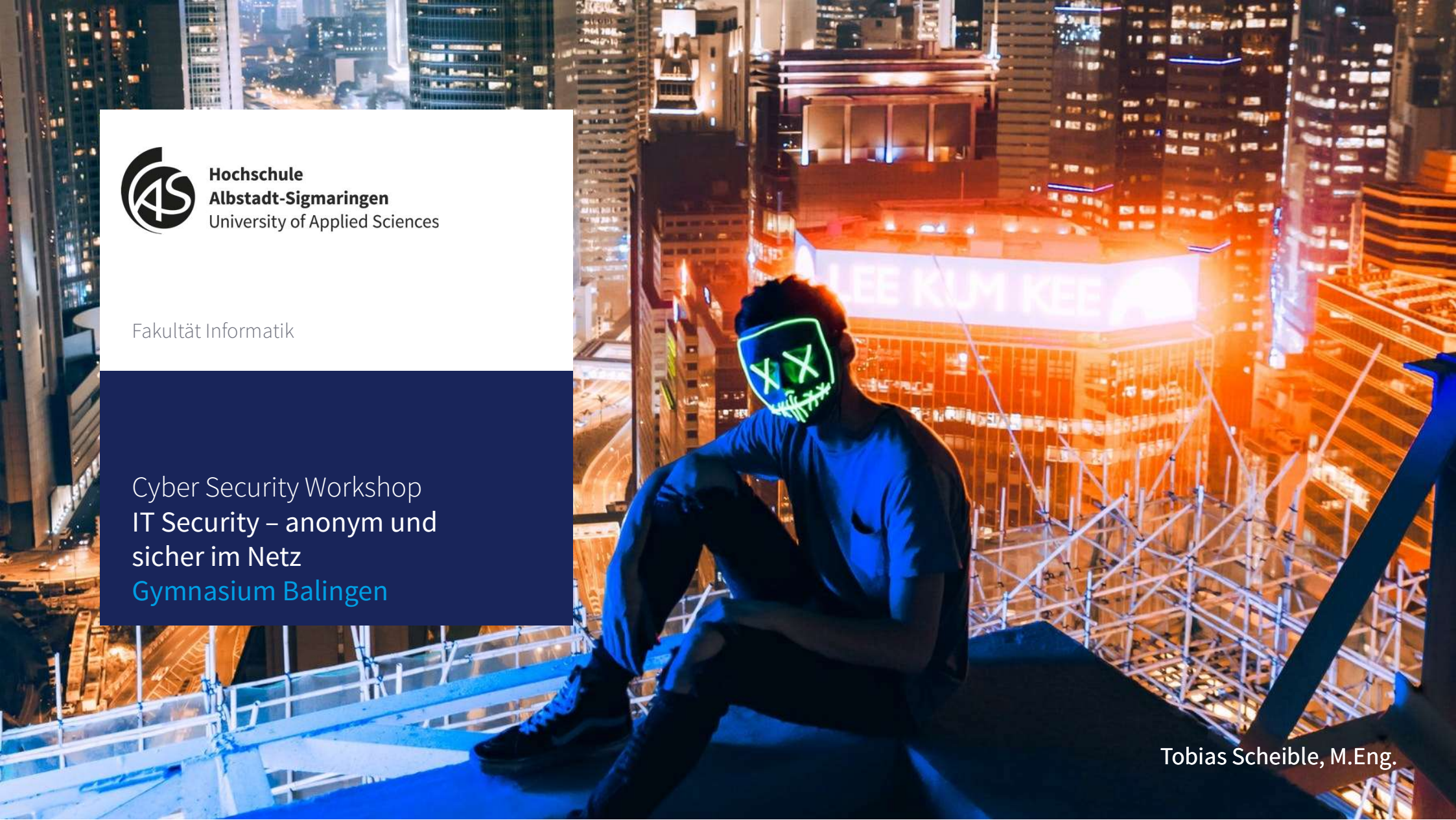


Hochschule
Albstadt-Sigmaringen
University of Applied Sciences

Fakultät Informatik

Cyber Security Workshop
IT Security – anonym und sicher im Netz
Gymnasium Balingen

Tobias Scheible, M.Eng.

Tobias Scheible, M.Eng.

Hochschule
Albstadt-Sigmaringen
University of Applied Sciences

Fakultät Informatik

- Studium Kommunikations- und Softwaretechnik, Fachrichtung Kommunikationstechnik, Hochschule Albstadt-Sigmaringen
- 2009 bis 2012: Softwareingenieur im Bereich Web Development
- Seit 2012: Wissenschaftlicher Mitarbeiter an der Hochschule Albstadt-Sigmaringen im Bereich IT-Sicherheit & Digitale Forensik
  - Forschungsschwerpunkte

Web Forensics | Web Application Security | Hacking Hardware | Benutzerzentrierte Didaktik

IT Security (Bachelor) – 4. Semester
Praktikum Cybersecurity

IT Security (Bachelor) – 5. Semester
Digitale Forensik

IT GRC Management – 4. Semester
Grundlagen der digitale Forensik

IT Security & Smart Textiles
Forschungsprojekt SEKT *www.projekt-sekt.de*

Vorträge & Workshops
LKA, IHK, VDI, Verbände, …

IT Security – anonym und sicher im Netz

Hochschule Albstadt-Sigmaringen

- 1971 Gründung der Fachhochschule Sigmaringen
- 1988/89 Campus Albstadt
- 2004 Fachhochschule wird in Hochschule umbenannt
- 24 Bachelor- und Masterstudiengänge

- Weiterbildung (berufsbegleitende Angebote)
  - Zertifikate, Data Science (Master), Digitale Forensik (Master) und IT GRC Management (Master)

IT Security – anonym und sicher im Netz

Zahlen & Fakten

Fakultät Informatik

Bachelorstudiengänge

+ IT Security
+ Technische Informatik
+ Wirtschaftsinformatik

(auch in individueller Teilzeit möglich)

Masterstudiengänge

+ Business and Security Analytics
+ Systems Engineering (Schwerpunkt Security)

Weiterbildungsangebote

+ Studium Initiale
+ Hochschulzertifikate
+ TI berufsbegleitend (BEng)
+ Data Science (MSc)
+ Digitale Forensik (MSc)
+ IT GRC Management (MSc)

Weitere Informationen:
http://hs-albsig.de/inf

Individuelle Teilzeit möglich | zum Teil auch als Kombi-Studium möglich

Agenda

- Cyber Security
- World Wide Web
- Social Engineering
- Passwortsicherheit
- Hacking Hardware

Download der Unterlage: https://hs-as.net/bl.pdf

Cyber Security

Wann gab es die ersten Computer Viren?

1985

A

1990

B

1995

C

2000

D

Geschichte der Schadsoftware

Gestern

Heute

Morgen

Gestern **Die ersten Entwicklungen**

- Proof of Concept
  - 80er Jahre Der Begriff Computervirus wird zum ersten Mal verwendet und erste Konzepte werden öffentlich vorgestellt und diskutiert
  - 1985 Zum ersten Mal berichtet eine deutschsprachige Zeitung über Computerviren
  - 1988 Zum ersten Mal werden Würmer (sich selbst replizierende Schadsoftware) eingesetzt
- Ausnutzung von Schwachstellen
  - 1997 Schadsoftware nutzt nun gezielt Schwachstellen in Programmen, Betriebssystemen oder in Hardware aus
  - 2000 „I love you" Virus findet auch in Deutschland große Verbreitung
  - 2000 Erster Trojaner für mobile Endgeräte (PDAs)
- Krimineller Hintergrund
  - 2004 Schadsoftware wird immer mehr von organisierten Kriminellen eingesetzt
  - 2005 Erster Wurm verbreitet sich automatisch auf Symbian Smartphones per MMS

Quelle: gdata.de [1]

Gestern **Ransomware - AIDS**

- Bereits 1989 wurden die ersten Angriffe mit Ransomware durchgeführt
- Die Schadsoftware wurde per 5,25“ Diskette ca. 20.000 Mal mit der Post verschickt
- Nach 90 Starts wurden die Dateinamen auf dem Laufwerk C: verschlüsselt
  - Eine italienische AIDS Organisation verlor Forschungsergebnisse aus 10 Jahren
  - Ersteller der Ransomware wurde 1990 verhaftet

Quelle: wikipedia.org [2]

Heute **Cybercrime as a Service**

Quelle: youtube.com [3]

Heute **Cybercrime as a Service**

IT Security – anonym und sicher im Netz

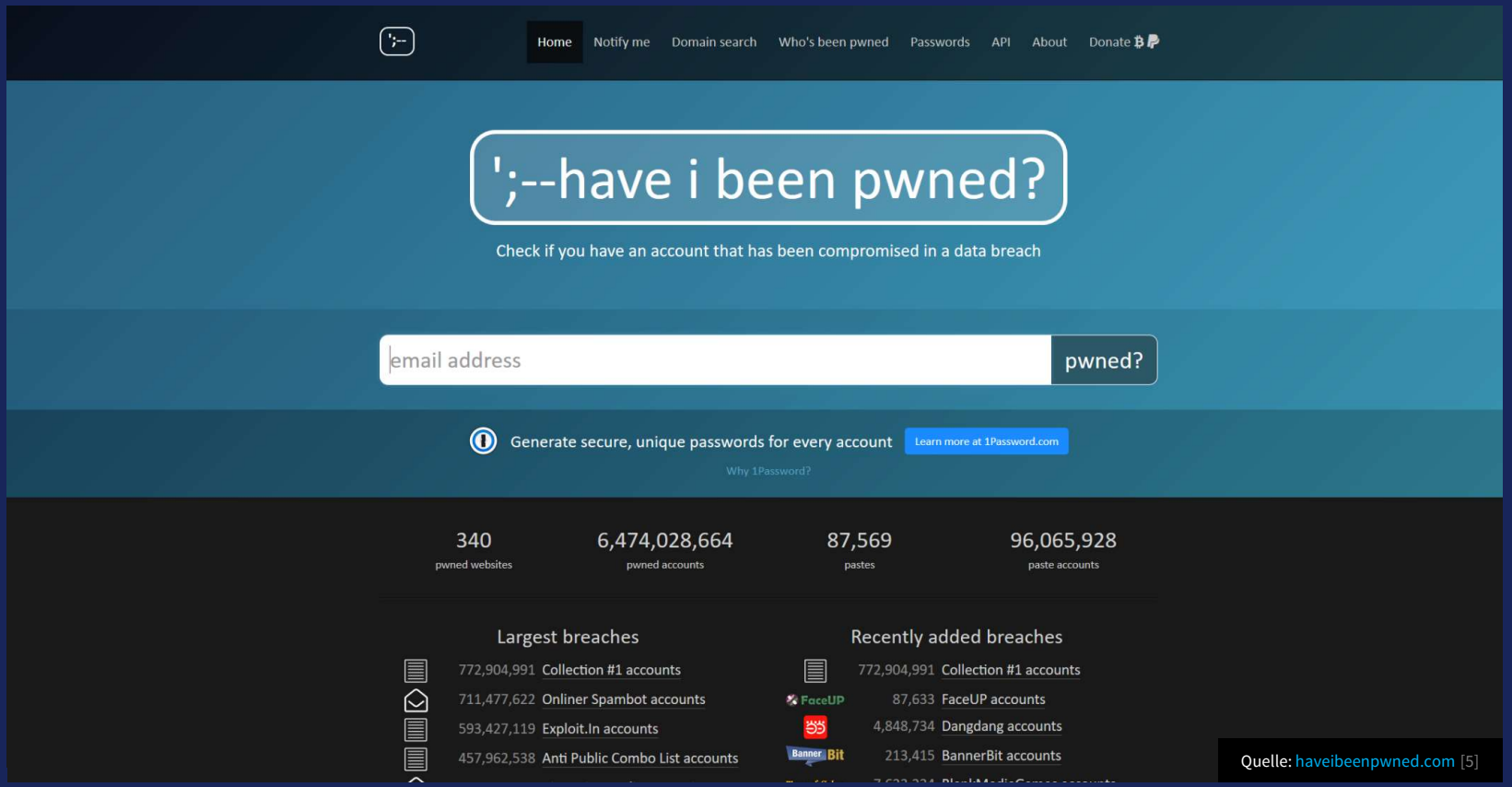
Heute **Ransomware - Locky**

- Effektive Methode, um Geld zu ergaunern
- Auf deutsche Benutzer ausgerichtete Varianten
- Verschlüsselt alle Benutzerdateien, auch auf Netzwerklaufwerke

- Zeitlicher Ablauf:
  - 15.02.2016 Locky wird als Schläfer aktiviert (Makros)
  - 22.02.2016 Gefälschte Unternehmensrechnung (JScript)
  - 24.02.2016 Gefälschtes Sipgate Fax (JScript)
  - 26.02.2016 Neue Infektionstechnik mit Batch-Dateien
  - 02.03.2016 Gefälschte BKA E-Mail (EXE-Datei)

Quelle: wikipedia.org [4]

PRAXIS Geklaute Zugangsdaten



Quelle: haveibeenpwned.com [5]

Morgen **IoT – Internet of Things**

- Ein Bot-Netz, das sich aus IoT-Geräten zusammensetzt
- Es wurde genutzt, um DDOS-Angriffe auszuführen
- Konnte auch gemietet werden
- Seiteneffekte:
  - Es wurde versucht, Router über eine Schnittstelle zur Fernwartung zu übernehmen
  - Durch eine fehlerhafte Umsetzung „stürzten“ die Router ab
  - 900.000 Router der Deutschen Telekom waren nicht mehr erreichbar

