Hochschule
Albstadt-Sigmaringen
University of Applied Sciences

Fakultät Informatik

Cyber Security
Angreifer & Bedrohungen verstehen
Wintertagung 2019 - LBB

Tobias Scheible, M.Eng.

Tobias Scheible, M.Eng.

- 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
  - Bachelorstudiengang IT Security
  - Institut für Wissenschaftliche Weiterbildung

Praktikum Cybersecurity
IT Security (Bachelor) – 4. Semester
Prof. Holger Morgenstern

Seminar Cybersecurity
IT Security (Bachelor) – 4. Semester
Prof. Holger Morgenstern

Digitale Forensik
IT Security (Bachelor) – 5. Semester
Prof. Holger Morgenstern

Projektstudium
IT Security (Bachelor) – 5. Semester
Prof. Holger Morgenstern

Grundlagen Digitale Forensik
IT GRC Management – 4. Semester
Prof. Dr. Stefan Ruf

Workshops & Vorträge
LKA, VDI, IHK, Sparkasse, …
Online veröffentlicht: https://scheible.it

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)

Cyber Security
Angreifer & Bedrohungen verstehen

Fakultät Informatik

Bachelorstudiengänge

+ IT Security
+ Technische Informatik
+ Wirtschaftsinformatik

Masterstudiengänge

+ Business Analytics
+ Systems Engineering

Weiterbildungsangebote

+ Studium Initiale
+ Hochschulzertifikate
+ Data Science
+ Digitale Forensik
+ IT GRC Management

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

Cyber Security
Angreifer & Bedrohungen verstehen

Zahlen & Fakten

167
Lehrbe-
auftragte

201
Mitarbeiter

134
Mitarbeiter
Studiengänge

67
Verwaltung
und zentrale
Einrichtungen

57 %
Campus
Albstadt

43 %
Campus
Sigmaringen

3.374
Studierende

184
Studentische
Hilfskräfte

87
Professoren /
Professorinnen

Hochschule
Albstadt-Sigmaringen
University of Applied Sciences

Fakultät Informatik

Cyber Security
Angreifer & Bedrohungen verstehen

Agenda

- Cyber Security
  - Schadsoftware
  - Aktuelle Vorfälle
  - Bug or Feature?
  - Suchmaschinen
  - Internet of Things
  - Cybercrime as a Service
- Social Engineering
  - Faktor Mensch
  - Website manipulieren
  - CEO Fraud
- Passwortsicherheit
  - Öffentliche Passwörter
  - Angriffe auf Passwörter
  - Sperrmuster
  - Sichere Passwörter
- Hardware Hacks
  - Probe Requests Scanner
  - Hardware Tools
  - BadUSB
- Zukünftige Entwicklung


Cyber Security

00000000

?

Quelle: heise.de (1)

00000000

Launch-Code für die in den USA stationierten Atomraketen

(1962 bis 1977)

Quelle: heise.de (1)

Atomraketen: Steuerungstechnik aus den 70ern

Quelle: zeit.de (2)

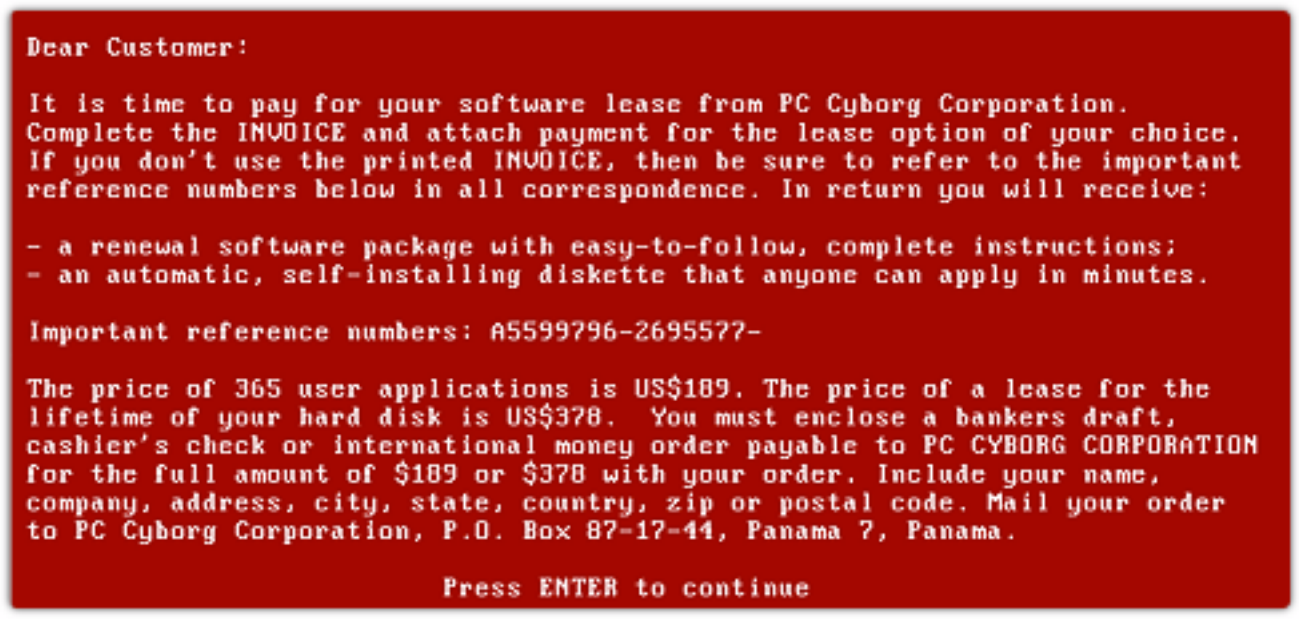
Geschichte der Schadsoftware

- 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 (3)

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 (4)

Aktuelle Vorfälle - Doxing

8. Januar 2019, 12:22 Uhr Private Daten im Netz

Doxing - eine alte Hacker-Waffe trifft den deutschen Mainstream

Im Unterschied zum investigativen Journalismus oder Whistleblowing, ist die Intension beim Doxing, eine Person bloßzustellen oder einzuschüchtern. (Foto: imago/photothek)

