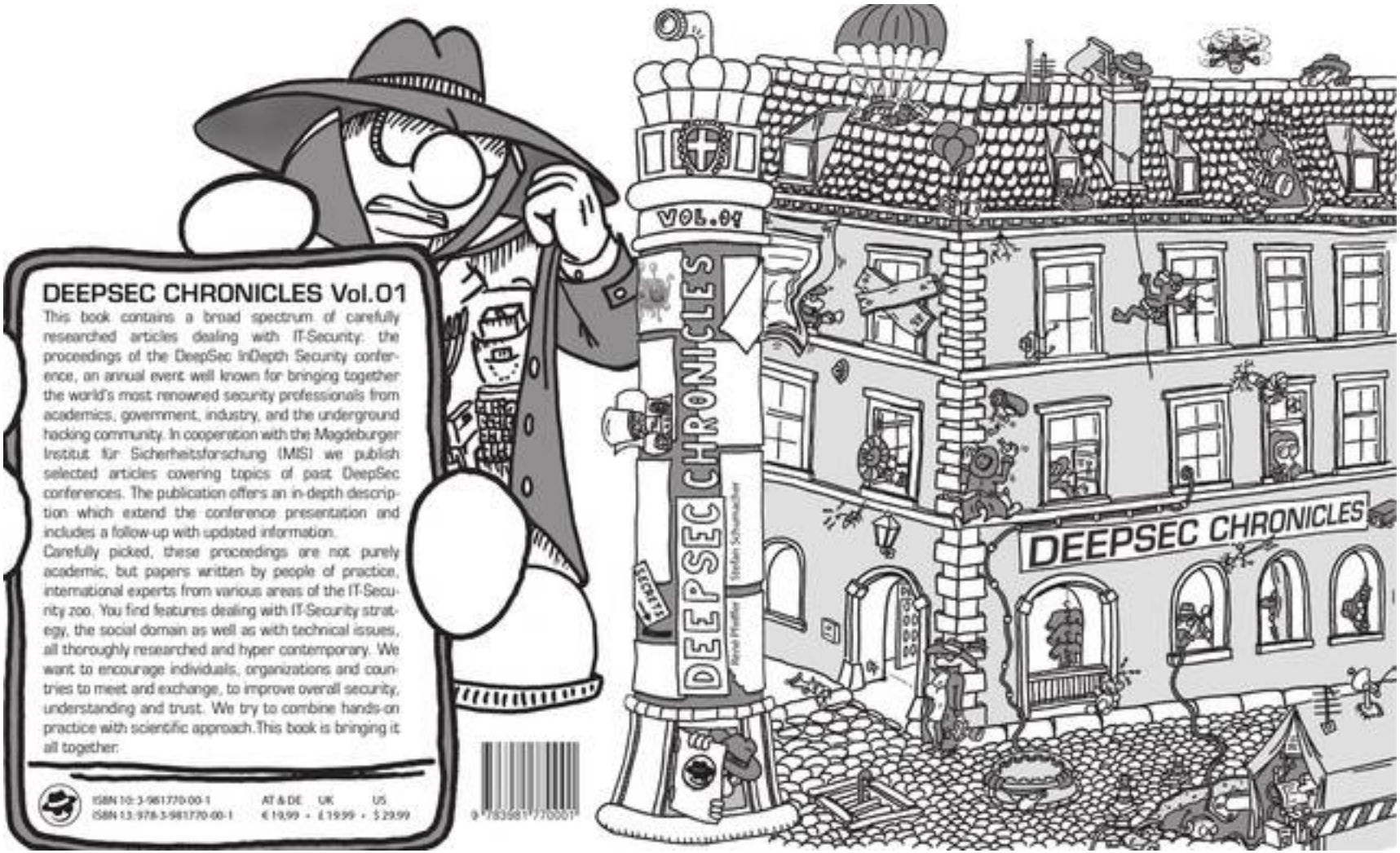
- Bildungswissenschaft/Psychologie
- 20+ Jahre Hacker, einige Jahre NetBSD-Entwickler
- Berater für Unternehmenssicherheit `www.Kaishakunin.com`
- Berater für Finanzinstitute, Regierungen, Sicherheitsbehörden
- Organisationssicherheit, Social Engineering, Security Awareness
- Direktor des Magdeburger Instituts für Sicherheitsforschung
- Herausgeber des Magdeburger Journals zur Sicherheitsforschung
- `www.Sicherheitsforschung-Magdeburg.de`
- Lehrbeauftragter

Forschungsprogramme des MIS

- Psychologie der Sicherheit
  - Social Engineering
  - Security Awareness, Sicherheit in Organisationen
  - Didaktik der Sicherheit
  - Didaktik der Kryptographie
- Lehrerfortbildung
  - Lernfelder: Fachinformatiker IT-Sicherheit
  - Lernfelder: IT-Sicherheit für Kaufleute
  - Lernfelder: IT-Sicherheit für Elektroberufe
- IT-Sicherheit in KMU
  - empirische Grundlagenforschung
  - didaktische Aufbereitung
  - Schulungen

Schulungs- und Beratungsangebote

- Sicher unterwegs in Internet
- Security Awareness Kampagnen konzipieren
- Die psychologischen Grundlagen des Social Engineerings
- Anonymität und Überwachung im Internet
- Der digitale Untergrund: zur aktuellen Bedrohungslage im Internet
- Kryptographie - Konzepte, Methoden und Anwendungen
- Strategien im Wirtschaftskrieg
- Selbstschutz in Krisengebieten
- Netzwerke absichern


DEEPSEC CHRONICLES Vol.01
This book contains a broad spectrum of carefully researched articles dealing with IT-Security: the proceedings of the DeepSec InDepth Security conference, an annual event well known for bringing together the world's most renowned security professionals from academics, government, industry, and the underground hacking community. In cooperation with the Magdeburger Institut für Sicherheitsforschung (MIS) we publish selected articles covering topics of past DeepSec conferences. The publication offers an in-depth description which extend the conference presentation and includes a follow-up with updated information.
Carefully picked, these proceedings are not purely academic, but papers written by people of practice, international experts from various areas of the IT-Security zoo. You find features dealing with IT-Security strategy, the social domain as well as with technical issues, all thoroughly researched and hyper contemporary. We want to encourage individuals, organizations and countries to meet and exchange, to improve overall security, understanding and trust. We try to combine hands-on practice with scientific approach.This book is bringing it all together.
ISBN 10: 3-981770-00-1
ISBN 13: 978-3-981770-00-1
AT & DE UK US
€ 19,99 £ 19,99 $ 29,99
Vol.01
DEEPSEC CHRONICLES
DEEPSEC CHRONICLES