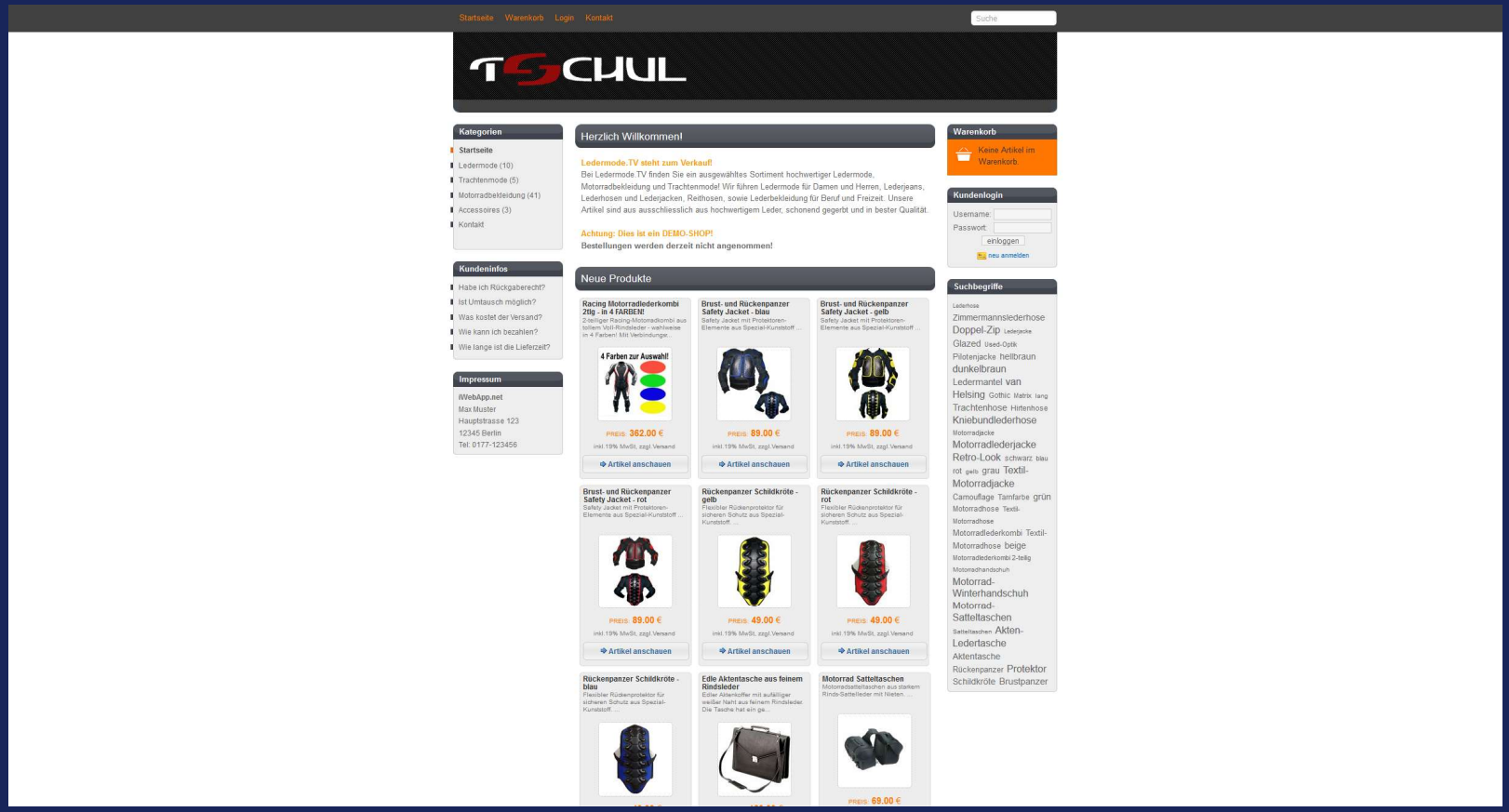
Quelle: securityaffairs.com [6]

Morgen **Ransomware - IoT & Industrieanlagen**

Quelle: computerworld.com [7]

World Wide Web

DEMO Live-Hack



Quelle: ledermode.tv [8]

Das World Wide Web

Das World Wide Web ist ein über das Internet abrufbares System von elektronischen Hypertext-Dokumenten, sogenannten Webseiten, welche mit HTML beschrieben werden. Sie sind durch Hyperlinks untereinander verknüpft und werden im Internet über die Protokolle HTTP oder HTTPS übertragen.

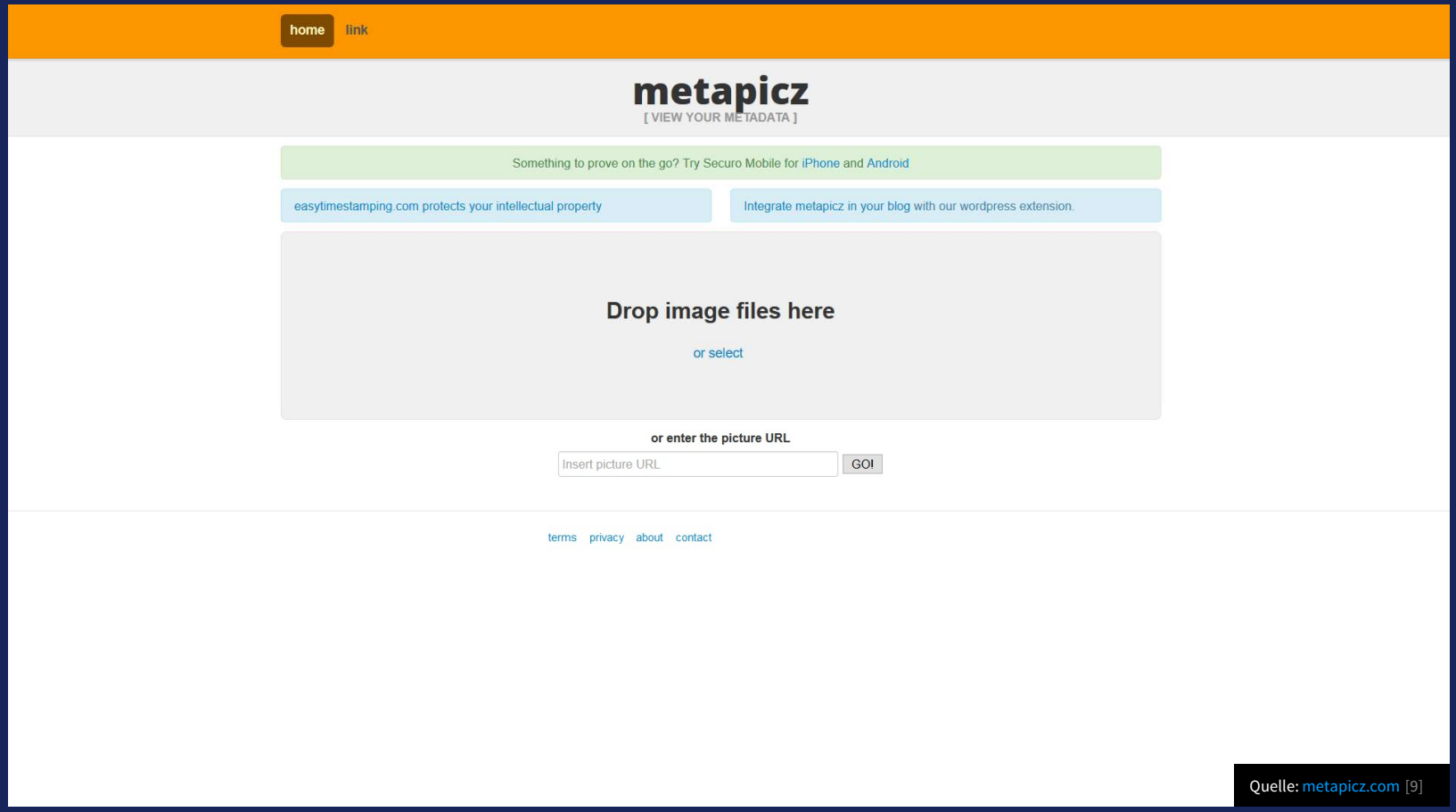
- Internet ≠ World Wide Web | Bedroht durch Walled Garden (Apps)

- Datenschutz & Privatsphäre
  - Das Nutzerverhalten von Internetnutzern wird gezielt und möglichst seitenübergreifend aufgezeichnet.
  - Gründe dafür sind die Optimierung von Dienstleitungen, zielgerichtetes Marketing sowie die Profildaten im Allgemeinen.
  - Dies lässt sich nicht vollständig vermeiden, jedoch zumindest etwas einschränken, wenn man auch etwas "Komfort" dabei einbüßt.

PRAXIS Web-Browser absichern

- Laden Sie den Portable Browser Firefox herunter und rufen Sie die Seite http://mybrowserinfo.com auf.
- Installieren Sie die foglenden AddOns:
  - uBlock Origin, Canvas Defender & User Agent Switcher
- Weitere Hinweise zur Installation:
  - https://scheible.it/firefox-web-browser-security-tuning/
- Prüfen Sie, wie sich die genannten Websites bei aktiviertem / deaktiviertem AddOn unterschiedlich verhalten.

Versteckte Informationen auslesen



Quelle: metapicz.com [9]

PRAXIS Versteckte Informationen auslesen

- Fotos, die mit dem iPhone, Android Smartphone oder mit einer Digitalkamera gemacht werden, enthalten in der Regel Metadaten. Das sind z. B.:
  - Aufnahmedatum, Autor, …
  - Kameramodell, Belichtungszeit, Blitzeinstellung…
  - aber auch Geoinformationen / GPS-Koordinaten
- Schauen Sie sich an, ob Sie im Internet Fotos finden, die entsprechende Metadaten enthalten.

  http://metapicz.com

Wie können versteckte Systeme gefunden werden?

Spezielle Software

A

Suchmaschinen

B

Geheime Datenbanken

C

Darknet

D

Hochschule
Albstadt-Sigmaringen
University of Applied Sciences

Fakultät Informatik

Hacking mit Google

Quelle: google.de [10]

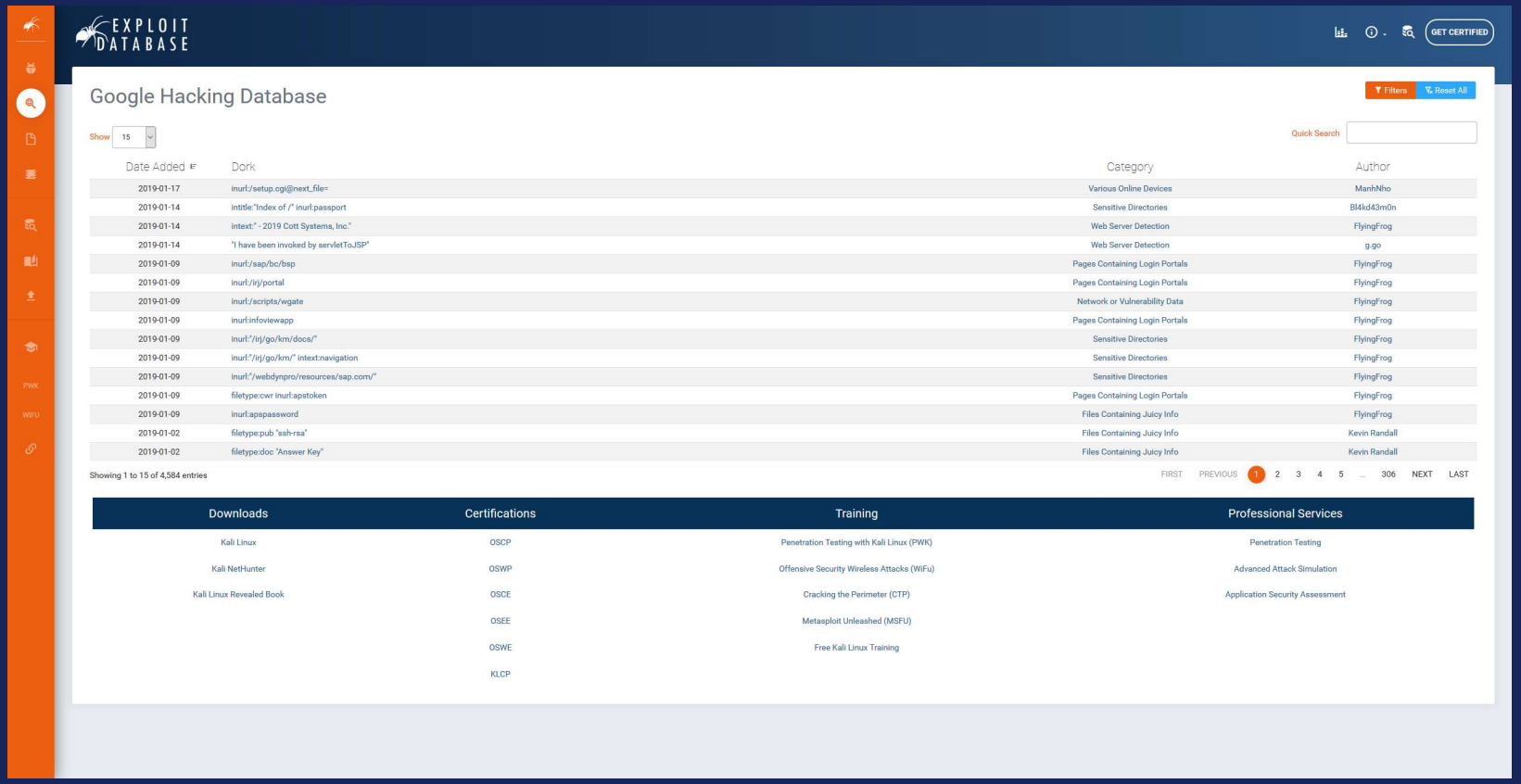
Hacking mit Google

Parameter	Beschreibung
site:	Eine Suche mit dem Suchparameter "site"in Verbindung mit einer Domain oder URL liefert alle Seiten dieser Domain, die verfügbar sind. Beispiel: *it security site:hs-albsig.de*
intitle:	Eine Suche mit dem Suchparameter "intitle" in Verbindung mit einem Suchbegfriff liefert Ergebnisse von Webseiten, deren Titel diesen Suchbegriff enthält. Beispiel: *intitle:"it security"*
inurl:	Eine Suche mit dem Suchparameter "inurl:" in Verbindung mit einem Suchbegfriff liefert Ergebnisse von Webseiten, deren URL den Suchbegriff enthält. Beispiel: *inurl:"it-security"*
intext:	Mit dem Suchparameter "intext" in Verbindung mit einem Suchbegriff werden Webseiten angezeigt, in denen der Begriff im Text der Seite vorkommt. Beispiel: *intext:"it security bachelor"*