Feedback

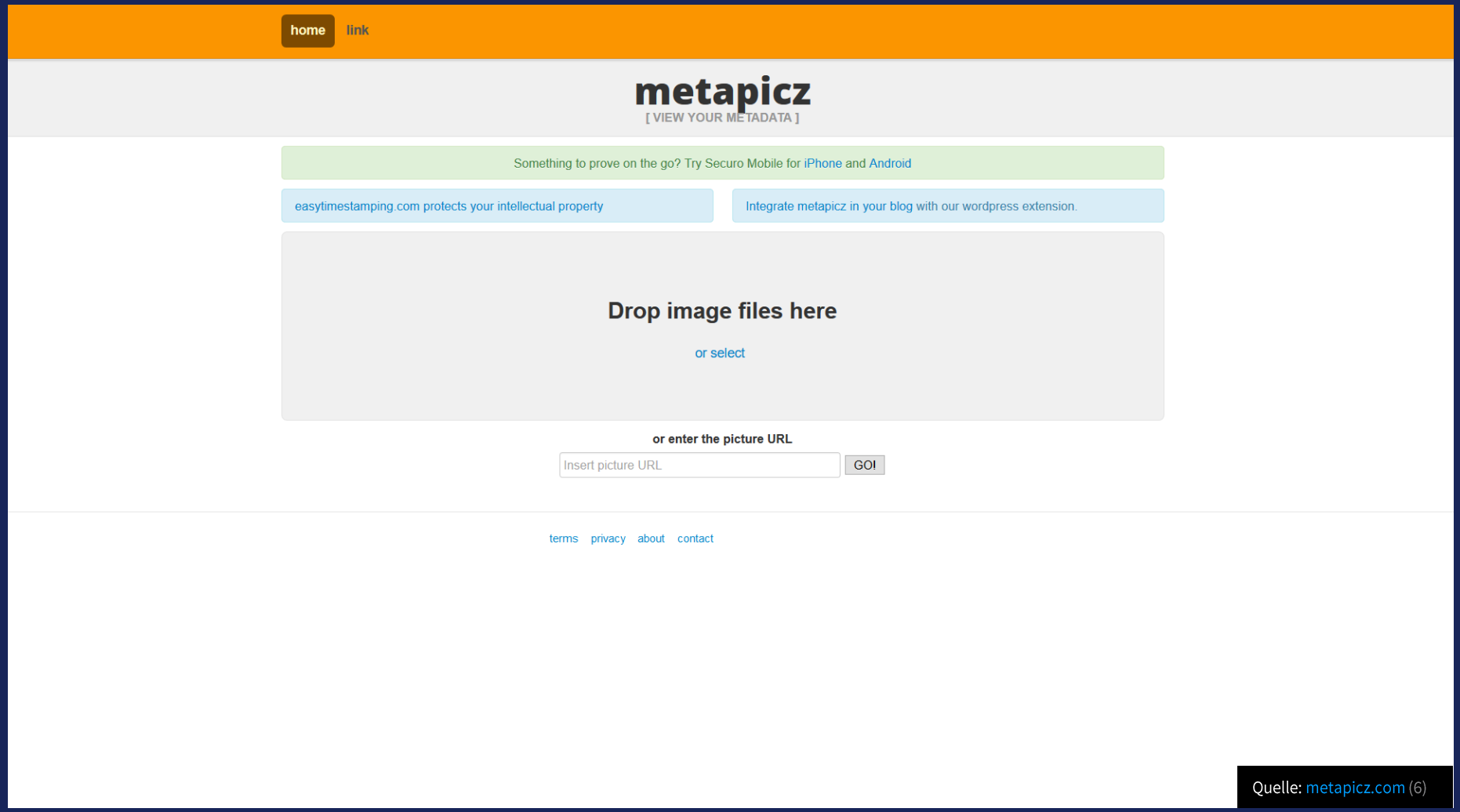
Schon in den Neunzigern nutzen Hacker die Entblößung ihrer Kontrahenten im Netz als digitalen Flammenwerfer. Heute wird damit schmutzig Politik gemacht.

Von Jannis Brühl

Für Schattenkrieger ist das Wichtigste, dass niemand ihr Gesicht und ihren Namen kennt. Deshalb fürchteten Hacker schon in den Neunzigern das, was die Szene später Doxing taufen sollte: Eine Person veröffentlicht strategisch eine

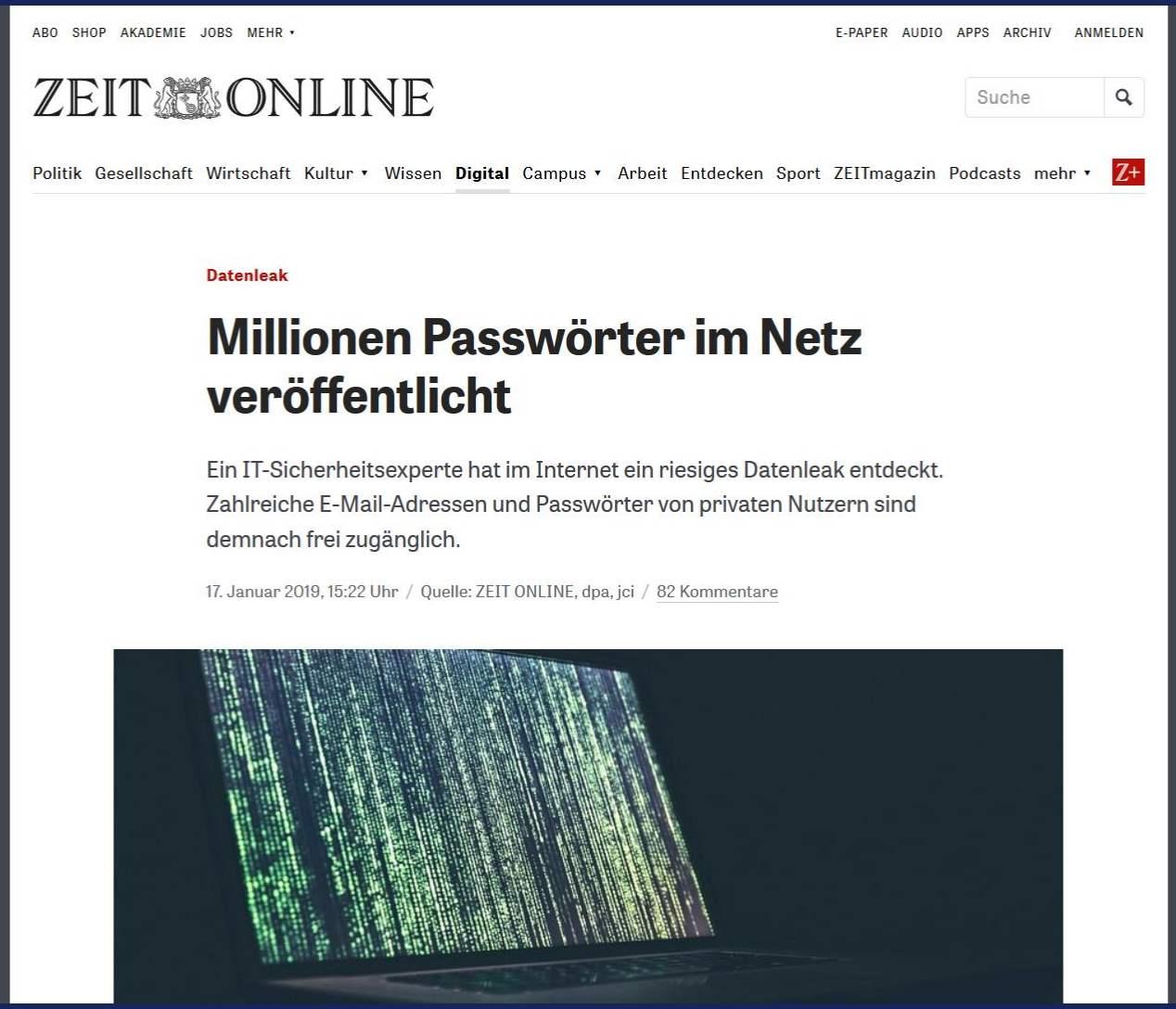
Quelle: sueddeutsche.de (5)

DEMO Versteckte Informationen auslesen



Quelle: metapicz.com (6)

Aktuelle Vorfälle – Data Leaks



ABO SHOP AKADEMIE JOBS MEHR ▾ E-PAPER AUDIO APPS ARCHIV ANMELDEN

ZEIT ONLINE

Suche

Politik Gesellschaft Wirtschaft Kultur ▾ Wissen **Digital** Campus ▾ Arbeit Entdecken Sport ZEITmagazin Podcasts mehr ▾ Z+

