Security Awareness für Systemadministratoren

Stefan Schumacher

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

Berlin
Secure Linux Administration Conference 2017



Über Mich



Über Mich

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



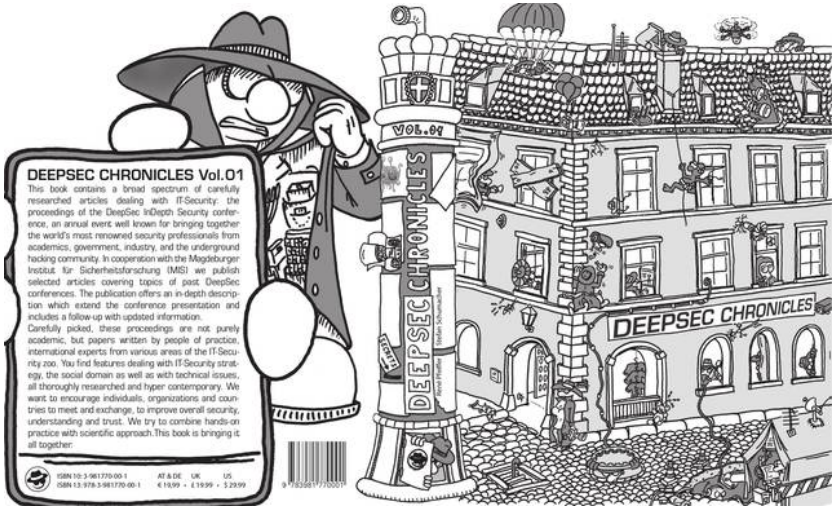
Forschungsprogramme des MIS

- 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 € 19.99
UK £ 19.99
US $ 29.99
Vol.01
DEEPSEC CHRONICLES
Stefan Schumacher
Bernd Stiefel
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

- Security Awareness Kampagnen
- Beispiel: sichere Passwörter



Social Engineering

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



Social Engineering

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 I

Security Awareness Kampagnen



Table of Contents

1. Einführung/Motivation
2. Psychologie
3. Veränderungen in Organisationen
4. Motivation
5. Sicherheitsrichtlinie



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

1 Einführung/Motivation

2 Psychologie

3 Veränderungen in Organisationen

4 Motivation

5 Sicherheitsrichtlinie



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

1 Einführung/Motivation

2 Psychologie

3 Veränderungen in Organisationen

4 Motivation

5 Sicherheitsrichtlinie



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

1 Einführung/Motivation

2 Psychologie

3 Veränderungen in Organisationen

4 Motivation

5 Sicherheitsrichtlinie



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
I	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

1 Einführung/Motivation

2 Psychologie

3 Veränderungen in Organisationen

4 Motivation

5 Sicherheitsrichtlinie



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 II

Beispiel: Sichere Passwörter



Table of Contents

6 Live-Hacking

7 Passwörter



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

6 Live-Hacking

7 Passwörter



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
- ⇝ 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
- ⇝ 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
- ⇝ 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
- Wörter: LilaDederonKittelschürzeSchattenmorellenZuckerkuchen



Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen ,
  Eines Freundes Freund zu sein.
  - Friedrich Schiller, 1805
- ⇝ 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
- Wörter: LilaDederonKittelschürzeSchattenmorellenZuckerkuchen
- 1920Mainz1923Quedlinburg1931Stralsund1935Rostock

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen ,
  Eines Freundes Freund zu sein.
  - Friedrich Schiller, 1805
- ⇝ 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
- Wörter: LilaDederonKittelschürzeSchattenmorellenZuckerkuchen
- 1920Mainz1923Quedlinburg1931Stralsund1935Rostock

Passwortflyer

http://www.sicherheitsforschung-magdeburg.de/uploads/material/Passwoerter-Regeln-A4.pdf



- 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