PRAXIS Hacking mit Google

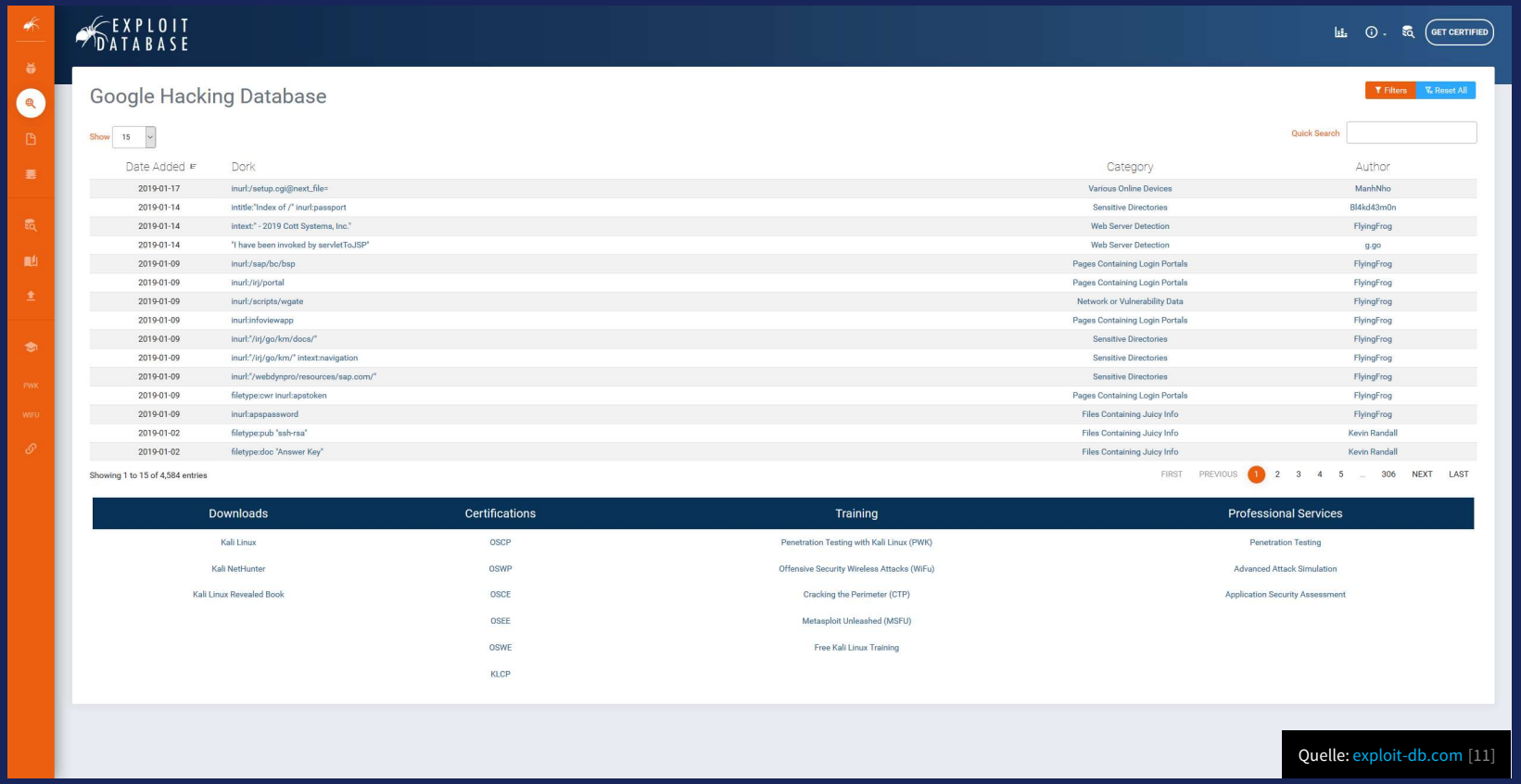
- Beispiel Suchanfragen nach Webcams:
  - intitle:webcam 7 inurl:8080 -intext:8080
  - intext:"powered by webcamXP 5“
  - inurl:"viewerframe?mode=motion"
  - intitle:"Live View / - AXIS"
  - inurl:indexFrame.shtml
  - intitle:"EvoCam" inurl:"webcam.html"

Hacking mit Google - GHDB



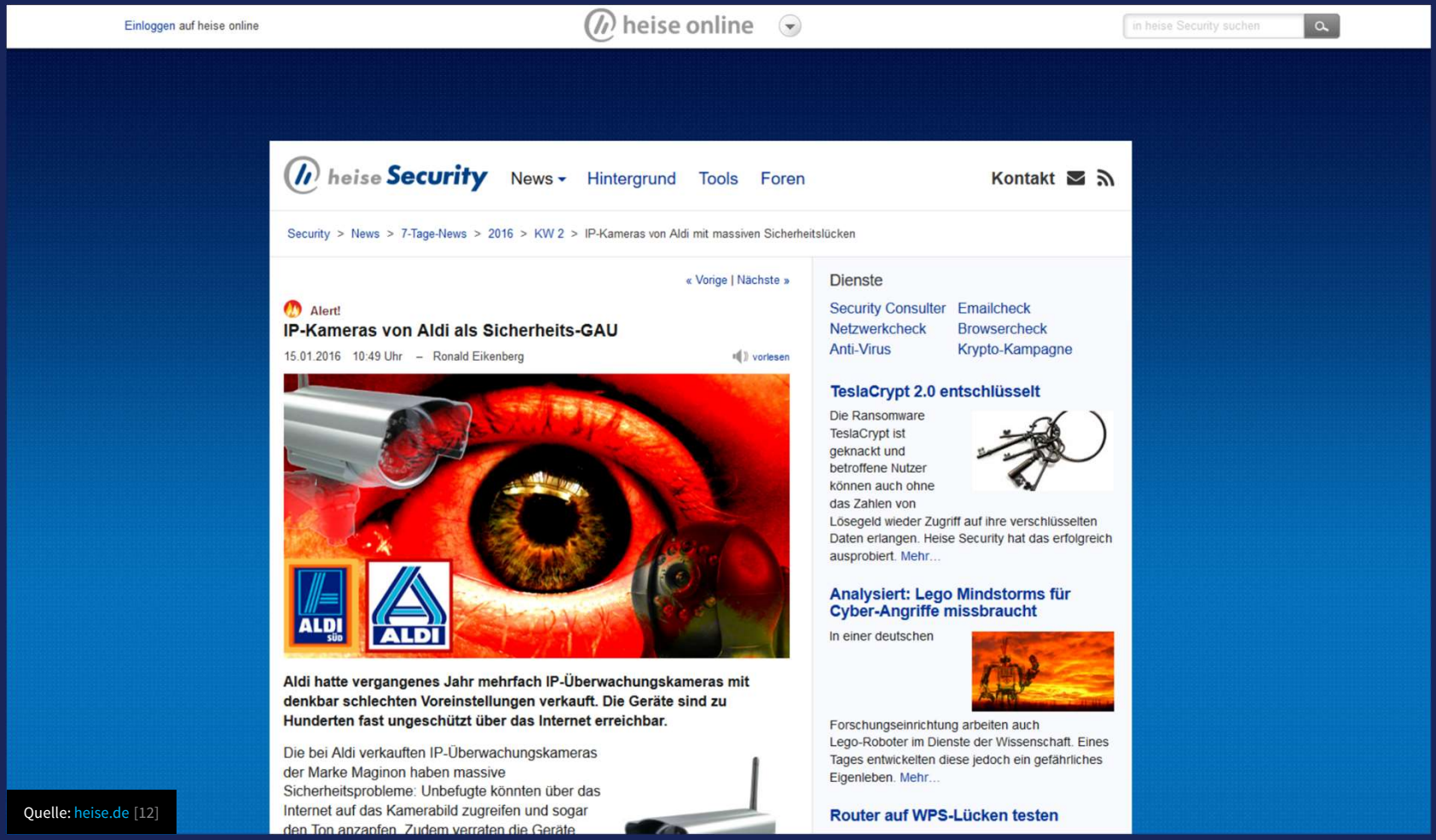
Quelle: exploit-db.com [11]

PRAXIS Hacking mit Google - GHDB



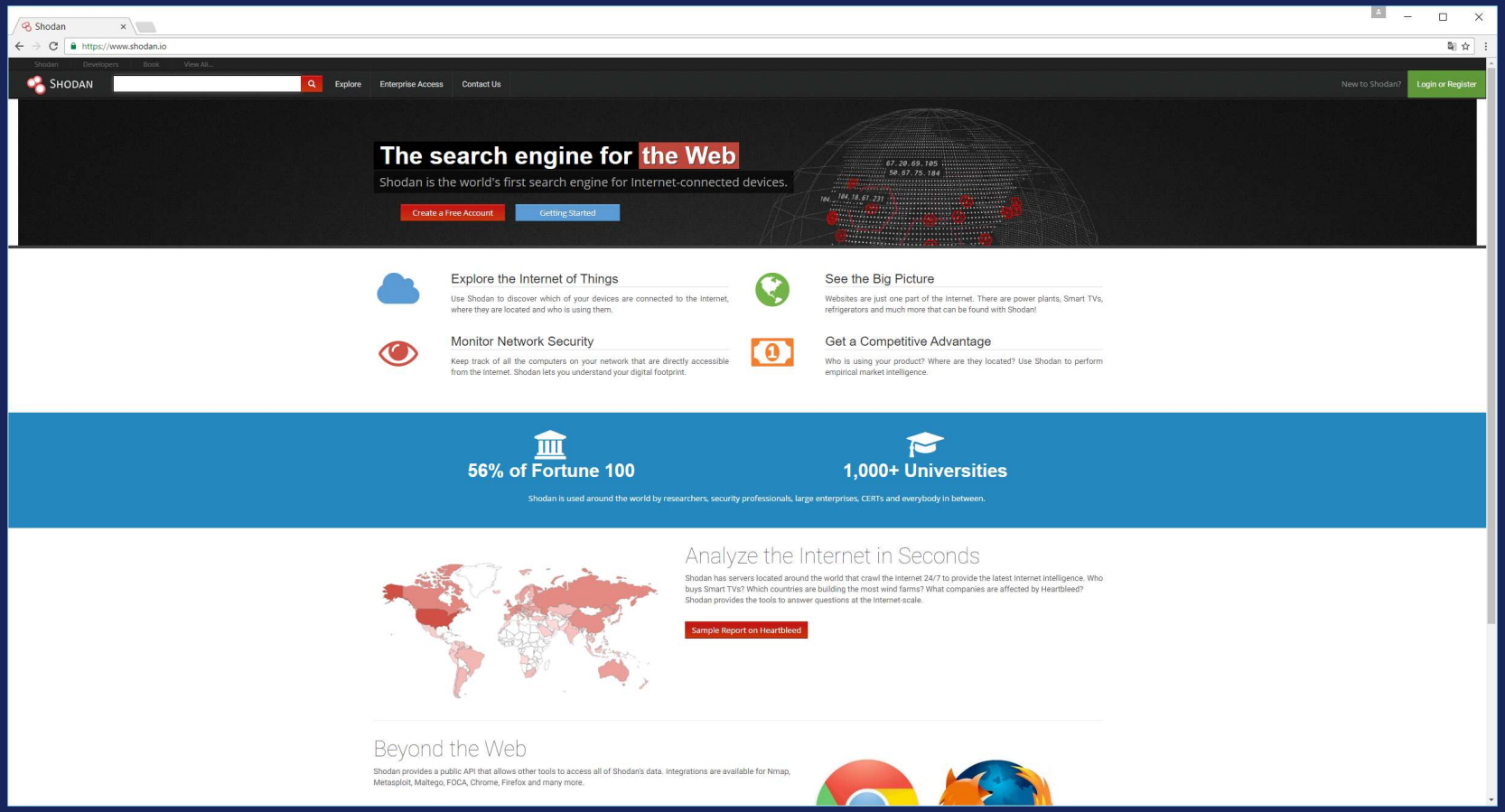
Quelle: exploit-db.com [11]

Bug or Feature?



Quelle: heise.de [12]

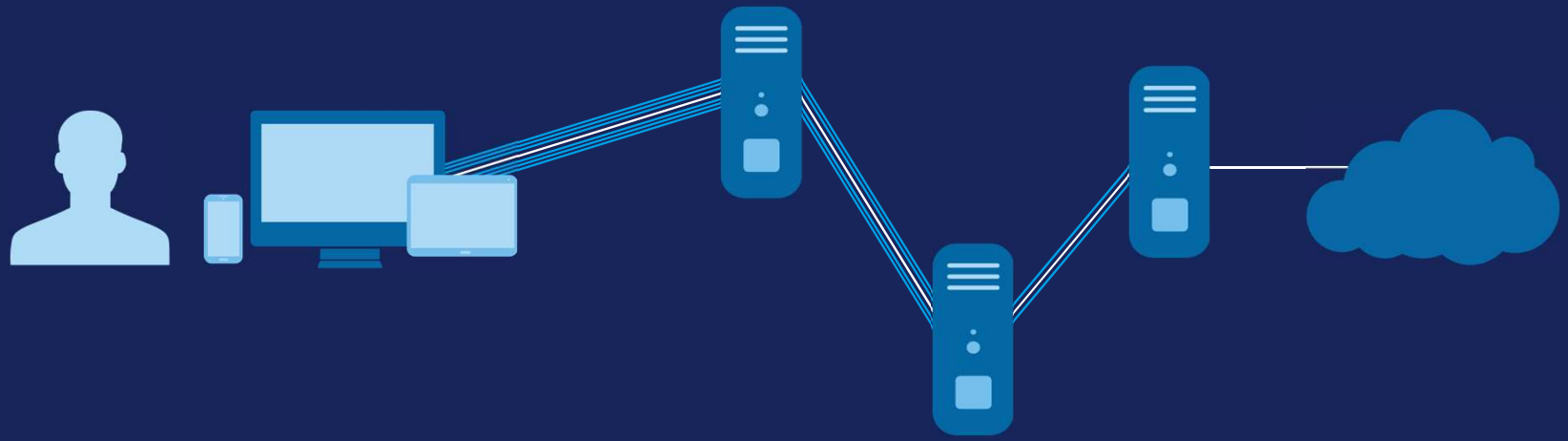
DEMO Suchmaschine für das Internet der Dinge



Quelle: shodan.io [13]

Tor Netzwerk

- Spendenfinanziertes Opensource-Projekt mit über 5000 Tor-Nodes
- Komplette Browser Bundles für Windows, Mac OS X, Linux, Android
- Zufällige und verschlüsselte Route über drei Tor-Nodes
- Jede Note kennt immer nur den Vorgänger und den Nachfolger
- Wichtig: nur Anonymisierung, keine Verschlüsselung und Integritätsschutz



PRAXIS Tor Netzwerk - Darknet

- Laden Sie den TOR-Browser herunter
  - https://www.torproject.org/projects/torbrowser.html.en
- Welche Informationen werden zur Verfügung gestellt?
  - http://www.utrace.de und http://mybrowserinfo.com
- Surfen Sie auf einer Website und prüfen Sie, welche Verbindungsroute gewählt wurde
  - Wechseln Sie Ihre Identität
- Öffnen Sie die folgenden Hidden Services (Darknet-Websites):
  - https://3g2upl4pq6kufc4m.onion
  - http://vfqnd6mieccqyiit.onion

Fazit World Wide Web

- Wenn Sie Fotos online stellen, entfernen Sie alle Metadaten von diesen Fotos.
- Die Surfgewohnheiten können sehr einfach erfasst werden, auch wenn der Verlauf und alle Cookies gelöscht werden. Daher müssen Plugins eingesetzt werden, um die Spuren zu verschleiern.
- Nutzen Sie mehrere Web-Browser (Firefox, Chrome & Edge) für unterschiedliche Aktivitäten. Einen für die dauerhaften Logins, einen für die tägliche Recherche und einen für Medien.
- Nutzen Sie den Tor-Browser, um Ihre Privatsphäre zu schützen, wenn Sie nach sehr privaten Themen im Internet suchen.