- Stefan Schumacher and René Pfeiffer (editors)
- In Depth Security – Proceedings of the DeepSec Conference
- 360 Pages
- Magdeburger Institut für Sicherheitsforschung
- 978-3981770001
- `http://www.amazon.de/Depth-Security-Stefan-Schumacher/dp/3981770005/ref=sr_1_1?ie=UTF8&qid=1448888706`

- Schumacher, Stefan (2011)
  Die psychologischen Grundlagen des Social Engineerings
  in: *Magdeburger Journal zur Sicherheitsforschung*, 01/2011, S. 1-26
  `http://www.sicherheitsforschung-magdeburg.de/publikationen/journal.html#c291`
- Schumacher, Stefan (2012)
  Sicherheit messen. Eine Operationalisierung als latentes soziales Konstrukt. In: Die sicherheitspolitische Streitkultur in der Bundesrepublik Deutschland. Hrsg. von S. Adorf, J. Schaffeld und Dietmar Schössler. Magdeburg: Meine Verlag, S. 1–38.

Inhalt

- Die Psychologischen Grundlagen des Social Engineerings
- Security Awareness Kampagnen
- Beispiel: sichere Passwörter
- 2FA mit Yubikey

Teil I

Psychologischen Grundlagen des Social Engineering

Social Engineering

Jawoll, Herr Hauptmann ...

- Ausnutzen menschlicher Verhaltensweisen
- Warum sollte ich `/etc/master.passwd` cracken, wenn ich doch einen Benutzer dazu bringen kann, mir sein Passwort zu geben.
- »Hacking People«
- Ausnutzen psychologischer Verhaltensweisen

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

"Perhaps Monsieur would care for something more expensive?"

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

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

Reziprozität

Abwehr

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

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

Furby

How the Furby Flies

It seems that every holiday season, parents find at least one highly prized toy sold out after they have promised it to their children. If the parents can't secure a toy in time for the holidays, that promise spurs them to purchase one later.

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

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?

Commitment und Konsistenz

Zusammenfassung

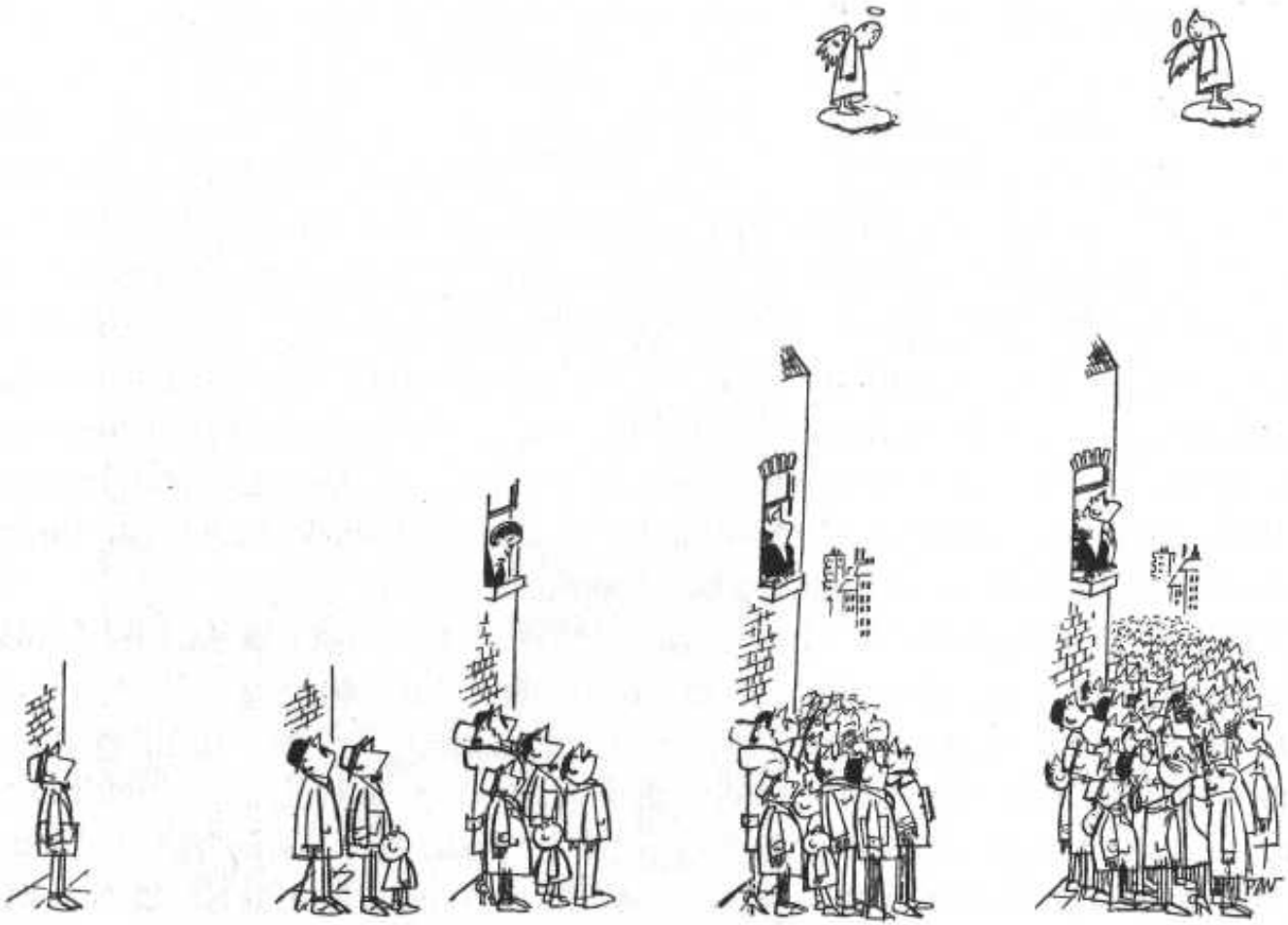
- persönliche Konsistenz wird von der Gesellschaft erwartet und wertgeschätzt
- Konsistenz vereinfacht das komplexe tägliche Leben
- Nach einem Commitment sind Menschen gewillter, Anfragen zu erfüllen, wenn diese in ihr Commitment passen
- sogar falsche Commitments können selbst-erfüllend werden