Datenleak

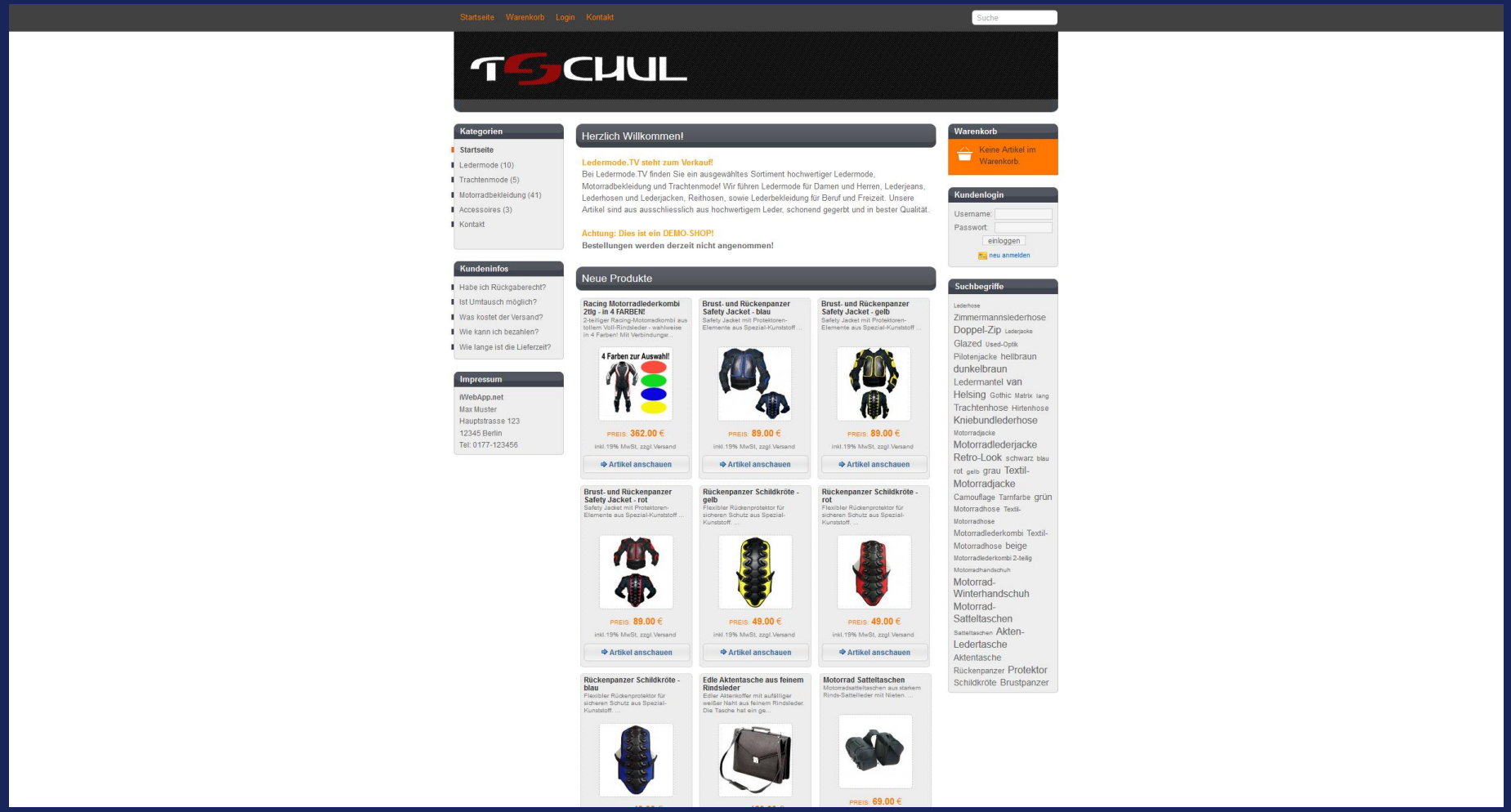
Millionen Passwörter im Netz veröffentlicht

Ein IT-Sicherheitsexperte hat im Internet ein riesiges Datenleak entdeckt. Zahlreiche E-Mail-Adressen und Passwörter von privaten Nutzern sind demnach frei zugänglich.

17. Januar 2019, 15:22 Uhr / Quelle: ZEIT ONLINE, dpa, jci / 82 Kommentare

Quelle: zeit.de (7)

DEMO Bug or Feature?



Quelle: ledermode.tv (8)

Suchmaschinen - Hacking mit Google

Quelle: google.de (9)

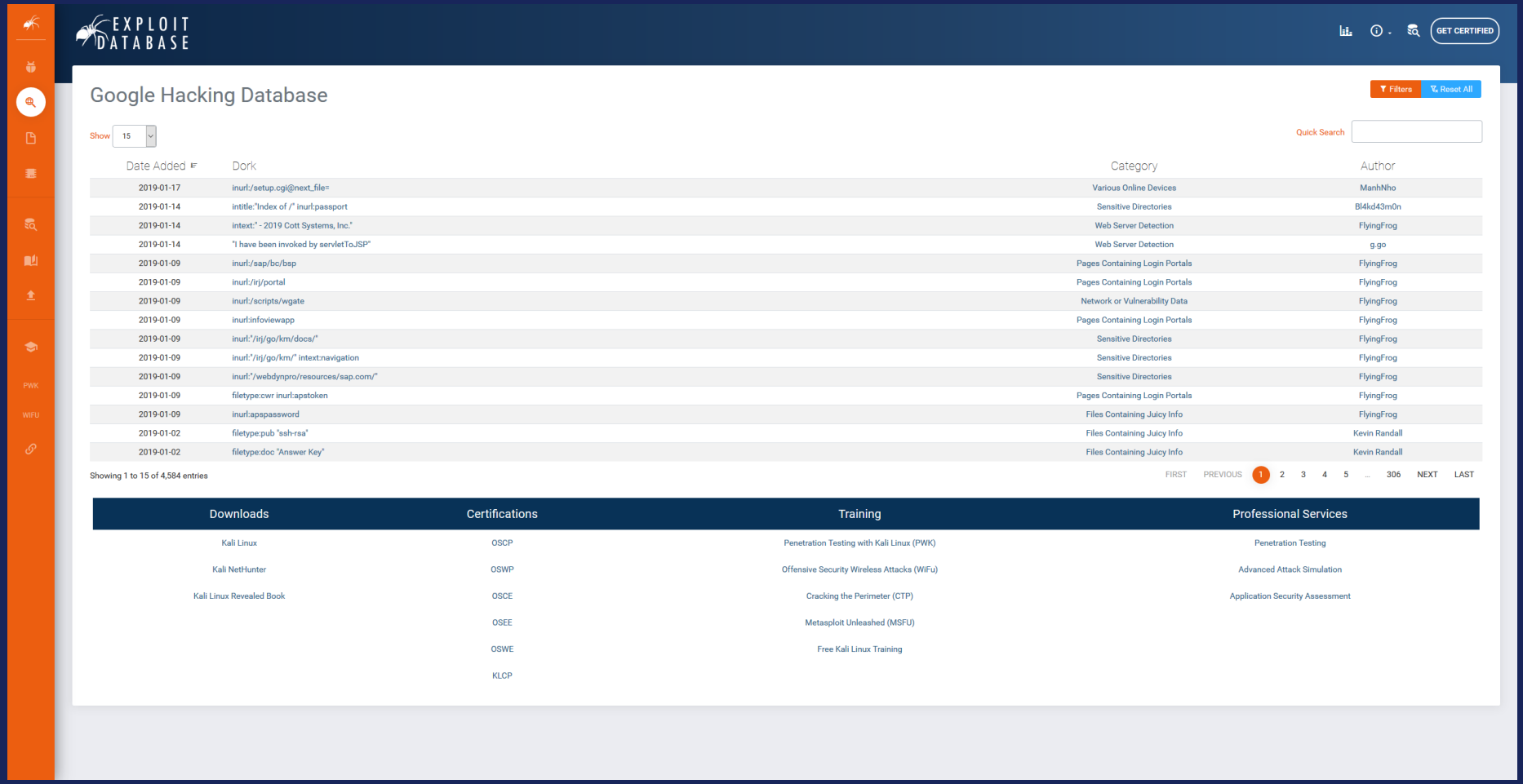
Suchmaschinen - Hacking mit Google

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 Suchbegriff liefert Ergebnisse von Webseiten, deren Titel diesen Suchbegriff enthält. Beispiel: *intitle:"it security"*
inurl:	Eine Suche mit dem Suchparameter "inurl:" in Verbindung mit einem Suchbegriff liefert Ergebnisse von Webseiten, deren URL den Suchbegriff enthalten. 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"*