Social Engineering

Was ist die häufigste Angriffsmethode?

Ausnutzung von Schwachstellen

A

Physische Attacken

B

Manipulation von Personen

C

Ausnutzung von Fehlern

D

Aktion der Groupe Mutuel

Quelle: youtube.com [14]

IT Security – anonym und sicher im Netz

Social Engineering - Gefälschte E-Mail

Home | Video | Themen | Forum | English | DER SPIEGEL | SPIEGEL TV | Abo | Shop Schlagzeilen | Wetter | TV-Programm | mehr ▼

Login | Registrierung

SPIEGEL ONLINE SCHULSPIEGEL

Abi - und dann? | Querweltein | Leben U21 | Wissen

Nachrichten > SchulSPIEGEL > Wetter > Schulfrei in Niedersachsen wegen gefälschter E-Mail

Gefälschte E-Mail: Schulfrei ermogelt

DPA

Winterwetter in Niedersachsen: Freier Tag im Schnee wegen gefälschter E-Mail

Eine gefälschte E-Mail hat Schülern in Niedersachsen einen freien Tag beschert. Der Unterricht falle wegen des Winterwetters aus, hieß es darin. Hunderte Schüler glaubten der Meldung - und blieben zu Hause.

Quelle: spiegel.de [15]

Moderner Gefängnisausbruch

- Moderner Ausbruch aus einem britischen Gefängnis (März 2015)
- Social Engineering Angriff auf das Gefängnis
  - Smartphone eingeschmuggelt
  - Domain reserviert, die dem zuständigen Gericht ähnelt
  - E-Mail-Adresse mit dieser Domain eingerichtet
  - Hat sich als leitender Beamter ausgegeben
  - Anweisungen zu seiner Entlassung gegeben

- Gefangener kam frei

Quelle: heise.de [16]

Faktor Mensch

Freitag, 12. Februar 2016 | Service | Abo | Shop | Newsletter | Login | Registrieren | Suchbegriff, WKN, ISIN

Wirtschafts Woche

UNTERNEHMEN FINANZEN POLITIK ERFOLG TECHNOLOGIE

Trends Management Gründer Beruf Jobsuche Campus & MBA Karriere Jobturbo

DAX ® 8.752,87 −2,93% | E-STOXX 50® 2.680,35 −3,90% | MDAX ® 17.594,68 −2,83% | Dow Jones 15.660,18 −1,60% | Gold (USD) 1.242,83 −0,30% | EUR/USD 1,1315 −0,00% | Börsenkurse | cfd Indikationen

Die WirtschaftsWoche > Erfolg > Management > Falsche Chefs zocken Firmen ab: Den Enkeltrick gibt's auch bei Unternehmen

Falsche Chefs zocken Firmen ab

18. August 2015

Den Enkeltrick gibt's auch bei Unternehmen

0 Kommentare

Versenden
Drucken
Merken
Startseite

FOTOS

Nicht nur gutgläubige Senioren werden Opfer von Trickbetrügern.

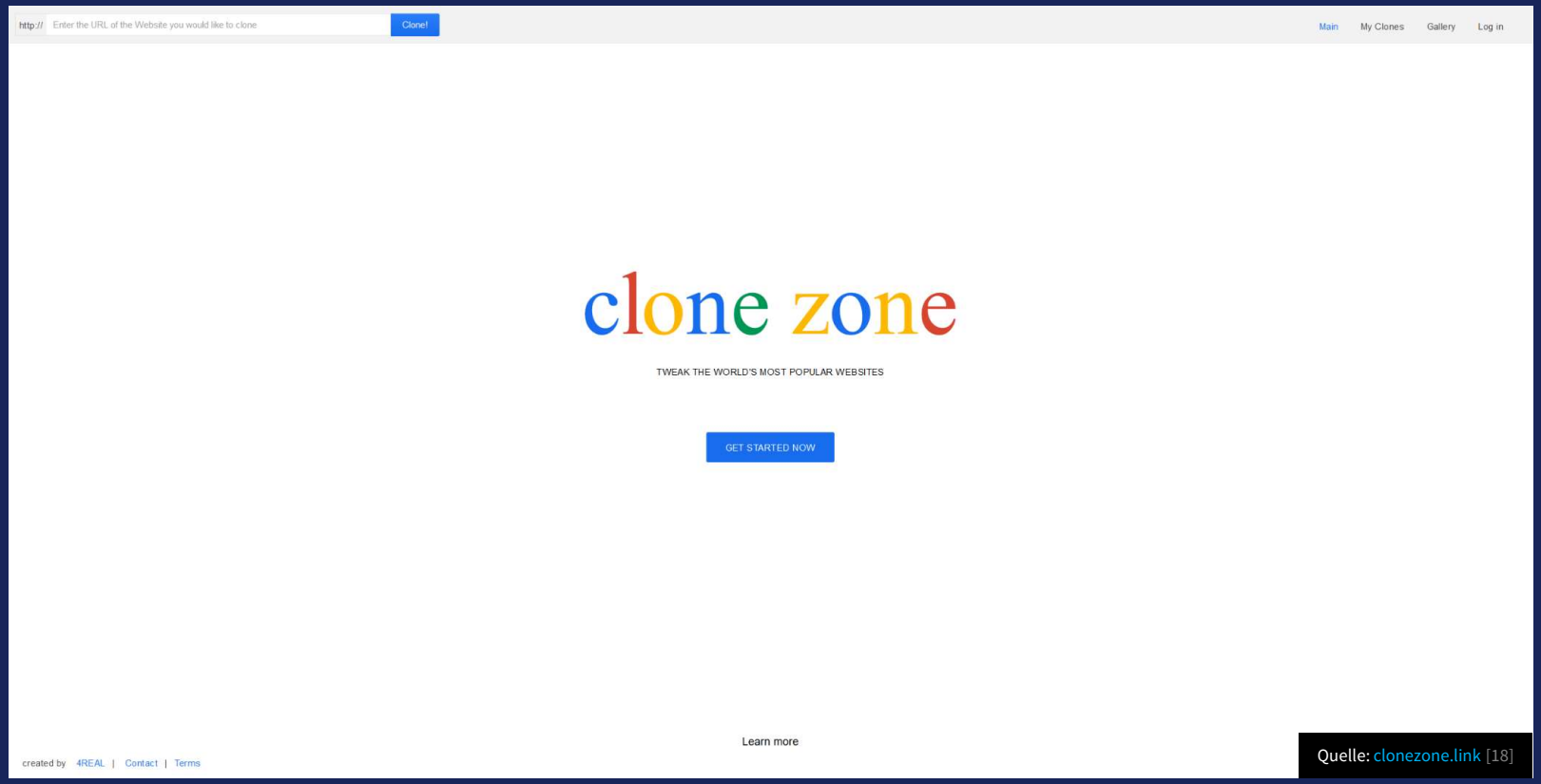
Bild: dpa

Während sich manche Betrüger als vermisste Enkel ausgeben, um ans Ersparte von Senioren zu kommen, probieren es andere eine Nummer größer. Sie geben sich als Chef aus und erleichtern Unternehmen um Millionenbeträge.

"Hallo, ich bin's, der Chef. Bitte überweisen Sie folgenden Betrag auf folgendes Konto..." So oder so ähnlich funktioniert die Betrugsmasche "CEO Fraud", die derzeit nach Deutschland schwappt. Dabei kontaktieren die mutmaßlichen Betrüger per Telefon und E-Mail Mitarbeiter von Unternehmen und geben sich

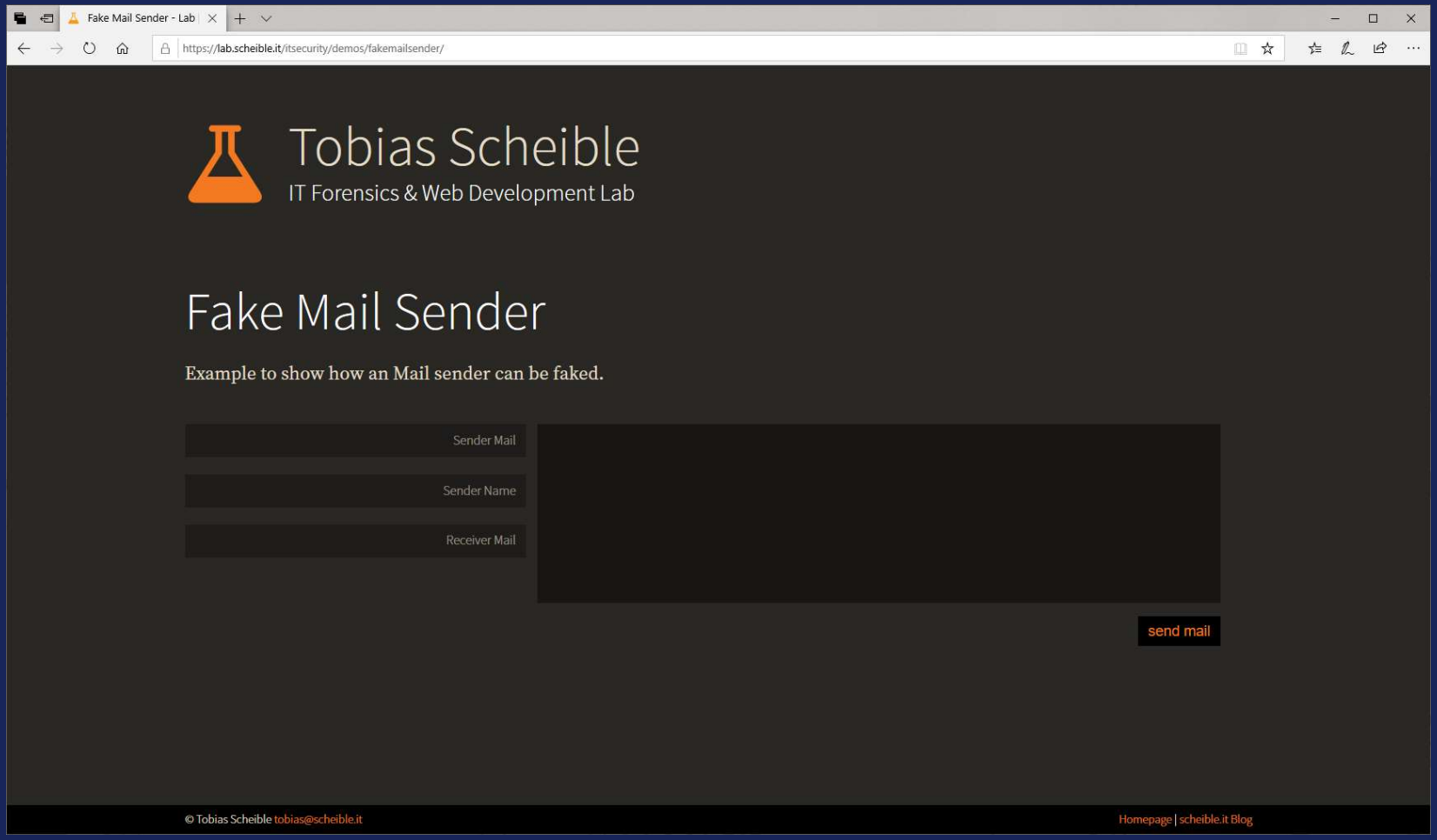
Quelle: wiwo.de [17]

PRAXIS Website manipulieren

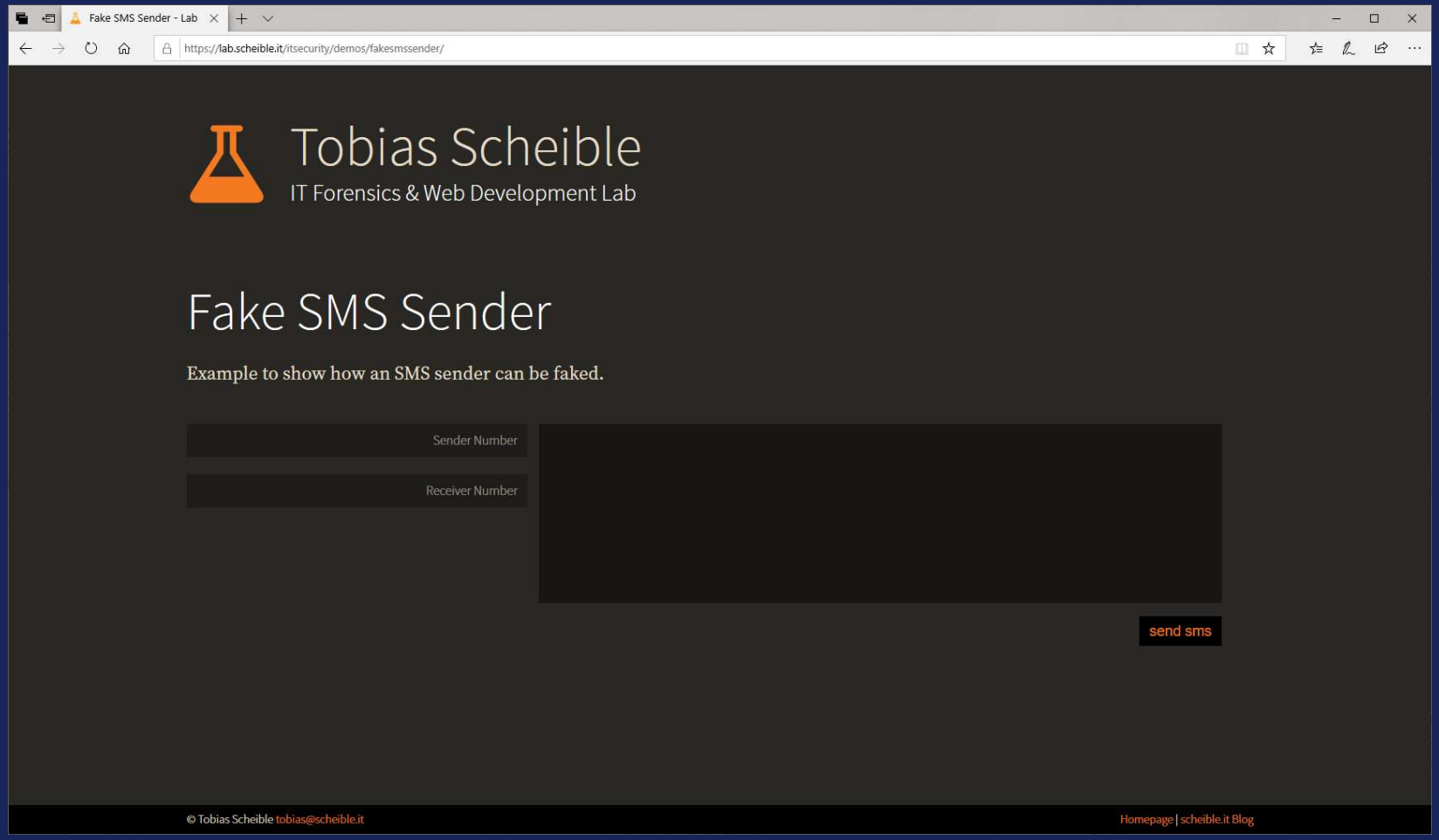


Quelle: clonezone.link [18]

DEMO E-Mail-Versand manipulieren



DEMO SMS-Versand manipulieren



Fazit Social Engineering

- Informationen im Internet, aber auch in der realen Welt, können sehr einfach gefälscht werden. Machen Sie sich Gedanken, wie Sie Informationen überprüfen können.
- E-Mails können sehr einfach gefälscht werden und können sogar die Absenderadresse eines persönlichen Kontaktes beinhalten.
- Allerdings können auch SMS und andere Nachrichten einfach gefälscht werden.
- Tipp: Auf einem anderen Kanal nachfragen, ob es wirklich stimmt.