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)



Looking for Higher (and Higher) Meaning
The draw of the crowd is devilishly strong.
© Punch/Rothco

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

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

Soziale Bewährtheit

Countermeasures

- ignoring Soziale Bewährtheit is impossible
- check the data you are getting (the trigger feature)
- is really the majority doing X? (ads)
- train your workforce

Soziale Bewährtheit

Countermeasures

- ignoring Soziale Bewährtheit is impossible
- check the data you are getting (the trigger feature)
- is really the majority doing X? (ads)
- train your workforce

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 Autorität
  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

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

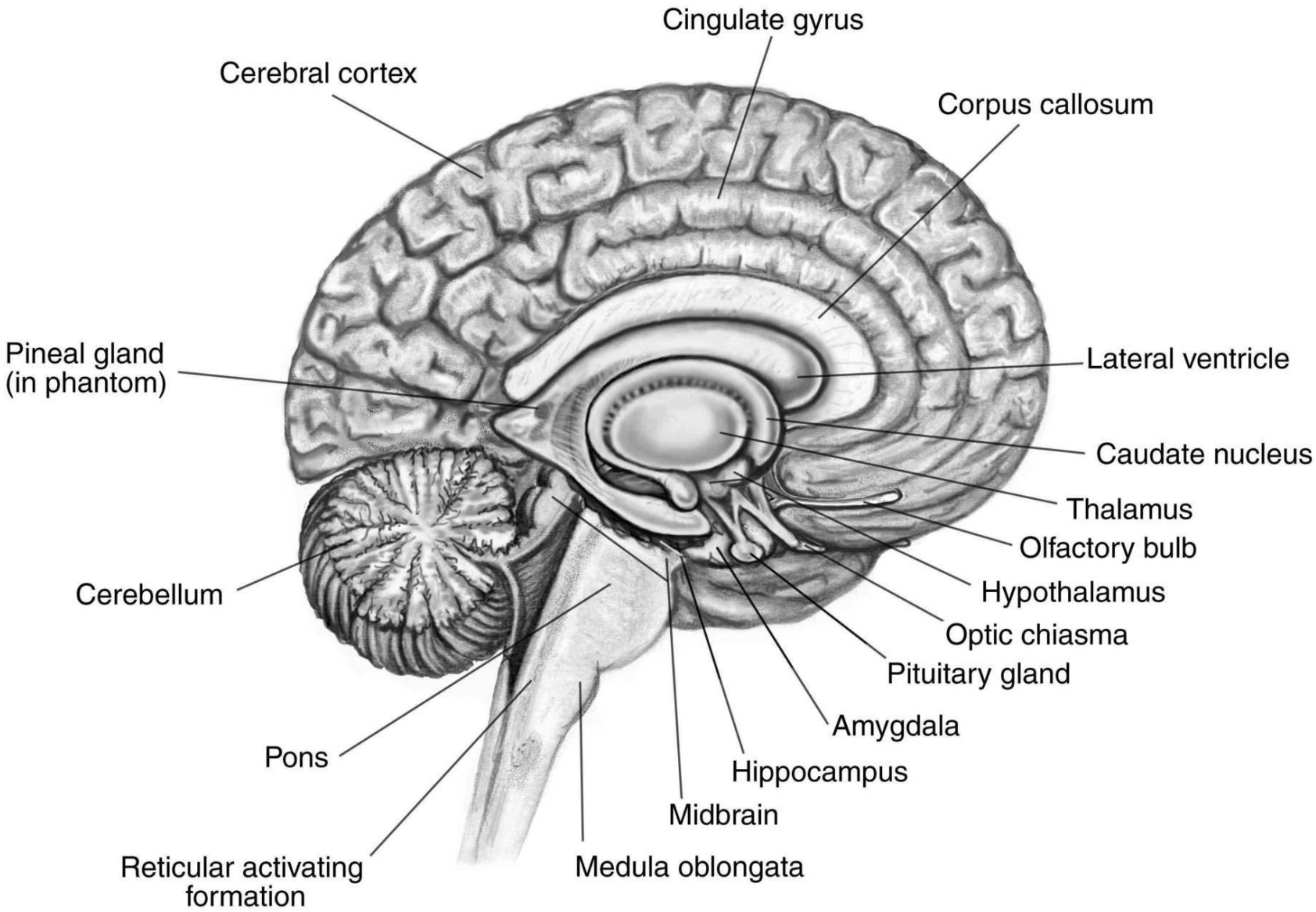
- limitierte Ausgabe (special limited edition)
- begrenzte Angebote (Time Life)
- Zensur
- Ebay/Auktionen

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

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
Hypothalamus
Optic chiasma
Pituitary gland
Cerebellum
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

Teil II

Security Awareness Kampagnen

Table of Contents

Was ist eine Security-Awareness-Kampagne?

- Gesamtheit aller Maßnahmen und notwendigen Ressourcen, um das Sicherheitsbewusstsein einer Organisation zu erhöhen.
- (technische) Sicherheitsmaßnahmen vermitteln
- Projektmanagement: Managementmethoden, Psychologie, Soziologie, Pädagogik
- Bewusstseinsveränderung: Psychologie, Bildungswissenschaft, Chemie ...
- Awareness; Training; Lernen

Organisation

- keine Einzelkämpfer-Lösung (Championmodell)
- Kooperation mit anderen Abteilungen
- Schulung muss auch bei Führungskräften ansetzen

Table of Contents

Wie wirklich ist die Wirklichkeit?

Paul Watzlawick

- Wirklichkeit wird im Subjekt konstruiert, ist damit abhängig von dessen Biografie (s. Radikaler Konstruktivismus)
- Watzlawick: Modell der zwei Wirklichkeiten
  - Wirklichkeit 1. Ordnung
    harte, also messbare, Realität (Temperatur, Alter, Gewicht)
  - Wirklichkeit 2. Ordnung
    gefühlte, konstruierte Realität (Ist es warm/kalt? Bin ich jung/alt, dünn/dick?)

Wie wirklich ist die Wirklichkeit?