DEMO Suchmaschinen - 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"

Suchmaschinen - GHDB



Quelle: exploit-db.com (10)

IoT - Bug or Feature?

heise online

Anmelden Suchen Menü

IT Mobiles Entertainment Wissen Netzpolitik Wirtschaft Journal Newsticker Foren

TOPTHEMEN: CES 2019 DSGVO WINDOWS 10 ANDROID AMAZON KI ANZEIGE: CLOUD SERVICES ZUKUNFTSMACHER

Security 〉7-Tage-News 〉01/2016 〉IP-Kameras von Aldi mit massiven Sicherheitslücken

Alert! 15.01.2016 10:49 Uhr | Security

IP-Kameras von Aldi als Sicherheits-GAU

Aldi hatte vergangenes Jahr mehrfach IP-Überwachungskameras mit denkbar schlechten Voreinstellungen verkauft. Die Geräte sind zu Hunderten fast ungeschützt über das Internet erreichbar.

Von Ronald Eikenberg 411

Die bei Aldi verkauften IP-Überwachungskameras der Marke Maginon haben massive Sicherheitsprobleme: Unbefugte könnten über das Internet auf das Kamerabild zugreifen und sogar den Ton anzapfen. Zudem verraten die Geräte unter anderem die Passwörter für WLAN, E-Mail und FTP-Zugang ihres Besitzers. Hunderte Aldi-Kameras sind nahezu ungeschützt über das Internet erreichbar. Darauf hat uns der Zusammenschluss Digitale Gesellschaft aufmerksam gemacht.

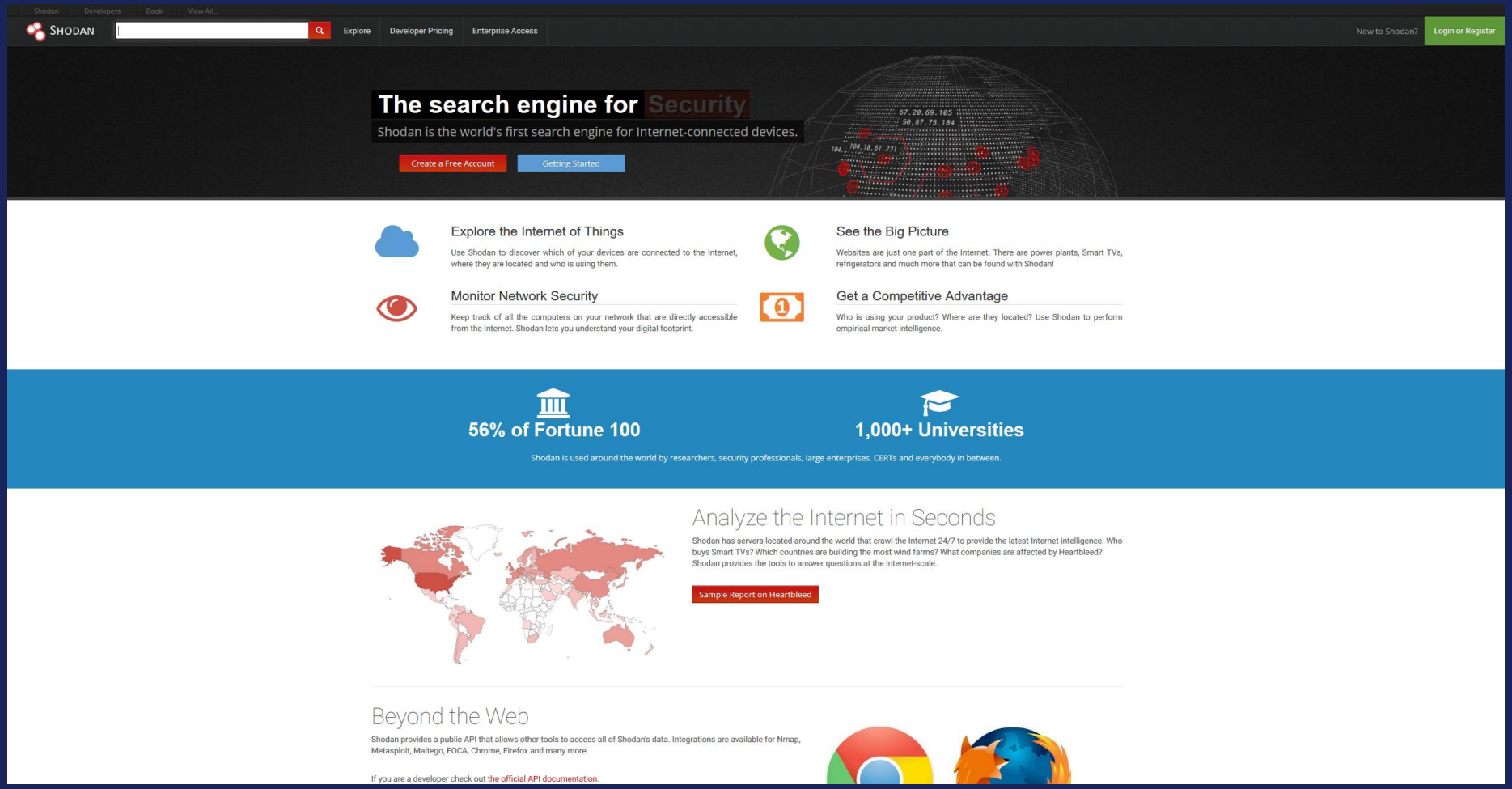
Betroffen ist unter anderem die Außenkamera IPC-20 C. (Bild: Hersteller)