Passwortsicherheit

00000000

?

Quelle: heise.de [19]

Wofür wurde der Pin-Code verwendet?

Fort Knox

A

Alcatraz

B

Area 51

C

Atomraketen

D

00000000

Launch-Code für die in den USA stationierten Atomraketen

(1962 bis 1977)

Quelle: heise.de [19]

Faktor Mensch

Quelle: pics-for-fun.com [20]

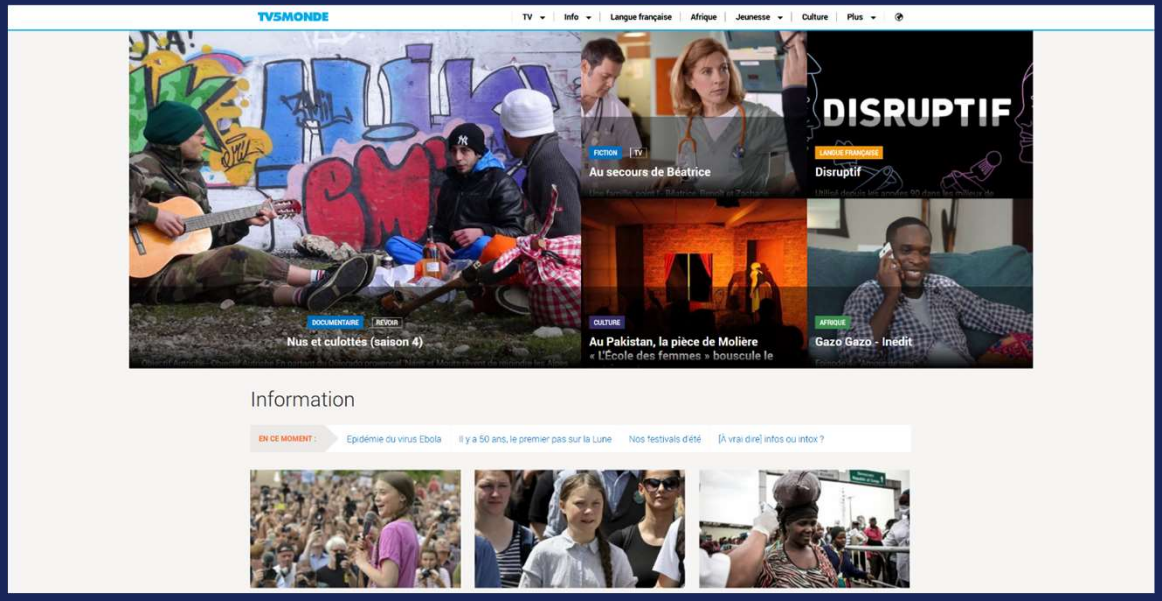
Quelle: : de.pinterest.com [21]

Passwortsicherheit

Quelle: youtube.com [22]

Angriff auf den Fernsehsender TV5

- Umfangreicher Angriff auf den französischen Sender TV5Monde
  - Alle Kanäle des Fernsehunternehmens TV5Monde gingen offline
  - Die Website verbreitete kurzfristig islamistische Drohungen
  - Auf der Facebook-Seite wurden ebenfalls Drohungen verbreitet
  - Spekulationen über öffentlich einsehbare Passwörter



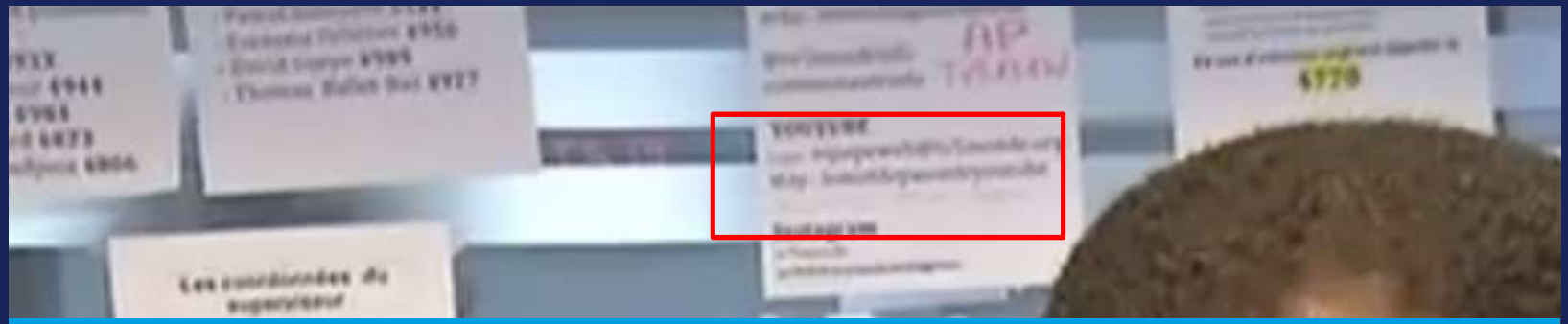
Quelle: heise.de [23]

Angriff auf den Fernsehsender TV5

Quelle: heise.de [23]

IT Security – anonym und sicher im Netz

Angriff auf den Fernsehsender TV5



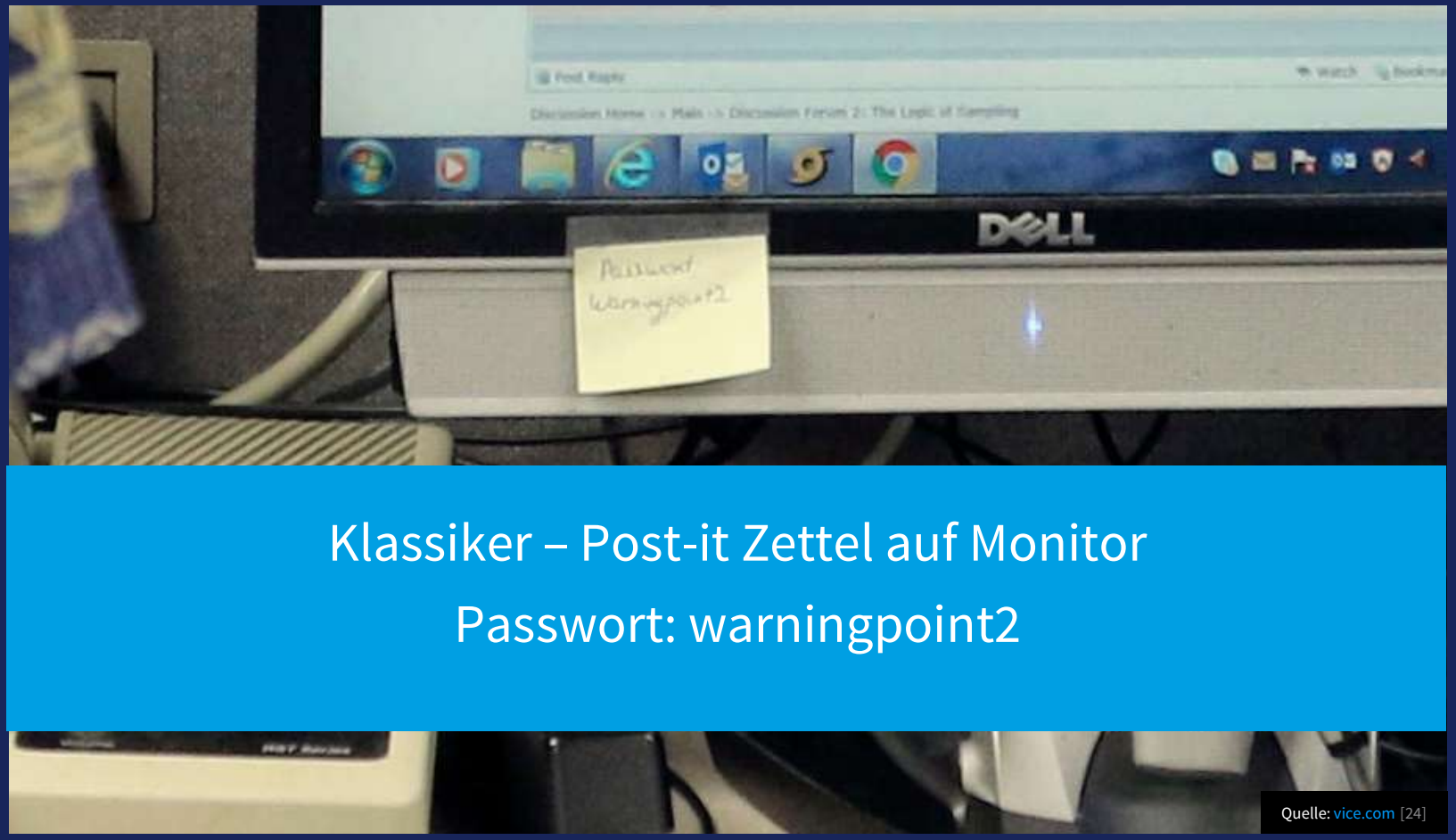
YouTube Passwort: "lemotdepassedeyoutube"
(etwa "dasyoutubepasswort")

Quelle: heise.de [23]

Faktor Mensch

Quelle: vice.com [24]

Faktor Mensch



Klassiker – Post-it Zettel auf Monitor

Passwort: warningpoint2

Quelle: vice.com [24]

Angriffe auf Passwörter

Passwörter erraten

Brute-Force Methode

Bekannte Passwörter

Passwörter erraten

- Angreifer analysieren das Umfeld eines Opfers, um auf potentielle Passwörter schließen zu können und so diese zu erraten.
  - Alle Seiten bzw. Profile von einem Opfer werden gesucht und analysiert.
  - Dabei werden bevorzugt Inhalte von Social Media Seiten automatisch gescannt.
  - Auch Fotos werden ausgewertet und Texte automatisch erkannt – z.B. Autokennzeichen.
  - Typische Informationen wie Namen von Verwandten, Adressen, Geburtsdaten oder Haustiere werden gezielt gesucht.
  - Aus diesen Informationen werden individuelle Listen mit potentiellen Passwörtern generiert.

- Bei Unternehmen wird die Website gescannt und alle Dokumente analysiert.
  - Aus den gefundenen Begriffen werden vielfältige Kombinationen generiert.

PRAXIS Passwörter erraten

- Versuchen Sie, die geschützten Dokumente zu knacken
  - Laden Sie die Test-Dateien herunter und analysieren Sie den Lebenslauf
  - Probieren Sie verschiedene Passwortkombinationen aus
  - Versuchen Sie, die PDF-Dateien zu öffnen

Wie lauten die Passwörter der Dateien? Finden Sie mindestens eines heraus.

Bekannte Passwörter

124 lines (115 sloc) | 6.67 KB

Raw Blame History

```
Top 100 Adobe Passwords with Count

We do not (yet) have the keys Adobe used to encrypt the passwords of 130,324,429 users affected by
their most recent breach. However, thanks to Adobe choosing symmetric key encryption over hashing,
selecting ECB mode, and using the same key for every password, combined with a large number of
known plaintexts and the generosity of users who flat-out gave us their password in their password
hint, this is not preventing us from presenting you with this list of the top 100 passwords
selected by Adobe users.

While we are fairly confident in the accuracy of this list, we have no way to actually verify it
right now. We don't have the keys, and Adobe is not letting any of the affected accounts log in
until the owners reset their passwords. So, it is possible there is an error or two in here. Caveat
emptor and such.
```

Quelle: github.com [25]

Was ist das häufigste Passwort?

password

A

123456

B

adobe123

C

qwerty

D

Bekannte Passwörter

124 lines (115 sloc) | 6.67 KB

Raw Blame History

```
Top 100 Adobe Passwords with Count

We do not (yet) have the keys Adobe used to encrypt the passwords of 130,324,429 users affected by
their most recent breach. However, thanks to Adobe choosing symmetric key encryption over hashing,
selecting ECB mode, and using the same key for every password, combined with a large number of
known plaintexts and the generosity of users who flat-out gave us their password in their password
hint, this is not preventing us from presenting you with this list of the top 100 passwords
selected by Adobe users.

While we are fairly confident in the accuracy of this list, we have no way to actually verify it
right now. We don't have the keys, and Adobe is not letting any of the affected accounts log in
until the owners reset their passwords. So, it is possible there is an error or two in here. Caveat
emptor and such.


                                    Plaintext
                                ------------------
                                    123456
                                    123456789
                                    password
                                    adobe123
                                    12345678
                                    qwerty
                                    1234567
                                    111111
```

Quelle: github.com [25]

Wie häufig kam das Passwort 123456 vor?