Paul Watzlawick

- Wirklichkeit wird im Subjekt konstruiert, ist damit abhängig von dessen Biografie (s. Radikaler Konstruktivismus)
- Watzlawick: Modell der zwei Wirklichkeiten
  - Wirklichkeit 1. Ordnung
    harte, also messbare, Realität (Temperatur, Alter, Gewicht)
  - Wirklichkeit 2. Ordnung
    gefühlte, konstruierte Realität (Ist es warm/kalt? Bin ich jung/alt, dünn/dick?)
- Jedes Subjekt konstruiert seine eigene, immanente Realität
- *Die* Wirklichkeit gibt es nicht!

Wie wirklich ist die Wirklichkeit?

Paul Watzlawick

- Wirklichkeit wird im Subjekt konstruiert, ist damit abhängig von dessen Biografie (s. Radikaler Konstruktivismus)
- Watzlawick: Modell der zwei Wirklichkeiten
  - Wirklichkeit 1. Ordnung
    harte, also messbare, Realität (Temperatur, Alter, Gewicht)
  - Wirklichkeit 2. Ordnung
    gefühlte, konstruierte Realität (Ist es warm/kalt? Bin ich jung/alt, dünn/dick?)
- Jedes Subjekt konstruiert seine eigene, immanente Realität
- *Die* Wirklichkeit gibt es nicht!
- s. a.: Jean Piaget, von Foerster, von Bertalanffy (Kybernetik 2. Ordnung)

Wie wirklich ist die Wirklichkeit?

Paul Watzlawick

- Wirklichkeit wird im Subjekt konstruiert, ist damit abhängig von dessen Biografie (s. Radikaler Konstruktivismus)
- Watzlawick: Modell der zwei Wirklichkeiten
  - Wirklichkeit 1. Ordnung
    harte, also messbare, Realität (Temperatur, Alter, Gewicht)
  - Wirklichkeit 2. Ordnung
    gefühlte, konstruierte Realität (Ist es warm/kalt? Bin ich jung/alt, dünn/dick?)
- Jedes Subjekt konstruiert seine eigene, immanente Realität
- *Die* Wirklichkeit gibt es nicht!
- s. a.: Jean Piaget, von Foerster, von Bertalanffy (Kybernetik 2. Ordnung)

Perspektivenübernahme

- Admin lebt in seiner Realität ./. User lebt in seiner Realität
- Admin will Systeme am laufen halten, dazu gehört auch Sicherheit, Benutzer umgehen Sicherheitsmaßnahmen
- User will seine Aufgaben erledigen, und dazu möglichst einfach die Systeme nutzen, Sicherheit als Barriere wahrgenommen

Perspektivenübernahme

- Admin lebt in seiner Realität ./. User lebt in seiner Realität
- Admin will Systeme am laufen halten, dazu gehört auch Sicherheit, Benutzer umgehen Sicherheitsmaßnahmen
- User will seine Aufgaben erledigen, und dazu möglichst einfach die Systeme nutzen, Sicherheit als Barriere wahrgenommen
- Führt zu Interessenkonflikt!?

Perspektivenübernahme

- Admin lebt in seiner Realität ./. User lebt in seiner Realität
- Admin will Systeme am laufen halten, dazu gehört auch Sicherheit, Benutzer umgehen Sicherheitsmaßnahmen
- User will seine Aufgaben erledigen, und dazu möglichst einfach die Systeme nutzen, Sicherheit als Barriere wahrgenommen
- Führt zu Interessenkonflikt!?
- nicht zwangsläufig, wenn die Realitäten berücksichtigt werden
- Perspektivenübernahme, Empathie
- Perspektivziel Admin *und* User: eigene Aufgaben erledigen, Unternehmen am laufen halten, angenehmen Arbeitsplatz behalten

Perspektivenübernahme

- Admin lebt in seiner Realität ./. User lebt in seiner Realität
- Admin will Systeme am laufen halten, dazu gehört auch Sicherheit, Benutzer umgehen Sicherheitsmaßnahmen
- User will seine Aufgaben erledigen, und dazu möglichst einfach die Systeme nutzen, Sicherheit als Barriere wahrgenommen
- Führt zu Interessenkonflikt!?
- nicht zwangsläufig, wenn die Realitäten berücksichtigt werden
- Perspektivenübernahme, Empathie
- Perspektivziel Admin *und* User: eigene Aufgaben erledigen, Unternehmen am laufen halten, angenehmen Arbeitsplatz behalten

Was heißt das?

- Niemand tut etwas gegen den eigenen Willen!
- Allerdings ist der »eigene Wille« adjustierbar
- Ziel der SAK: Einstellungsänderung
- Verhalten: extrinsisch (Anschnallen, sonst Strafe)
- Einstellung: intrinsisch (Anschnallen, weil sicherer)
- User soll sich als sicherheitsbewusst wahrnehmen und auch so handeln
- Kompetenzentwicklung

Was heißt das?

- Niemand tut etwas gegen den eigenen Willen!
- Allerdings ist der »eigene Wille« adjustierbar
- Ziel der SAK: Einstellungsänderung
- Verhalten: extrinsisch (Anschnallen, sonst Strafe)
- Einstellung: intrinsisch (Anschnallen, weil sicherer)
- User soll sich als sicherheitsbewusst wahrnehmen und auch so handeln
- Kompetenzentwicklung

Motivationspsychologie

Entwicklung als probabilistische Epigenese

Definition

Der Einfluss, den ein Kontext auf eine Person ausübt, wird durch die Bedeutung bestimmt, die sie ihm beimisst.

PETERMANN, F. (Hrsg.):
Lehrbuch der klinischen Kinderpsychologie und -psychotherapie.
Göttingen : Hogrefe, 2002

Was heißt das?