Drei Modelle sind betroffen

Die Kameras IPC-10 AC, IPC-100 AC und IPC-20 C hat Aldi mit einer Firmware

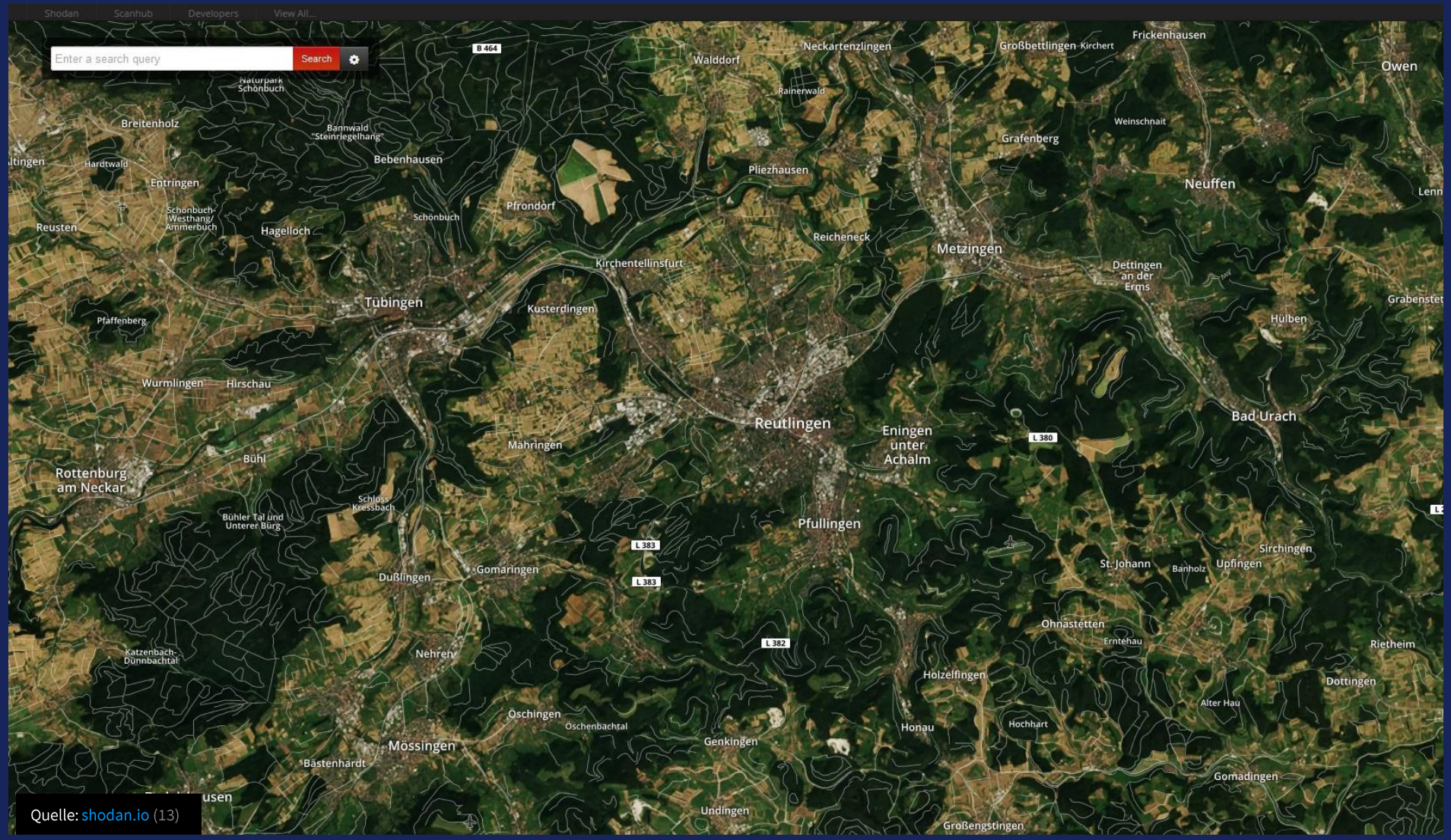
Quelle: heise.de (11)

IoT - Suchmaschine für das Internet der Dinge



Quelle: shodan.io (12)

DEMO IoT - Webcams mit Shodan finden



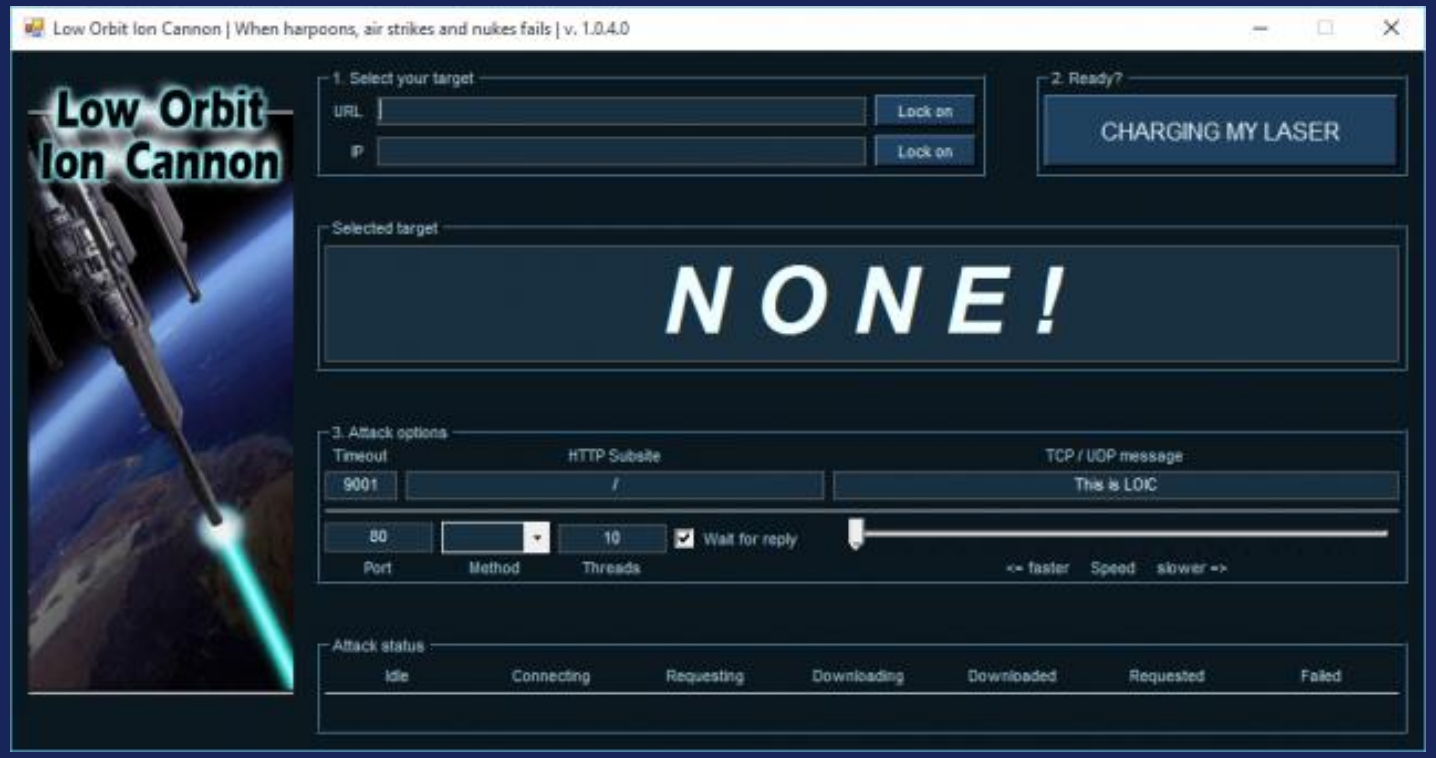
Quelle: shodan.io (13)

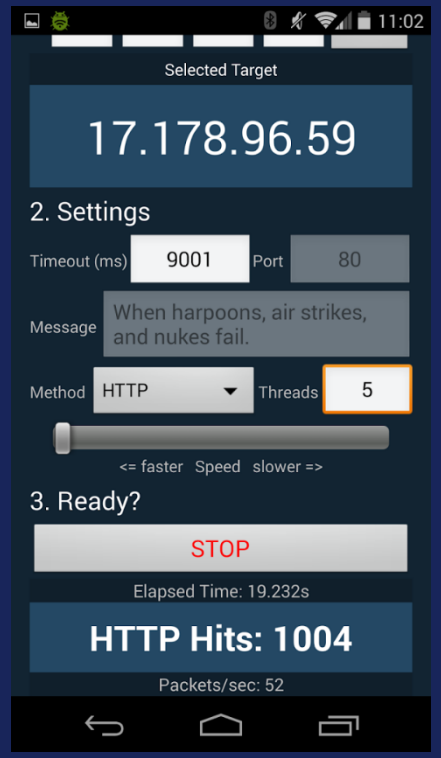
Hochschule Albstadt-Sigmaringen
University of Applied Sciences

Fakultät Informatik

Cyber Security
Angreifer & Bedrohungen verstehen

Cybercrime as a Service - Hackaktivisten





Quelle: wikipedia.org (14)

Quelle: 1mobile.com (15)

Cybercrime as a Service

Quelle: youtube.com (16)

Cybercrime as a Service

Cybercrime as a Service - 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 (17)

FAZIT Cyber Security

- Geräte oder Anwendungen, die im Internet sind, können nicht durch komplizierte Links oder weil die Adresse nirgendwo steht, geschützt werden.
- Die Standard-Passwörter von Geräten, die mit dem Internet verbunden sind, müssen immer geändert werden.
- Komponenten können sich auch selbstständig mit dem Internet verbinden, daher muss die Konfiguration immer geprüft werden.