ca. 500.000

A

ca. 1.000.000

B

ca. 2.000.000

C

ca. 3.000.000

D

Bekannte Passwörter

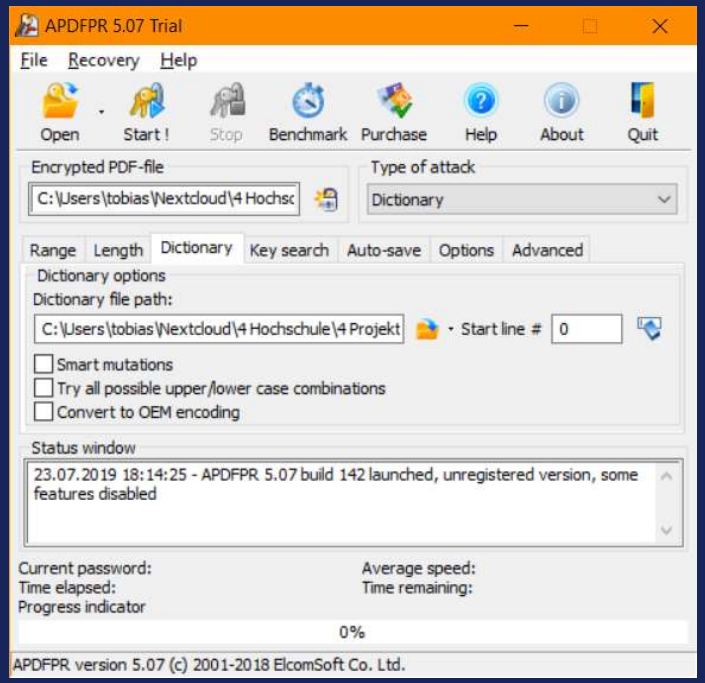
124 lines (115 sloc) | 6.67 KB Raw | Blame | History

```
Top 100 Adobe Passwords with Count

We do not (yet) have the keys Adobe used to encrypt the passwords of 130,324,429 users affected by
their most recent breach. However, thanks to Adobe choosing symmetric key encryption over hashing,
selecting ECB mode, and using the same key for every password, combined with a large number of
known plaintexts and the generosity of users who flat-out gave us their password in their password
hint, this is not preventing us from presenting you with this list of the top 100 passwords
selected by Adobe users.

While we are fairly confident in the accuracy of this list, we have no way to actually verify it
right now. We don't have the keys, and Adobe is not letting any of the affected accounts log in
until the owners reset their passwords. So, it is possible there is an error or two in here. Caveat
emptor and such.



#      Count      Ciphertext                      Plaintext
------------------------------------------------------------
1.   1911938      EQ7fIpT7i/Q=                    123456
2.    446162      j9p+HwtWWT86aMjgZFLzYg==        123456789
3.    345834      L8qbAD3jl3jioxG6CatHBw==        password
4.    211659      BB4e6X+b2xLioxG6CatHBw==        adobe123
5.    201580      j9p+HwtWWT/ioxG6CatHBw==        12345678
6.    130832      5djv7ZCI2ws=                    qwerty
7.    124253      dQi0asWPYvQ=                    1234567
8.    113884      7LqYzKVeq8I=                    111111
```

Quelle: github.com [25]

PRAXIS Bekannte Passwörter

- Laden Sie die Software herunter und knacken Sie die PDF-Dateien.
- Verwenden Sie als Wörterbuch die TXT-Datei aus der ZIP-Datei



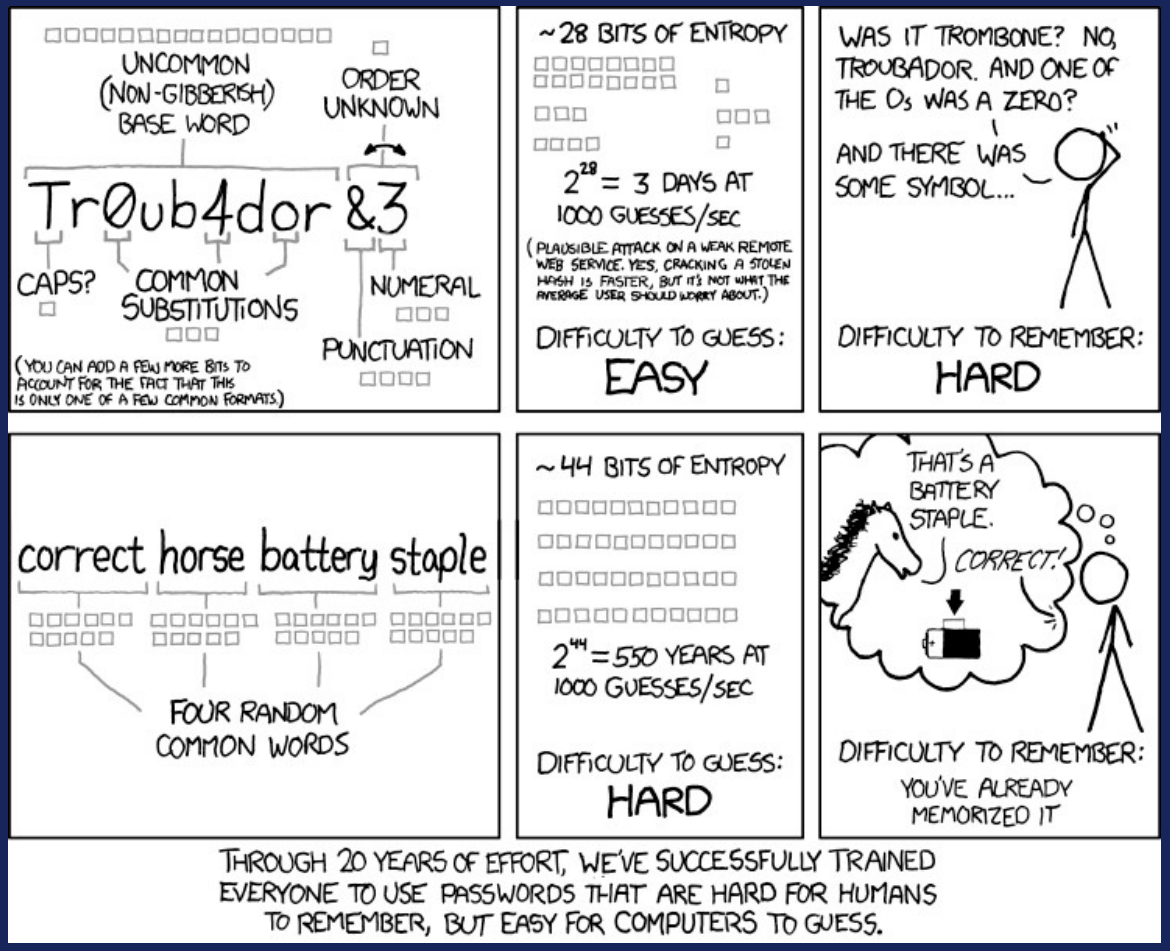
Brute-Force Methode

- Mit Brute-Force-Angriffen wird versucht, ein Passwort zu knacken, indem in schneller Abfolge verschiedene Zeichenkombinationen ausprobiert werden.
- Der Algorithmus ist sehr einfach und beschränkt sich auf das Ausprobieren möglichst vieler Zeichenkombinationen, weshalb auch von "erschöpfender Suche" gesprochen wird.
- Dabei hängt es von der verfügbaren Rechenleistung ab, wie viele Berechnungen pro Sekunde durchgeführt und entsprechend eine hohe Anzahl an Kombinationen ausprobiert werden können.
- Die Methode wird in der Praxis häufig erfolgreich eingesetzt, da viele Benutzer kurze Passwörter verwenden, die darüber hinaus oft nur aus Zeichen des Alphabets bestehen, womit die Anzahl der möglichen Kombinationen drastisch reduziert und das Erraten erleichtert wird.

Brute-Force Methode

- Komplexität von Passwörtern: Zeichenanzahl $^{\text{Passwortlänge}}$ = Kombinationen
  - Zeichenanzahl
    - Alphabet = 26 Zeichen
      - Mit Groß- und Kleinschreibung = 52 Zeichen
      - Mit den Umlauten = 59 Zeichen
    - Zahlen = 10 Zeichen
    - Sonderzeichen = 32 Zeichen
    - 101 verschiedene Zeichen
  - Beispiele
    - Kleinbuchstaben 26^4 = 456.976
    - Kleinbuchstaben + Zahlen 36^4 = 1.679.616
    - Alle Buchstaben + Zahlen 69^4 = 22.667.121
    - Alle Zeichen 101^4 = 104.060.401

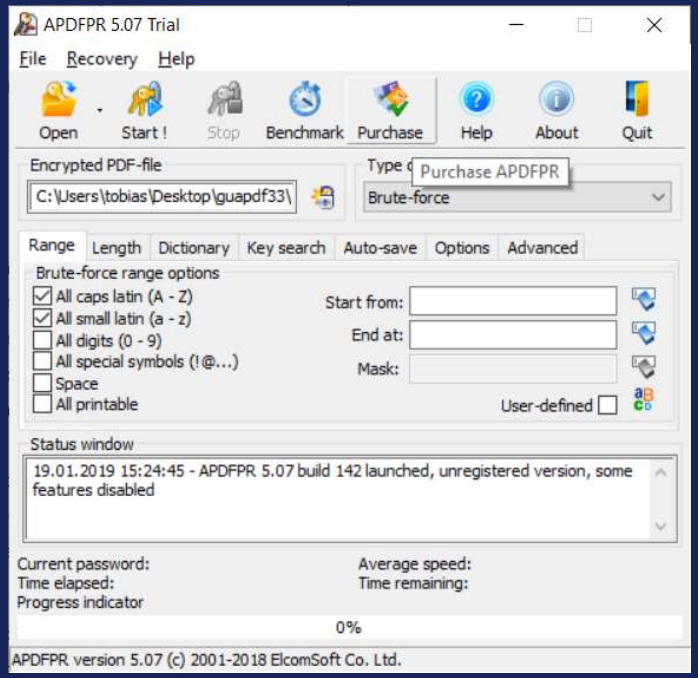
Brute-Force Methode



Quelle: xkcd.com [26]

PRAXIS Brute-Force Methode

- Verwenden Sie wieder die Software und knacken Sie die PDF-Dateien.
- Notieren Sie jeweils die benötigte Zeit für die unterschiedlichen Dateien.



Sichere Passwörter

Individuelle & lange Passwörter

Zwei-Faktor-Authentifizierung

Bekannte Passwörter

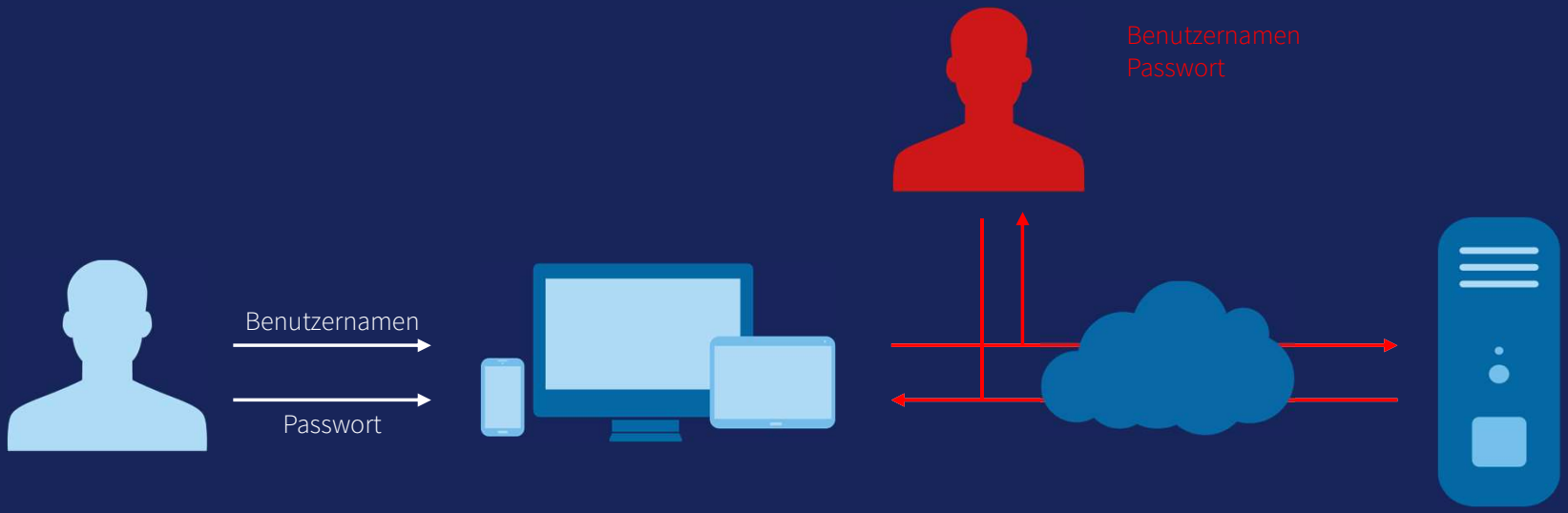
Individuelle & lange Passwörter

- Mythen
  - Passwörter brauchen möglichst viele Sonderzeichen
  - Häufige Passwortwechsel erhöhen die Sicherheit
  - Die Zwei-Faktor-Authentifizierung ist kompliziert und unnötig
  - Am besten merkt man sich Passwörter mit Stift und Papier
  - Biometrische Passwörter sind sicherer als Textpasswörter

- Möglichst lange Passwörter verwenden
- Bei jedem Dienst ein anderes Passwort verwenden
- Bildliches Szenario als Merkhilfe
- Eigenen Dialekt miteinfließen lassen