- Motivation zwingend erforderlich
- Begründung *warum* Sicherheitsmaßnahmen erforderlich
- Sich der Lebenswelt des Users nähern (Internetbanking, Zwei Schlüssel für Banktresore)
- Dem User seine Wichtigkeit zeigen (dein schlechtes Passwort kann das ganze Netzwerk gefährden)
- Verunsicherung ist MEGA-BÖSE, erleichtert Manipulation
- Auf neue User aufpassen: erst einweisen, dann ans Gerät lassen

Table of Contents

Sozialpsychologie

- SAK muss von *allen* getragen werden
- von oben nach unten
- Einstellungsänderungen bei *allen*, auch den Chefs und Schlipsen und den Nicht-Usern
- Führen durch Vorbild
- Prinzip der sozialen Bewährtheit

Table of Contents

Motivation

Motive

- treibt einen Organismus an, einem Ziel näher zu kommen
- bewusst oder unbewusst
- entspringt einem Bedürfnis, jedes Bedürfnis hat die Bedürfnis-Befriedigung zum Ziel
- ohne Motiv kein Verhalten
- ohne unbefriedigte Bedürfnisse kein Motiv
- Motive sind stabil, Motivation nicht

Motivation

Bedürfnishierarchie nach Maslow (2002)

Begründer der Humanistischen Psychologie (mit Rogers/Fromm)

Stufe	Bedürfnis
	Körperliche Bedürfnisse

Motivation

Bedürfnishierarchie nach Maslow (2002)

Begründer der Humanistischen Psychologie (mit Rogers/Fromm)

Stufe	Bedürfnis
II	Sicherheit
I	Körperliche Bedürfnisse

Motivation

Bedürfnishierarchie nach Maslow (2002)

Begründer der Humanistischen Psychologie (mit Rogers/Fromm)

Stufe	Bedürfnis
III	Soziale Beziehungen
II	Sicherheit
I	Körperliche Bedürfnisse

Motivation

Bedürfnishierarchie nach Maslow (2002)

Begründer der Humanistischen Psychologie (mit Rogers/Fromm)

Stufe	Bedürfnis
IV	Soziale Anerkennung
III	Soziale Beziehungen
II	Sicherheit
I	Körperliche Bedürfnisse

Motivation

Bedürfnishierarchie nach Maslow (2002)

Begründer der Humanistischen Psychologie (mit Rogers/Fromm)

Stufe	Bedürfnis
V	Selbstverwirklichung
IV	Soziale Anerkennung
III	Soziale Beziehungen
II	Sicherheit
I	Körperliche Bedürfnisse

Motivation

Bedürfnishierarchie nach Maslow (2002)

Begründer der Humanistischen Psychologie (mit Rogers/Fromm)

Stufe	Bedürfnis
V	Selbstverwirklichung
IV	Soziale Anerkennung
III	Soziale Beziehungen
II	Sicherheit
I	Körperliche Bedürfnisse

Motivation

Zwei-Faktoren-Theorie nach Herzberg

- Zufriedenheit und Unzufriedenheit als unabhängige Dimensionen
- Unzufriedenheit wird durch extrinsische Faktoren begünstigt
  Status, Entlassungsdruck, Beziehung zu Vorgesetzten und Kollegen
- Zufriedenheit nur durch intrinsische Faktoren begünstigt
  Erfolgserlebnisse, Anerkennung, Verantwortung

Motivation

Motivation vs. Manipulation

- Bei Manipulationen werden nur die Bedürfnisse des Manipulierenden befriedigt, während die Bedürfnisse des Manipulierten außer acht gelassen werden. Am Ende ist nur der Manipulierende zufrieden.
- Das Kriterium optimaler Motivation ist, daß beide Parteien hinterher zufrieden sind (da die Bedürfnisse beider befriedigt wurden).

Motivation

intrinsisch/extrinsisch

intrinsische Motivation aus der Tätigkeit selbst

extrinsische Motivation von außen (Belohnung/Bestrafung)

Überrechtfertigungseffekt externe Motivation untergräbt vorhandene intrinsische Motivation

Motivation

intrinsisch/extrinsisch

intrinsische Motivation aus der Tätigkeit selbst

extrinsische Motivation von außen (Belohnung/Bestrafung)

Überrechtfertigungseffekt externe Motivation untergräbt vorhandene intrinsische Motivation

Motivation

Grundlagen

- Optimal kommunizieren heißt: den anderen richtig motivieren
- Jemanden motivieren heißt, jemanden dazu zu bewegen, ein von mir gewünschtes Verhalten an den Tag zu legen.
- Jemanden motivieren heißt: jemanden veranlassen, ein altes Verhaltensmuster zugunsten eines neuen aufzugeben.
- Ich motiviere jemanden, indem ich eines seiner unbefriedigten Bedürfnisse anspreche und ihm zeige, durch welches Verhalten er dieses befriedigen kann.
- Je besser der andere sich die Zielsituation vorstellen kann, desto motivierter wird er.

Motivation

Grundlagen

Don’t sell the steak – sell the sizzle

Motivation

Vorgehensweise

- Nur momentanes Verhalten kann sofort beeinflußt werden.
- Jedes regelmäßige Verhalten ist durch Lernprozesse entstanden.
- Jede Änderung von regelmäßigem Verhalten bedarf eines neuen Lernprozesses.
- Jeder Lernprozess braucht Zeit.

Veränderungen in Organisationen durchsetzen

Promotoren-Modell

Definition

Promotoren ergreifen die Initiative und fördern Innovationen aktiv und intensiv. Die Aktivitäten von Promotoren sind von ihrer Persönlichkeit, vom Motivationspotenzial der Innovation und der Promotorenrolle vorbestimmt.

WITTE, Eberhard:
Organisation für Innovationsentscheidungen - Das Promotoren-Modell.
Göttingen : Schwartz, 1973.

Veränderungen in Organisationen durchsetzen

Promotoren-Modell

Fachpromotor überwindet Fähigkeitsbarrieren (Nicht-Wissen) durch objektspezifisches Fachwissen

- Ideengenerierung
- Alternativentwicklung
- Konzeptevaluierung
- Informationsbereitstellung

Machtpromotor überwindet Willens- und Hierarchiebarrieren (Nicht-Wollen) durch hierarchisches Potenzial

- Zieldefinition
- Ressourcenbereitstellung
- Schutz vor Opponenten
- Prozesssteuerung

Veränderungen in Organisationen durchsetzen

Promotoren-Modell

Fachpromotor überwindet Fähigkeitsbarrieren (Nicht-Wissen) durch objektspezifisches Fachwissen

- Ideengenerierung
- Alternativentwicklung
- Konzeptevaluierung
- Informationsbereitstellung

Machtpromotor überwindet Willens- und Hierarchiebarrieren (Nicht-Wollen) durch hierarchisches Potenzial

- Zieldefinition
- Ressourcenbereitstellung
- Schutz vor Opponenten
- Prozesssteuerung

Veränderungen in Organisationen durchsetzen

Promotoren-Modell

Prozesspromotor überwindet Fähigkeits- und Abhängigkeitsbarrieren (Nicht-Dürfen) durch Organisationskenntnis und Kommunikationsfähigkeit

- Zusammenführung
- Vermittlung/Konfliktmanagement
- Prozesssteuerung/-koordination