Social Engineering

Was ist die häufigste Angriffsmethode?

Ausnutzung von Schwachstellen

A

Physische Attacken

B

Manipulation von Personen

C

Ausnutzung von Fehlern

D

Faktor Mensch - 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 (18)

Faktor Mensch - Beispiel

Quelle: youtube.com (19)

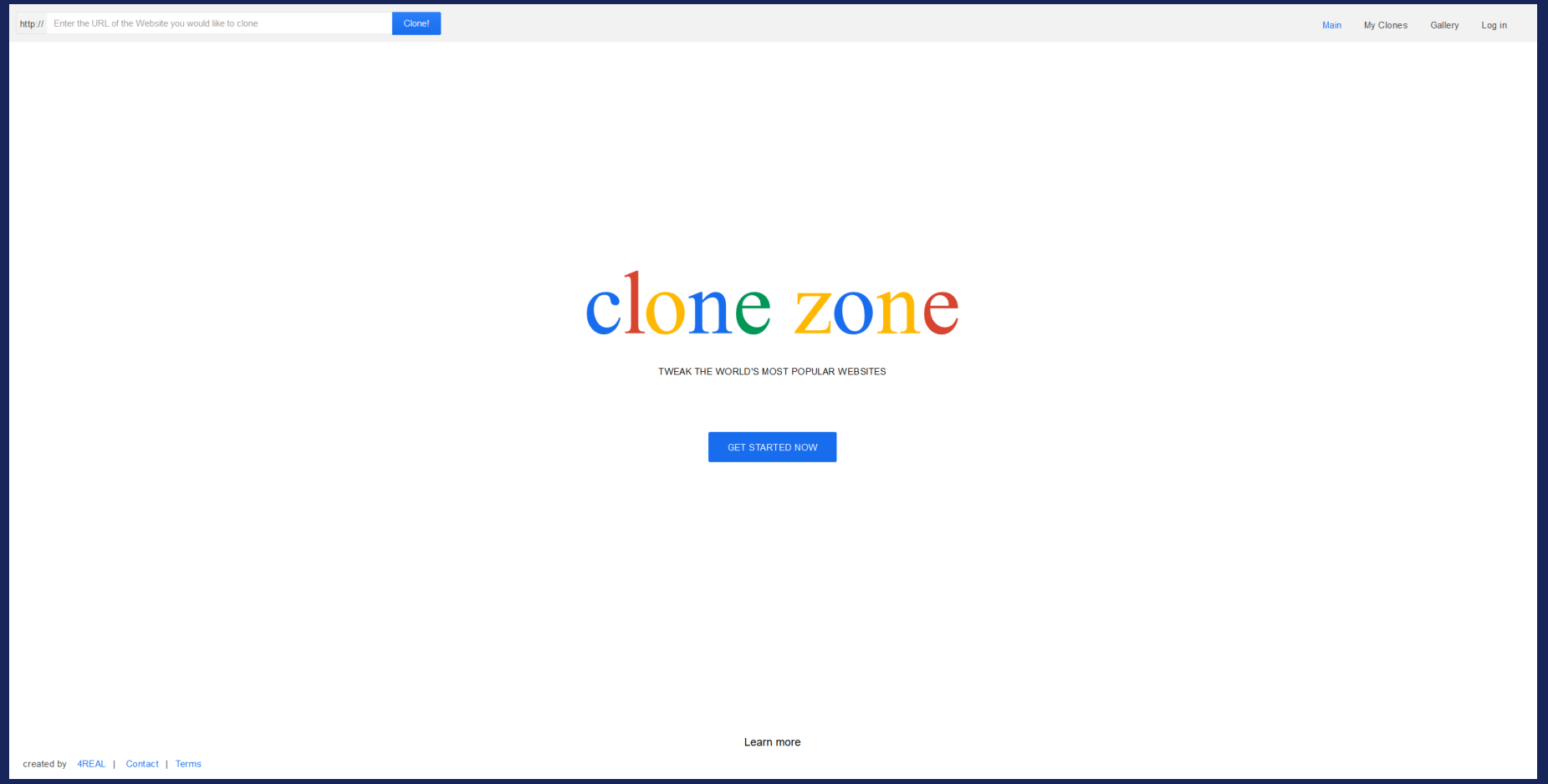
Social Engineering - Gefängnisausbruch

- 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

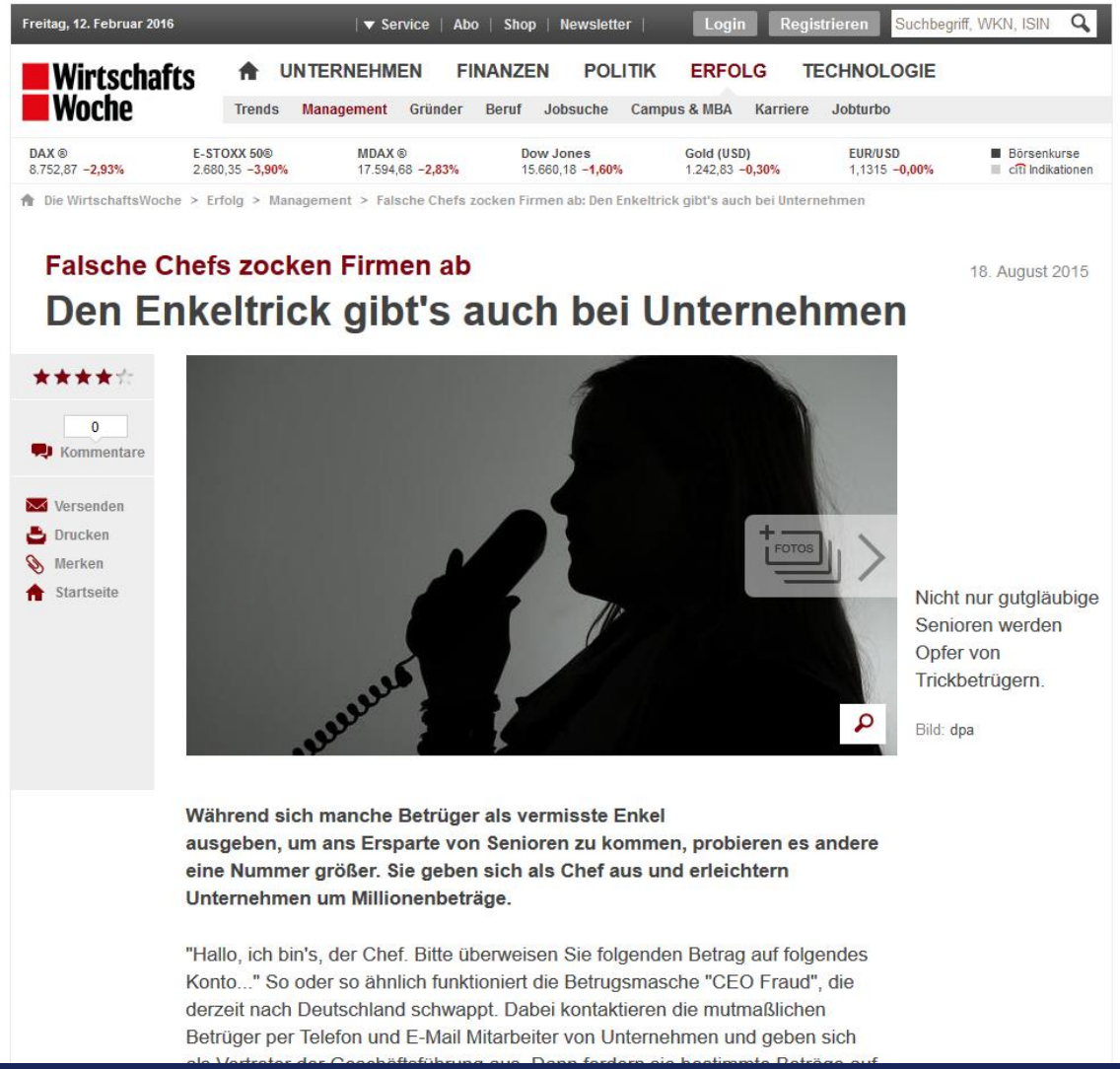
Quelle: heise.de (20)