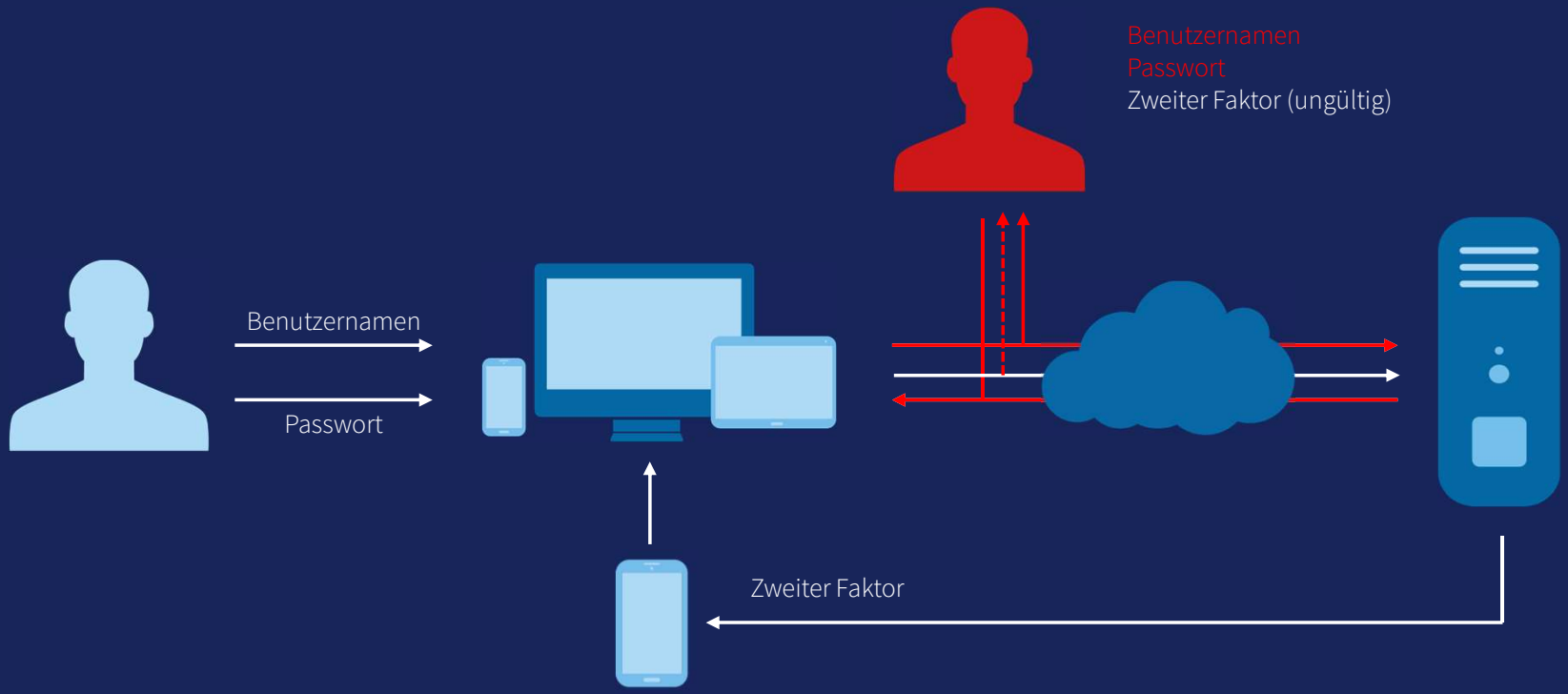
Zwei-Faktor-Authentifizierung

- Klassische Authentifizierung



Zwei-Faktor-Authentifizierung

- Klassische Authentifizierung



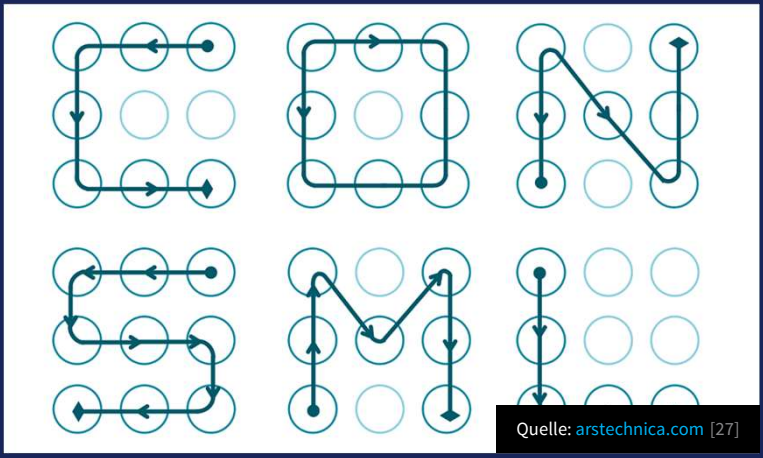
Passwortmanager

Wer viele Online-Accounts hat, für den empfiehlt sich ein Passwort-Verwaltungsprogramm. Diese Programme können neben der Passwort-Verwaltung auch starke Passwörter generieren. Sie müssen sich dann nur noch ein gutes Masterpasswort überlegen und merken.

- Speichert Passwörter in einem verschlüsselten Container mit einem Masterpasswort
- Unterstützt bei der Generierung von Passwörtern
- Verschiedene Lösungen sind vorhanden – z.B. KeePassXC
  - Viele Möglichkeiten zur Erweiterung (Firefox / Chrome Plugin, …)

Bad Lock Patterns

- Studie von Marte Løge analysierte über 4000 Android Entsperrmuster im Rahmen ihrer Master Thesis
  - 10 % aller Versuchspersonen nutzen ein Muster, das einem Buchstaben ähnelt
  - 44 % starten oben links
  - 77 % fangen in einer der vier Ecken an
  - Durchschnittliche Anzahl von fünf verwendeten Knoten
  - Muster von links → rechts; oben → unten werden häufig verwendet



Quelle: arstechnica.com [27]

Sperrmuster vs. PIN

Länge	Wischmuster Kombinationen	PIN Kombinationen
4	1624	10^4 = 10000
5	7152	10^5 = 100000
6	26016	10^6 = 1000000
7	72912	10^7 = 10000000
8	140704	10^8 = 100000000
9	140704	10^9 = 1000000000

Fünf Versuche möglich, dann 30 Sekunden Wartepause. Dadurch ist ein 5-stelliges Wischmuster in ~ 12 Stunden zu knacken (ein 4- oder 5- stelliges in ~15 Stunden).

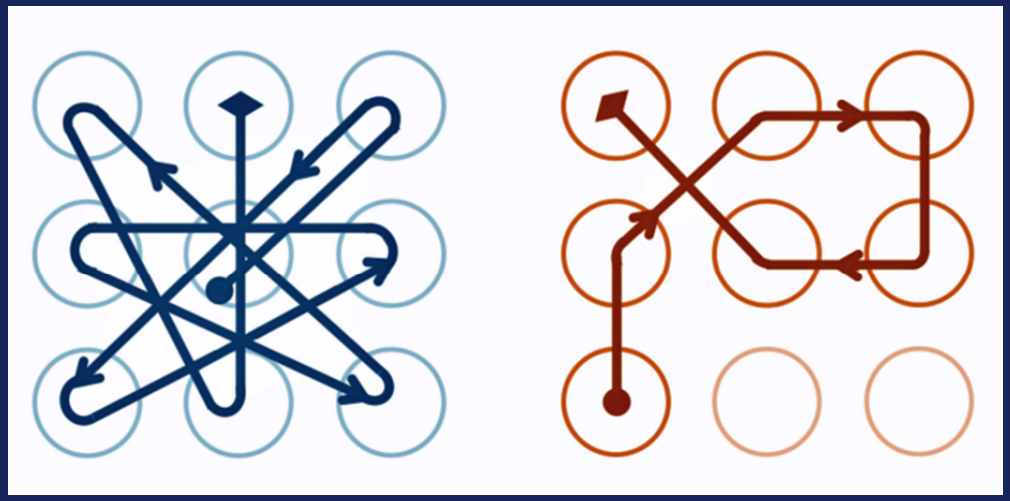
Ein 4-stelliger Pin ist in ~17 Stunden knackbar.

Sperrmuster - Brute-Force

Quelle: youtube.com [28]

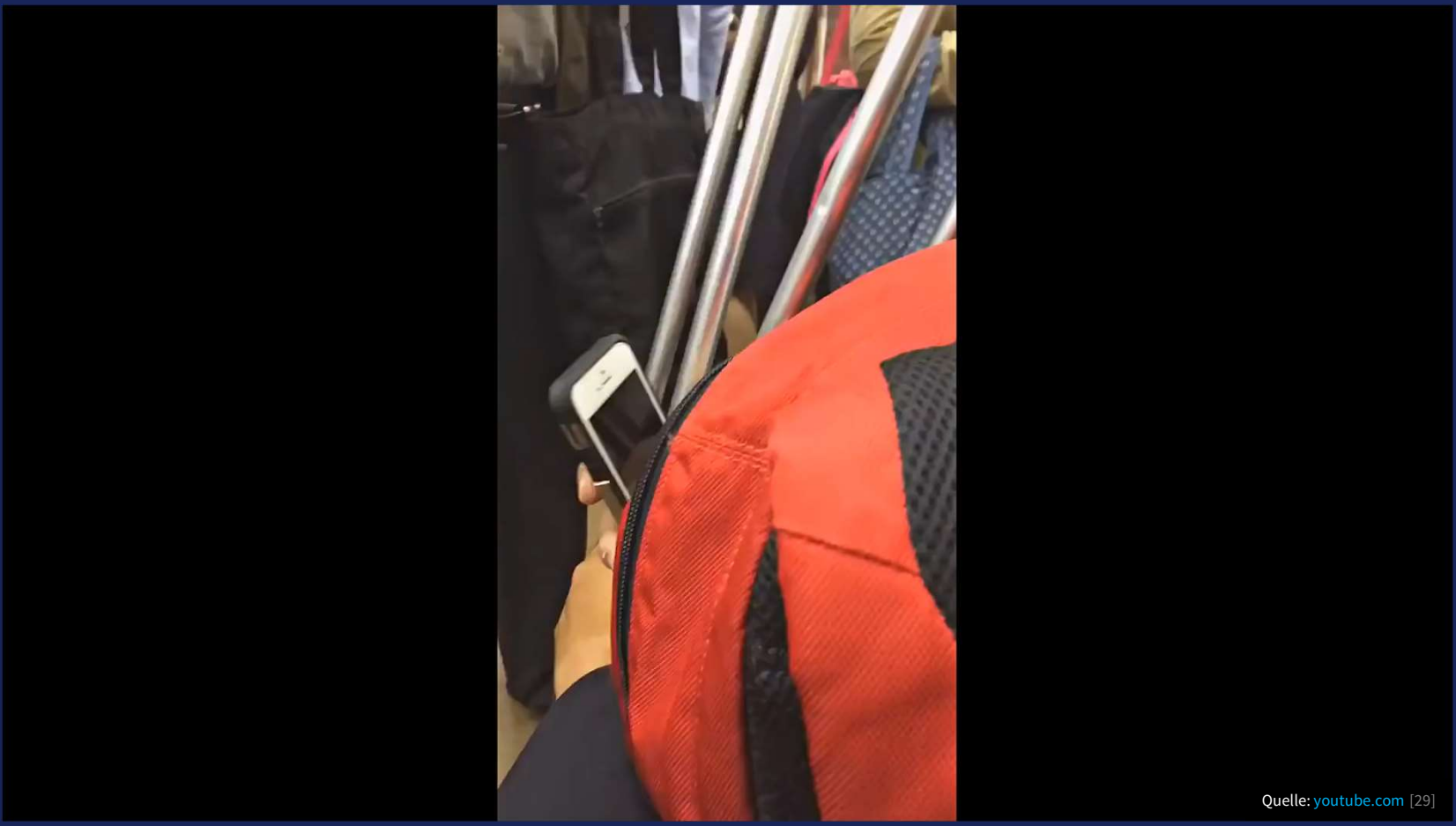
Bad Lock Patterns - Gegenmaßnahmen

- Komplizierte Muster verwenden
- Allerdings sind weitere mögliche Angriffsvektoren vorhanden:
  - Angriffe über ADB (Android Debug Bridge)
- Lange PINs verwenden



Quelle: arstechnica.com [27]

Bad Lock Patterns - Gegenmaßnahmen



Quelle: youtube.com [29]

Passwortkarten

Nr: Kategorie:

	abc	def	ghi	jkl	mno	pqr	stu	vwx	yz	#
1										
2										
3										
4										
5										
6										
7										
8										

Passwortkarten

Nr: 1 Kategorie: Online-Banking

	abc	def	ghi	jkl	mno	pqr	stu	vwx	yz	#
1	x!	Q*	S<	bL	Pn	X:	V=	dd	n3	9K
2	T8	wb	eT	98	C,	6<	ff	aO	X>	Hm
3	Bd	dD	C)	7c	gz	er	q]	p=	t&	1P
4	ne	a@	e-	W8	k-	G2	>d	PE	z3	z:
5	V·	H>	d*	W-	Wl	J8	Qi	U,	ld	7R
6	5=	mF	2n	XY	m:	f<	YH	mo	h4	7-
7	vT	ej	R:	+<	Vg	Nh	a9	6;	dJ	N{
8	d6	G7	p)	ek	pJ	mb	y2	e?	Jm	Rv

Passwortkarten

Link: sparkasse.de Passwort:

Nr: 1 Kategorie: Online-Banking

	abc	def	ghi	jkl	mno	pqr	stu	vwx	yz	#
1	x!	Q*	S<	bL	Pn	X:	V=	dd	n3	9K
2	T8	wb	eT	98	C,	6<	ff	aO	X>	Hm
3	Bd	dD	C)	7c	gz	er	q]	p=	t&	1P
4	ne	a@	e-	W8	k-	G2	>d	PE	z3	z:
5	V·	H>	d*	W-	Wl	J8	Qi	U,	Id	7R
6	5=	mF	2n	XY	m:	f<	YH	mo	h4	7-
7	vT	ej	R:	+<	Vg	Nh	a9	6;	dJ	N{
8	d6	G7	p)	ek	pJ	mb	y2	e?	Jm	Rv

Passwortkarten

Link: sparkasse.de Passwort: V=

Nr: 1 Kategorie: Online-Banking

	abc	def	ghi	jkl	mno	pqr	stu	vwx	yz	#
1	x!	Q*	S<	bL	Pn	X:	V=	dd	n3	9K
2	T8	wb	eT	98	C,	6<	ff	aO	X>	Hm
3	Bd	dD	C)	7c	gz	er	q]	p=	t&	1P
4	ne	a@	e-	W8	k-	G2	>d	PE	z3	z:
5	V·	H>	d*	W-	Wl	J8	Qi	U,	Id	7R
6	5=	mF	2n	XY	m:	f<	YH	mo	h4	7-
7	vT	ej	R:	+<	Vg	Nh	a9	6;	dJ	N{
8	d6	G7	p)	ek	pJ	mb	y2	e?	Jm	Rv

Passwortkarten

Link: sparkasse.de Passwort: V=6<

Nr: 1 Kategorie: Online-Banking

	abc	def	ghi	jkl	mno	pqr	stu	vwx	yz	#
1	x!	Q*	S<	bL	Pn	X:	V=	dd	n3	9K
2	T8	wb	eT	98	C,	6<	ff	aO	X>	Hm
3	Bd	dD	C)	7c	gz	er	q]	p=	t&	1P
4	ne	a@	e-	W8	k-	G2	>d	PE	z3	z:
5	V·	H>	d*	W-	Wl	J8	Qi	U,	Id	7R
6	5=	mF	2n	XY	m:	f<	YH	mo	h4	7-
7	vT	ej	R:	+<	Vg	Nh	a9	6;	dJ	N{
8	d6	G7	p)	ek	pJ	mb	y2	e?	Jm	Rv