Beziehungspromotor überwindet fachübergreifende Fähigkeits- und Abhängigkeitsbarrieren (Nicht-Miteinander-Wollen/-Können/-Dürfen) durch soziale Kompetenzen, Netzwerkwissen und Beziehungen (*Vitamin B*)

- Informationsaustausch
- Konfliktmanagement
- Steuerung von Austauschprozessen
- Interaktionspartner zusammenbringen

Veränderungen in Organisationen durchsetzen

Promotoren-Modell

Prozesspromotor überwindet Fähigkeits- und Abhängigkeitsbarrieren (Nicht-Dürfen) durch Organisationskenntnis und Kommunikationsfähigkeit

- Zusammenführung
- Vermittlung/Konfliktmanagement
- Prozesssteuerung/-koordination

Beziehungspromotor überwindet fachübergreifende Fähigkeits- und Abhängigkeitsbarrieren (Nicht-Miteinander-Wollen/-Können/-Dürfen) durch soziale Kompetenzen, Netzwerkwissen und Beziehungen (*Vitamin B*)

- Informationsaustausch
- Konfliktmanagement
- Steuerung von Austauschprozessen
- Interaktionspartner zusammenbringen

Veränderungen in Organisationen durchsetzen

Promotoren-Modell

Technologischer Gatekeeper überwindet Wissensbarrieren durch Zugang zu fachspezifischen Informationen und die Kontrolle der Informationsflüsse

- Expertenwissen
- Meinungsführerschaft
- Kontaktvermittlung
- interpretiert fachspezifische Informationen

Table of Contents

Sicherheitsrichtlinie

Wozu?

- Organisatorische Richtschnur (Zielvorgaben)
- soll kopfloses Vorgehen verhindern
- Ziele festlegen und klar kommunizieren
- Verantwortliche festlegen
- Ansprechpartner und Meldewege festlegen
- Benutzer müssen sicherheitskonformes Vorgehen erlernen
- Sie wissen nicht was ein sicherers Passwort ist und es interessiert sie auch nicht so ohne weiteres!

Teil III

Beispiel: Sichere Passwörter

Table of Contents

Live-Hacking

- Wie lange brauche ich um einen Rechner zu hacken?
- Was muss ich dazu wissen und können?
- Welche Software benötige ich?

Metasploit-Demo
Ich stehle die Passwort-Datei ...

Table of Contents

Passwörter

- werden gehasht gespeichert
- Hash := mathematische Einwegfunktion
- Passwort $\rightsquigarrow$ Hash: einfach
- Hash $\rightsquigarrow$ Passwort: schwer

Magdeburg	`59aceadf846f772736c4b40eee7b155d`
magdeburg	`7712722364ae231b5f777bac5dd2eb80`
MagdeBurg	`eadfc761160224295a58847eee4cbdfc`
Magdeburger	`0c52463fc68f157a5756cdde4adf762d`
Magdeburgerin	`68a783bebaf27a448481d5341b77b4f9`

Wörterbuchangriffe

fröhliches Passwortraten: alle Kombinationen probieren

Kombinationen = Alphabet ^ Länge

26 Buchstaben (a-z), 5 Stellen: $26^5 = 11.881.376$

aaaaa	aaaba	aaaca	...	zzzya	zzzza
aaaab	aaabb	aaacb	...	zzzyb	zzzzb
aaaac	aaabc	aaacc	...	zzzyc	zzzzc
aaaad	aaabd	aaacd	...	zzzyd	zzzzd
aaaae	aaabe	aaace	...	zzzye	zzzze
			...		
aaaav	aaabv	aaacv	...	zzzyv	zzzzv
aaaaw	aaabw	aaacw	...	zzzyw	zzzzw
aaaax	aaabx	aaacx	...	zzzyx	zzzzx
aaaay	aaaby	aaacy	...	zzzyy	zzzzy
aaaaz	aaabz	aaacz	...	zzzyz	zzzzz

Wörterbuchangriffe

Kombinatorik

- $99^{10} = 90.438.207.500.880.449.001$
- $99^{15} = 860.058.354.641.288.524.893.953.951.499$
- $99^{20} = 8.179.069.375.972.308.708.891.986.605.443.361.898.001$
- Annahme: 5 Passwörter pro Sekunde $\rightsquigarrow$ 432000 pro Tag
- $\frac{26^5}{432.000} = 27,5$ Tage
- $(99^{10}/432.000)/365000 \approx 570$ Millionen Jahrtausende

Wörterbuchangriffe

Kombinatorik

- $99^{10} = 90.438.207.500.880.449.001$
- $99^{15} = 860.058.354.641.288.524.893.953.951.499$
- $99^{20} = 8.179.069.375.972.308.708.891.986.605.443.361.898.001$
- Annahme: 5 Passwörter pro Sekunde $\rightsquigarrow$ 432000 pro Tag
- $\frac{26^5}{432.000} = 27,5$ Tage
- $(99^{10}/432.000)/365000 \approx 570$ Millionen Jahrtausende
- Annahme: 5.000 Passwörter pro Sekunde $\rightsquigarrow$ 432.000.000 pro Tag
- $\frac{26^5}{432.000.000} \approx 40$ *Minuten*
- $(99^{10}/432.000.55)/365000 \approx 570$ Tausend Jahrtausende

Wörterbuchangriffe

Kombinatorik

- $99^{10} = 90.438.207.500.880.449.001$
- $99^{15} = 860.058.354.641.288.524.893.953.951.499$
- $99^{20} = 8.179.069.375.972.308.708.891.986.605.443.361.898.001$
- Annahme: 5 Passwörter pro Sekunde $\rightsquigarrow$ 432000 pro Tag
- $\frac{26^5}{432.000} = 27,5$ Tage
- $(99^{10}/432.000)/365000 \approx 570$ Millionen Jahrtausende
- Annahme: 5.000 Passwörter pro Sekunde $\rightsquigarrow$ 432.000.000 pro Tag
- $\frac{26^5}{432.000.000} \approx 40$ *Minuten*
- $(99^{10}/432.000.55)/365000 \approx 570$ Tausend Jahrtausende

Stratfor-Demo

- Stratfor-Demo

Wörterbuchangriffe

- Thomas Roth, 2010
- lässte alle 1-6 stelligen Passwörter generieren
- SHA-1 Hashes berechnen
- nutzt Amazon Cloud GPU Programm
- Dauer: 49 Minuten, Kosten 2,1$/h

Passwörter raten

- beliebte Social-Engineering-Methode
- Passwortwahl sagt einiges über den Benutzer aus
- muss einfach merkbar sein $\rightsquigarrow$ naheliegendes Datum
- Name des Sohnes/Tochter/Ehemann/Hund/Katze/Maus ...
- Postleitzahl, KFZ-Kennzeichen, Hochzeitstag, Geburtstag
- leicht herausfindbar (Pers-Akte, Lohnsteuerkarte, Blog, Homepage)
- Daher absolut verboten!