DEMO Website manipulieren



Quelle: clonezone.link (21)

CEO Fraud



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 ®	E-STOXX 50®	MDAX ®	Dow Jones	Gold (USD)	EUR/USD	Börsenkurse
8.752,87 −2,93%	2.680,35 −3,90%	17.594,68 −2,83%	15.660,18 −1,60%	1.242,83 −0,30%	1,1315 −0,00%	cm 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 (22)

CEO Fraud - Beispiel

Von: Gustav.Geschäftsführer@firma.de <Gustav.Geschäftsführer@firma-gmbh.de>

An: Otto Opfer

Sehr geehrter Herr Opfer!

Sind Sie im Moment verfügbar?

Hochachtungsvoll

Gustav Geschäftsführer

Quelle: LKA Präsentation, Bedrohungslage Cybercrime, Albstadt 21.1.2016, S. 21

CEO Fraud - Beispiel

..wir führen momentan eine finanzielle Transaktion durch, bei der es um eine Unternehmensübernahme in Asien geht.

Diese Übernahme **muss streng vertraulich behandelt werden**. Sie sind als einziger Ansprechpartner damit betraut worden, diesen Vorgang auszuführen und Zahlungen vorzunehmen (Alle Informationslecks oder die Nichteinhaltung des unten genannten Verfahrens können zu **Vertragsstrafen und Sanktionen** gegen unsere Firmen führen).

Die öffentliche Bekanntgabe der Übernahme wird am 15.09.2015 in unseren Räumlichkeiten in Anwesenheit des gesamten Managements stattfinden.

Sie finden diesbezüglich einen von der BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht) erteilten Zahlungsauftrag.

Bitte nehmen Sie zur Einreichung der Bankdaten zur sofortigen Ausführung der Zahlung umgehend Kontakt mit unserem französischen **Berater B. Berater** auf (Dieser interveniert zwischen BaFin und AMF, um unsere Interessen zu verteidigen).

Quelle: LKA Präsentation, Bedrohungslage Cybercrime, Albstadt 21.1.2016, S. 20

CEO Fraud - Beispiel

Bitte **vermeiden Sie in persönlichen wie in telefonischen Gesprächen jegliche Anspielung auf diesen Vorgang**. Nutzen Sie **ausschließlich** den E-Mail-Verkehr mit Herrn B. (Berater), der Ihr einziger Ansprechpartner für diesen Vorgang sein wird.

Kontaktdaten von Herrn **B. Berater.: B.Berater@berater-firma.com**

Sobald Sie die Bankdaten erhalten, führen Sie bitte die Zahlung gemäß der beigefügten Zahlungsanweisung auf eine Weise aus, **die Sie alleine vornehmen können**.

Ich bitte Sie auch, Herrn B. einen Zahlungsbeleg zuzusenden, sobald er zur Verfügung steht.

Ich möchte, dass Sie bei diesem Vorgang **der einzige Gesprächspartner und Ausführende innerhalb unseres Unternehmens sind**.

Vielen Dank für Ihr zügiges Vorgehen. Die Finanztransaktion läuft.

Quelle: LKA Präsentation, Bedrohungslage Cybercrime, Albstadt 21.1.2016, S. 21

CEO Fraud - Beispiel

Von: Gustav.Geschäftsführer@firma.de <Gustav.Geschäftsführer@firma-gmbh.de>

An: Otto Opfer

Konnten Sie das Nötige erledigen?

Hochachtungsvoll

Gustav Geschäftsführer

Quelle: LKA Präsentation, Bedrohungslage Cybercrime, Albstadt 21.1.2016, S. 21

CEO Fraud - Beispiel

Dear Mr Opfer,

Mr G. (Geschäftsführer) just sent me the document signed by him and Mr Z. (2. Genehmiger).

Unfortunately I need to provide to BaFin a Specimen of signature (for security reason) from them, can you please send to me an example of signature of Mr G. and Mr Z. on a document older than today ?

Thank you.

Best regards

B. Berater

BaFin /AMF Consultant

Quelle: LKA Präsentation, Bedrohungslage Cybercrime, Albstadt 21.1.2016, S. 22

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.
- Sensibilisieren der Mitarbeiter und Schulung der Mitarbeiter über Social Engineering-Strategien und –Methoden, regelmäßiger Hinweis auf die Bedeutung der Datenweitergabe.
- Schriftliche Festlegungen, welche Informationen vertraulich behandelt werden müssen, Festlegungen zur Form von Anfragen und Datenweitergabe und Vier-Augen-Prinzip.
- Tipp: Auf einem anderen Kanal nachfragen, ob es wirklich stimmt.

Passwortsicherheit

Öffentliche Passwörter

Quelle: pics-for-fun.com (23)

Quelle: : de.pinterest.com (24)

Öffentliche Passwörter - Interview

Quelle: youtube.com (25)

Angriff auf den Fernsehsender TV5Monde

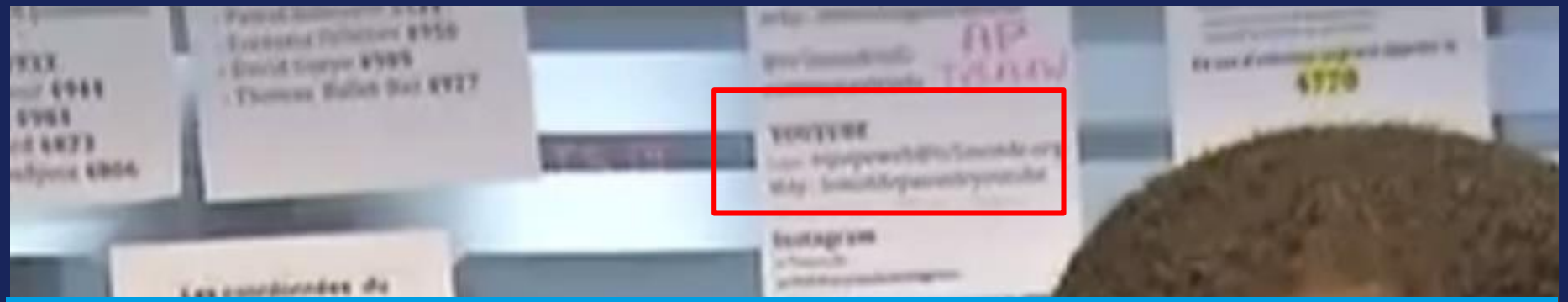
- Umfangreicher Angriff auf den französischen Sender TV5Monde
  - Alle Kanäle des Fernsehunternehmens TV5Monde gingen offline
  - Die Website verbreitete kurzfristig islamistische Drohungen
  - Auf der Facebook-Seite wurden ebenfalls Drohungen verbreitet
  - Spekulationen über öffentlich einsehbare Passwörter