Passwortkarten

Link: sparkasse.de

Passwort: V=6<Bd

Nr: 1

Kategorie: Online-Banking

	abc	def	ghi	jkl	mno	pqr	stu	vwx	yz	#
1	x!	Q*	S<	bL	Pn	X:	V=	dd	n3	9K
2	T8	wb	eT	98	C,	6<	ff	aO	X>	Hm
3	Bd	dD	C)	7c	gz	er	q]	p=	t&	1P
4	ne	a@	e-	W8	k-	G2	>d	PE	z3	z:
5	V·	H>	d*	W-	Wl	J8	Qi	U,	Id	7R
6	5=	mF	2n	XY	m:	f<	YH	mo	h4	7-
7	vT	ej	R:	+<	Vg	Nh	a9	6;	dJ	N{
8	d6	G7	p)	ek	pJ	mb	y2	e?	Jm	Rv

Passwortkarten

Link: sparkasse.de Passwort: V=6<BdG2

Nr: 1 Kategorie: Online-Banking

	abc	def	ghi	jkl	mno	pqr	stu	vwx	yz	#
1	x!	Q*	S<	bL	Pn	X:	V=	dd	n3	9K
2	T8	wb	eT	98	C,	6<	ff	aO	X>	Hm
3	Bd	dD	C)	7c	gz	er	q]	p=	t&	1P
4	ne	a@	e-	W8	k-	G2	>d	PE	z3	z:
5	V·	H>	d*	W-	Wl	J8	Qi	U,	ld	7R
6	5=	mF	2n	XY	m:	f<	YH	mo	h4	7-
7	vT	ej	R:	+<	Vg	Nh	a9	6;	dJ	N{
8	d6	G7	p)	ek	pJ	mb	y2	e?	Jm	Rv

Passwortkarten

Link: sparkasse.de Passwort: V=6<BdG2W-

Nr: 1 Kategorie: Online-Banking

	abc	def	ghi	jkl	mno	pqr	stu	vwx	yz	#
1	x!	Q*	S<	bL	Pn	X:	V=	dd	n3	9K
2	T8	wb	eT	98	C,	6<	ff	aO	X>	Hm
3	Bd	dD	C)	7c	gz	er	q]	p=	t&	1P
4	ne	a@	e-	W8	k-	G2	>d	PE	z3	z:
5	V·	H>	d*	W-	Wl	J8	Qi	U,	Id	7R
6	5=	mF	2n	XY	m:	f<	YH	mo	h4	7-
7	vT	ej	R:	+<	Vg	Nh	a9	6;	dJ	N{
8	d6	G7	p)	ek	pJ	mb	y2	e?	Jm	Rv

Fazit Passwortsicherheit

- Die Länge eines Passwortes ist ein entscheidender Faktor. Lange Passwörter sind, pauschal gesagt, sicherer als kurze.
- Das Passwort darf nicht mit Ihrem persönlichen Umfeld in Verbindung stehen.
- Nutzen Sie für jeden Dienst verschiedene Passwörter, damit nach einem Angriff nicht auch andere Accounts von Ihnen betroffen sind.
- Nutzen Sie einen Passwortmanager, um die unterschiedlichen Passwörter sicher zu speichern.
- Nutzen Sie überall, wo es geht, eine Zwei-Faktor-Authentifizierung.

Hacking Hardware

Gadgets – Spionage Kamera

Gadgets – GSM Wanze

Logger - Keylogger

Logger - Screenlogger

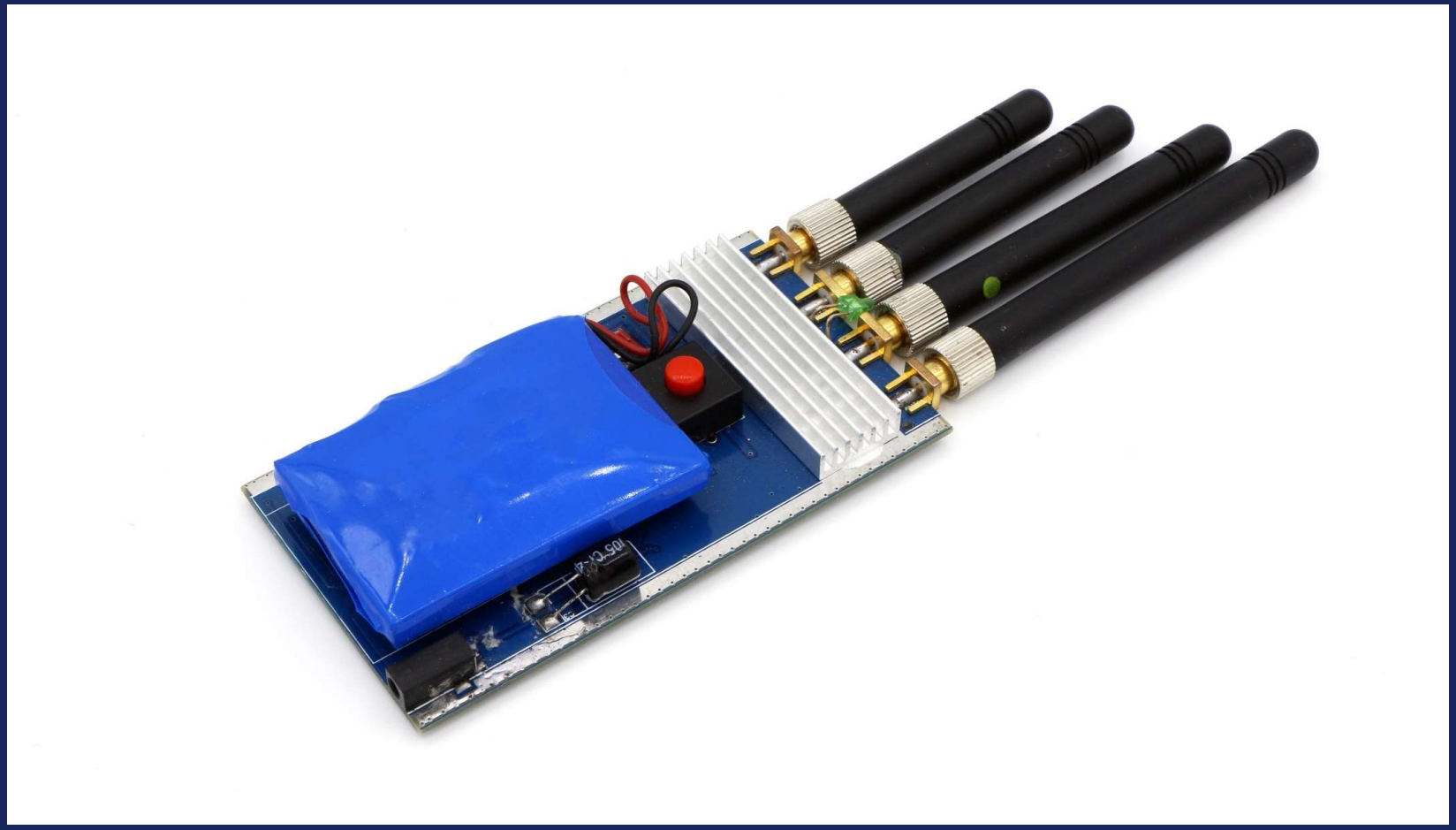
USB – BadUSB (Rubber Ducky)

IT Security – anonym und sicher im Netz

USB – BadUSB (USBNinja)

USB - USBKill

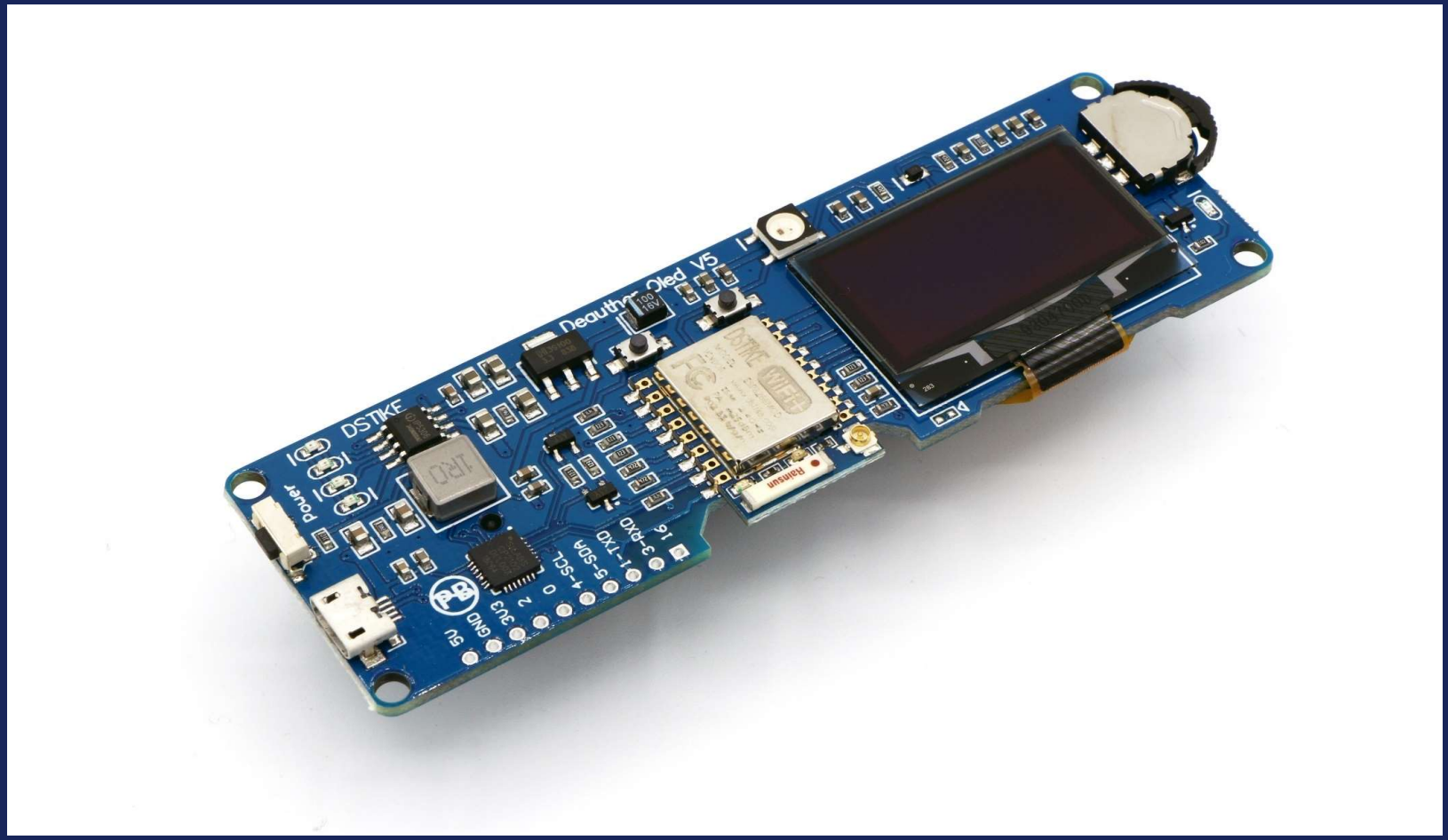
Funk - Störsender



Funk - Software Defined Radio

IT Security – anonym und sicher im Netz

Netzwerk – WiFi Deauther



IT Security – anonym und sicher im Netz

Netzwerk - Packet-Squirrel

IT Security – anonym und sicher im Netz

Vielen Dank für Ihre Aufmerksamkeit

Präsentation demnächst online unter: https://scheible.it

Quellen

(1) https://www.gdata.de/ratgeber/was-ist-eigentlich-die-geschichte-der-malware, abgerufen am 23.07.2019

(2) https://de.wikipedia.org/wiki/AIDS_(Schadprogramm) , abgerufen am 23.07.2019

(3) https://www.youtube.com/watch?v=5M9k7wfiWiI , abgerufen am 23.07.2019

(4) https://de.wikipedia.org/wiki/Locky , abgerufen am 23.07.2019

(5) https://haveibeenpwned.com , abgerufen am 23.07.2019

(6) https://securityaffairs.co/wordpress/53871/iot/deutsche-telekom-hack.html , abgerufen am 23.07.2019

(7) https://www.computerworld.com/article/3105001/security/hackers-demonstrated-first-ransomware-for-iot-thermostats-at-def-con.html , abgerufen am 23.07.2019

(8) http://www.shop.ledermode.tv/ , abgerufen am 23.07.2019

(9) http://metapicz.com/ , abgerufen am 23.07.2019

(10) http://google.de/ , abgerufen am 23.07.2019

(11) https://www.exploit-db.com/google-hacking-database , abgerufen am 23.07.2019

(12) http://www.heise.de/security/meldung/IP-Kameras-von-Aldi-als-Sicherheits-GAU-3069735.html , abgerufen am 23.07.2019

(13) https://shodan.io/ , abgerufen am 23.07.2019

(14) https://www.youtube.com/watch?v=WvRL5I1eU3E , abgerufen am 23.07.2019

(15) http://www.spiegel.de/schulspiegel/schulfrei-in-niedersachsen-wegen-gefaelschter-e-mail-a-1071105.html , abgerufen am 23.07.2019

(16) http://www.heise.de/newsticker/meldung/Gefaengnisausbruch-mittels-E-Mail-Betrug-2587303.html , abgerufen am 23.07.2019

(17) https://www.wiwo.de/erfolg/management/falsche-chefs-zocken-firmen-ab-den-enkeltrick-gibts-auch-bei-unternehmen/12201572.html , abgerufen am 23.07.2019

(18) http://clonezone.link/

Quellen

(19) http://www.heise.de/security/meldung/00000000-Passwort-fuer-US-Atomraketen-2060077.html , abgerufen am 23.07.2019

(20) http://pics-for-fun.com/wonder-what-the-code-could-be/ , abgerufen am 23.07.2019

(21) https://de.pinterest.com/pin/3025924727584002/ , abgerufen am 23.07.2019

(22) https://www.youtube.com/watch?v=opRMrEfAIiI , abgerufen am 23.07.2019

(23) http:\www.heise.de\newsticker\meldung\Passwoerter-im-TV-Bild-Spekulationen-zu-TV5-Attacke-2598298.html , abgerufen am 23.07.2019

(24) https://www.vice.com/en_us/article/qvwmx5/the-agency-that-messed-up-hawaiis-nuclear-alert-keeps-passwords-on-post-its-vgtrn , abgerufen am 23.07.2019

(25) https://github.com/morontt/symfobrute/blob/master/adobe-top100.txt , abgerufen am 23.07.2019

(26) https://xkcd.com/936/ , abgerufen am 23.07.2019

(27) https://arstechnica.com/information-technology/2015/08/new-data-uncovers-the-surprising-predictability-of-android-lock-patterns/ , abgerufen am 23.07.2019

(28) https://www.youtube.com/watch?v=WFaFL4mAzpQ , abgerufen am 23.07.2019

(29) https://www.youtube.com/watch?v=RybQ3EBmkfM , abgerufen am 23.07.2019