Passwörter raten

- beliebte Social-Engineering-Methode
- Passwortwahl sagt einiges über den Benutzer aus
- muss einfach merkbar sein $\rightsquigarrow$ naheliegendes Datum
- Name des Sohnes/Tochter/Ehemann/Hund/Katze/Maus ...
- Postleitzahl, KFZ-Kennzeichen, Hochzeitstag, Geburtstag
- leicht herausfindbar (Pers-Akte, Lohnsteuerkarte, Blog, Homepage)
- Daher absolut verboten!

Passwörter recyclen?

- mehrere Passwörter nötig $\rightsquigarrow$ Recycling
- Webforen etc. werden oft angegriffen
- Ist das Webforum vertrauenswürdig?
- Technisch einwandfrei? Oder gar Honeypot?

Auf keinen Fall überall das selbe Passwort verwenden!

Passwörter recyclen?

- mehrere Passwörter nötig $\rightsquigarrow$ Recycling
- Webforen etc. werden oft angegriffen
- Ist das Webforum vertrauenswürdig?
- Technisch einwandfrei? Oder gar Honeypot?

Auf keinen Fall überall das selbe Passwort verwenden!

Passwortregeln

- Verwenden Sie kein Passwort das erraten werden kann!
- Verwenden Sie kein Passwort das in einem Wörterbuch steht!
- Verwenden Sie ein langes Passwort mit Groß- und Kleinschreibung, Zahlen und Sonderzeichen!
- Das Passwort muss geheim bleiben!
- Verwenden Sie nicht überall das selbe Passwort!
- Wechseln Sie Ihre Passwörter!

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen ,
  Eines Freundes Freund zu sein.
  - Friedrich Schiller, 1805

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen ,
  Eines Freundes Freund zu sein.
  - Friedrich Schiller, 1805
- $\rightsquigarrow$ WdgWg,EFFzs.-FS,1805

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen ,
  Eines Freundes Freund zu sein.
  - Friedrich Schiller, 1805
- $\rightsquigarrow$ W d g W g , E F F z s . - F S , 1 8 0 5

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen ,
  Eines Freundes Freund zu sein.
  - Friedrich Schiller, 1805
- $\rightsquigarrow$ W d g W g , E F F z s . - F S , 1 8 0 5
- Leetspeak: `D03s Any1 in |-|3r3 5pE4|< 31337?`

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen ,
  Eines Freundes Freund zu sein.
  - Friedrich Schiller, 1805
- $\rightsquigarrow$ W d g W g , E F F z s . - F S , 1 8 0 5
- Leetspeak: `D03s Any1 in |-|3r3 5pE4|< 31337?`
- Dialekte: Vocheljesank in Machteburch; Motschekiebschen

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen ,
  Eines Freundes Freund zu sein.
  - Friedrich Schiller, 1805
- $\rightsquigarrow$ W d g W g , E F F z s . - F S , 1 8 0 5
- Leetspeak: `D03s Any1 in |-|3r3 5pE4|< 31337?`
- Dialekte: Vocheljesank in Machteburch;
  Motschekiebschen

Teil IV

2FA mit Yubikey

Authentifizierung

- Authentifizierung: Nachweis einer bestimmten Eigenschaft
- Bsp: Benutzername/Passwort; Anruf/Parole; Person/Personalausweis;
- Problem: Jeder der Benutzername und Passwort kennt, kann sich als der Benutzer ausgeben
- schwache Passwörter, schlechte Passwortsicherheit
- Stratfor-Hack: Kundendatenbank gestohlen, Passwörter als MD5 gehasht
- Thomas Roth: 1-6 stellige SHA1-Hashes in 50 Minuten/2$ auf Amazon EC2

Zwei-Faktor-Authentifizierung

- Zwei-Faktor-Authentifizierung: Einführung eines 2. Faktors zur Authentifizierung
- Einbrechern kann Passwort kennen, benötigt aber 2. Faktor (Token)
- Schutz vor Shouldersurfing, schwachen Passwörtern, schlechten Datenbanken
- Schutz vor Man-in-the-Middle möglich

- Wissen: Passwort, Pin, TAN
- Besitz: Schlüssel, EC-Karte, Token, Datei
- Sein: Fingerabdruck, Iris, Stimme, Gesicht
- Kombinationen: Benutzername+Passwort+Token; Benutzername+TAN+Token; Smartcard+Token
- Nachteile: Token muss mitgeführt werden und kostet Geld

- Wissen: Passwort, Pin, TAN
- Besitz: Schlüssel, EC-Karte, Token, Datei
- Sein: Fingerabdruck, Iris, Stimme, Gesicht
- Kombinationen: Benutzername+Passwort+Token; Benutzername+TAN+Token; Smartcard+Token
- Nachteile: Token muss mitgeführt werden und kostet Geld

Table of Contents

OATH

- Initiative for Open Authentication (OATH)
- Industriezusammenschluss
- Mitgliedschaft kostet Geld
- HOTP: RFC4226
- TOTP: RFC6238

FIDO

- Industrie-Konsortium mit 200 Mitgliedern, u.a. Google, Paypal, Lenovo, Alibaba, NTT DoCoMo, Samsung, Visa, RSA, Intel, ING, Yubico
- Spezifikationsrahmen u.a. für Biometrie, Trusted Platform Modules, Smart Cards, NFC
- Authentifikation mittels asymmetrischer Kryptographie
- U2F: Universal 2nd Factor, *offener* Standard für 2FA via USB oder NFC
- Integriert in Chrome seit 38, Firefox, Windows 10 und Edge folgen

Table of Contents


yubico
yubico
fido

Yubikey Token

- Yubikey Neo: 55€, USB+NFC, OTP, PIV, OpenPGP (2048bit), U2F
- Yubikey 4: 48€, USB, OTP, PIV, OpenPGP (4096bit), U2F, PKCS#11
- Yubikey 4 Nano: 60€
- FIDO U2F Security Key: 17€, nur U2F
- Plug-up U2F: 5€
- Yubikey Neo/4: 2 Slots, müssen programmiert werden

Fähigkeiten

- Public-Key-basiertes Challenge-Response Protokoll
- Phishing und MitM-Schutz
- applikationsspezifische Schlüssel,
- Erkennung geklonter Token
- Beglaubigung von Token

One Time Passwort (OTP)

- Passwort, welches nur einmal gültig ist
- verfällt nach (missglücktem) Login-Vorgang
- passives Mithören, Replay-Attacken nicht möglich
- MitMA können funktionieren
- Alice und Bob müssen das gültige OTP kennen
- Kennwortliste oder Kennwortgenerator

One Time Passwort (OTP)

Kennwortgeneratoren

- übertragen das *Ergebnis* eines Algorithmus
- Zeitgesteuerte Generatoren
  wohldefiniertes Zeitintervall, Uhren müssen synchron sein
- Ereignisgesteuerte Generatoren
  Ereignis löst Kennwortgenerator aus, keine Uhr/Strom nötig, OTP kann theoretisch ∞ gültig bleiben
- Challenge-Response-gesteuerte Generatoren
  Client berechnet OTP basierend auf Challenge, Challenge sollte Zufallsgeneriert sein
- HOTP: HMAC-SHA1 via Zähler und Seed, SHA1 + Key + Message +XOR (definierte Werte)

U2F Login

- Login auf Google.com
- Benutzername und Passwort eingeben
- wenn Passwort korrekt, Token einstecken (oder SMS)
- Kontaktschalter drücken
- Token authentifiziert sich via U2F Server
- Google akzeptiert Login wenn der Token eingetragen ist
- Browser kann per Cookie aktiviert bleiben

U2F Schema

- Token hat k_{priv} und sendet k_{pub} an Relying Party (RP)
- Schlüsselpaar wird im Token generiert, kann nicht manipuliert werden
- Browser kompiliert Informationen (URI, TLS Channel ID) über HTTP-Verbindung
- Token signiert diese Informationen und schickt sie an RP

U2F Schema

- Token generiert neues Schlüsselpaar mit App ID und Key Handle für jede Registrierung $\rightsquigarrow$ RP weiß nicht, dass Alice und Bob das selbe Token nutzen
- Authentifikationszähler inkrementiert bei jeder Authentifizierung, RP vergleicht Zähler mit gespeichertem Stand $Z_T > Z_R P$
- Beglaubigungs-Zertifikat kann vom Hersteller ausgefüllt und auf Token gespeichert werden $\rightsquigarrow$ RP kann nur bestimmte Token zulassen (z.B. Yubikey ja, RSA nein, oder spezielle Yubikeys)

U2F Unterstützung

- Google, Dropbox, Github, PAM,
- Wordpress, Django, Ruby on Rails
- OpenSSH, Login, OpenVPN, FreeRADIUS via PAM
- LastPass, Dashlane, Password Safe, Passpack, Password Tote, pwSafe, KeePass

U2F Unterstützung

- Google, Dropbox, Github, PAM,
- Wordpress, Django, Ruby on Rails
- OpenSSH, Login, OpenVPN, FreeRADIUS via PAM
- LastPass, Dashlane, Password Safe, Passpack, Password Tote, pwSafe, KeePass

Google einrichten

1. Mein Konto,
2. Anmeldung und Sicherheit
3. Bestätigung in zwei Schritten
4. Sicherheitsschlüssel
5. Unter Bestätigungscodes: Handy registrieren und SMS einrichten oder Google Authenticator App einrichten
6. Zusätzlich: Ersatzcodes einrichten (TAN-Liste), ausdrucken und wegschließen

Web.de unterstützt U2F nicht

- OATH-HOTP im Yubikey Personalization Tool einrichten, Secret Key generieren
- KeePass installieren und einrichten, Plugin OtpKeyProv installieren, Secret Key hinterlegen
- sicheres Passwort für Keepass vergeben
- Zufallspasswort (256HEX Bit) generieren und bei Web.de eintragen

  `09137f0ac6627f9e94e2af2342d2610bf20ff0ee929114d27b3629e3823e11ea`
- KeePass mit dem Webbrowser via Plugin verbinden
- KeePass-Datenbank mit Passwort und Token entschlüsseln, Browser holt User/Passwort für Web.de via Plugin aus DB.

Yubico für eigene Dienste

- Plugins existieren u.a. für Wordpress, Django etc.
- PAM-Modul (`yubico-pam` kann eingebunden werden
- Yubikey-Server existiert als Paket, YubiHSM als Hardwareerweiterung
- Online-Validierung via YubiCloud oder eigenem Validierungsserver
- seit 2.6 Offline-Validierung dank HMAC-SHA1 Challenge-Response
- PAM-Modul installieren und konfigurieren, Conf-Datei landet in $HOME, Obacht bei ECryptFS
- SSH (Passwort + Token) per PAM
- OpenVPN und Radius via PAM

yubikey-luks

- System verschlüsselt installieren, mit sehr langem Zufallspasswort
- Das Zufallspasswort bleibt immer aktiviert, LUKS kann auch ohne Yubikey eingebunden werden
- `cryptsetup luksDump /dev/sda2` Keyslots anzeigen lassen
- standardmäßig gibt es 7 Keyslots $\rightsquigarrow$ 7 Passwörter für ein LUKS
- `ppa:yubico/stable` und `ppa:privacyidea/privacyidea-dev` installieren
  `ykpersonalize -2 -ochal-resp -ochal-hmac -ohmac-lt64 -oserial-api-visible`
- Challenge-Response Authentifikation mit HMAC-SHA1 aktivieren
- `cryptsetup luksAddKey -key-slot 7 /dev/sda2`
- `yubikey-luks-enroll -d /dev/sda5 -s 7 -c` - neues Passwort für LUKS + Yubikey vergeben

- sicherheitsforschung-magdeburg.de
- stefan.schumacher@sicherheitsforschung-magdeburg.de
  9475 1687 4218 026F 6ACF 89EE 8B63 6058 D015 B8EF
- sicherheitsforschung-magdeburg.de/publikationen/journal.html

- youtube.de/Sicherheitsforschung
- Twitter: 0xKaishakunin
- Xing: Stefan Schumacher
- ZRTP: 0xKaishakunin@ostel.co