Quelle: heise.de (26)

Faktor Mensch - Angriff auf TV5 Monde

Quelle: heise.de (26)

Faktor Mensch - Angriff auf TV5 Monde



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

Quelle: heise.de (26)

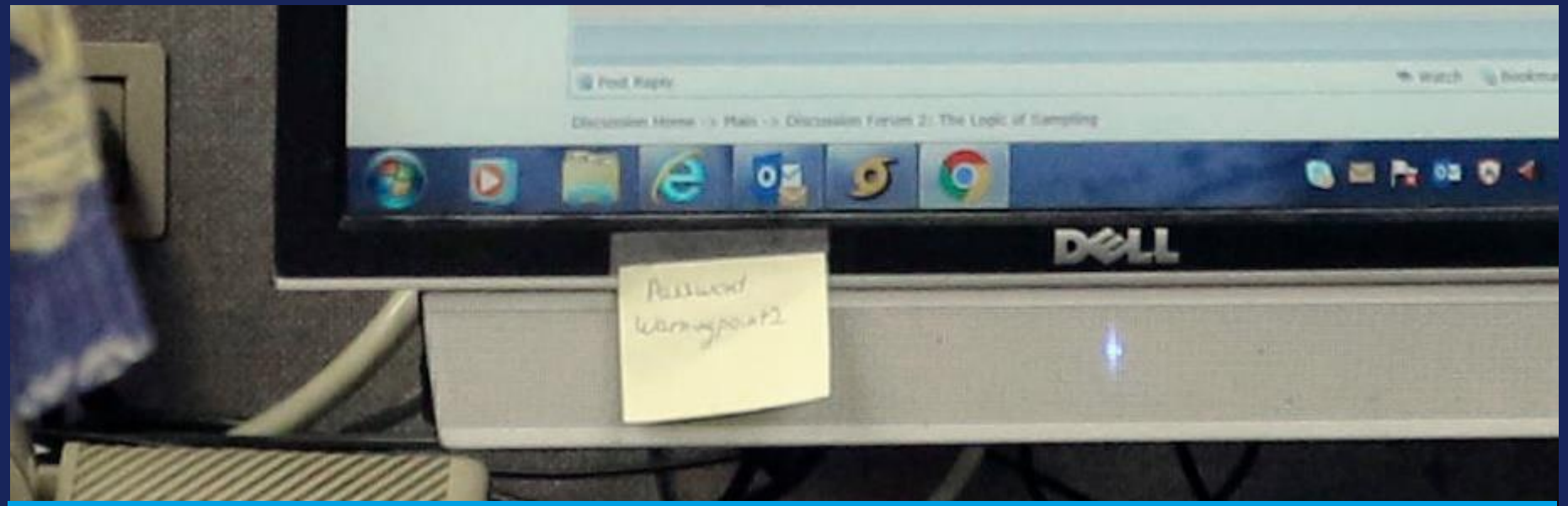
Faktor Mensch

Quelle: vice.com (27)

Hochschule
Albstadt-Sigmaringen
University of Applied Sciences

Fakultät Informatik

Faktor Mensch



Klassiker – Post-it Zettel auf Monitor

Passwort: warningpoint2

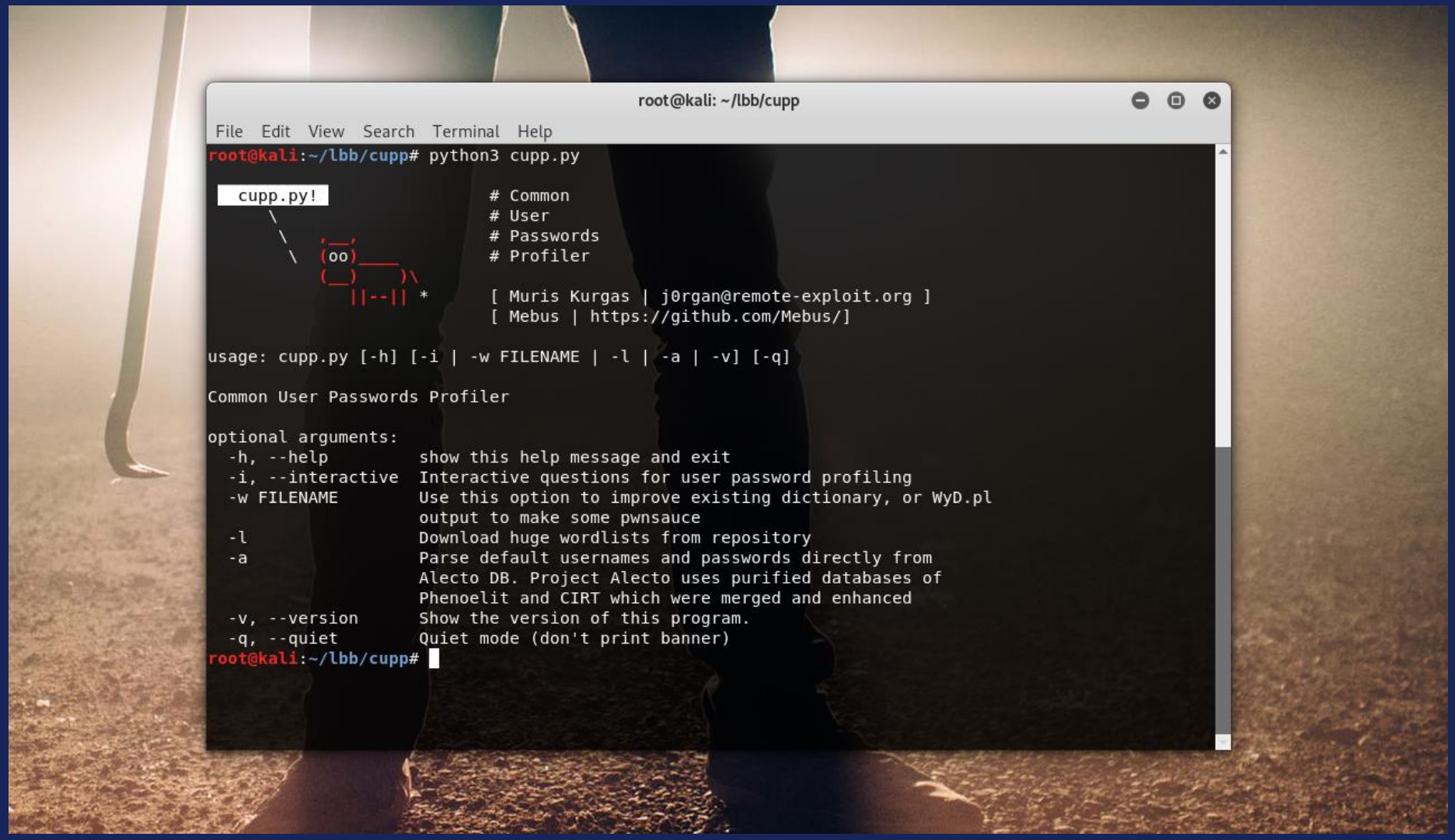
Quelle: vice.com (27)

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.

DEMO Passwörter erraten – Generator



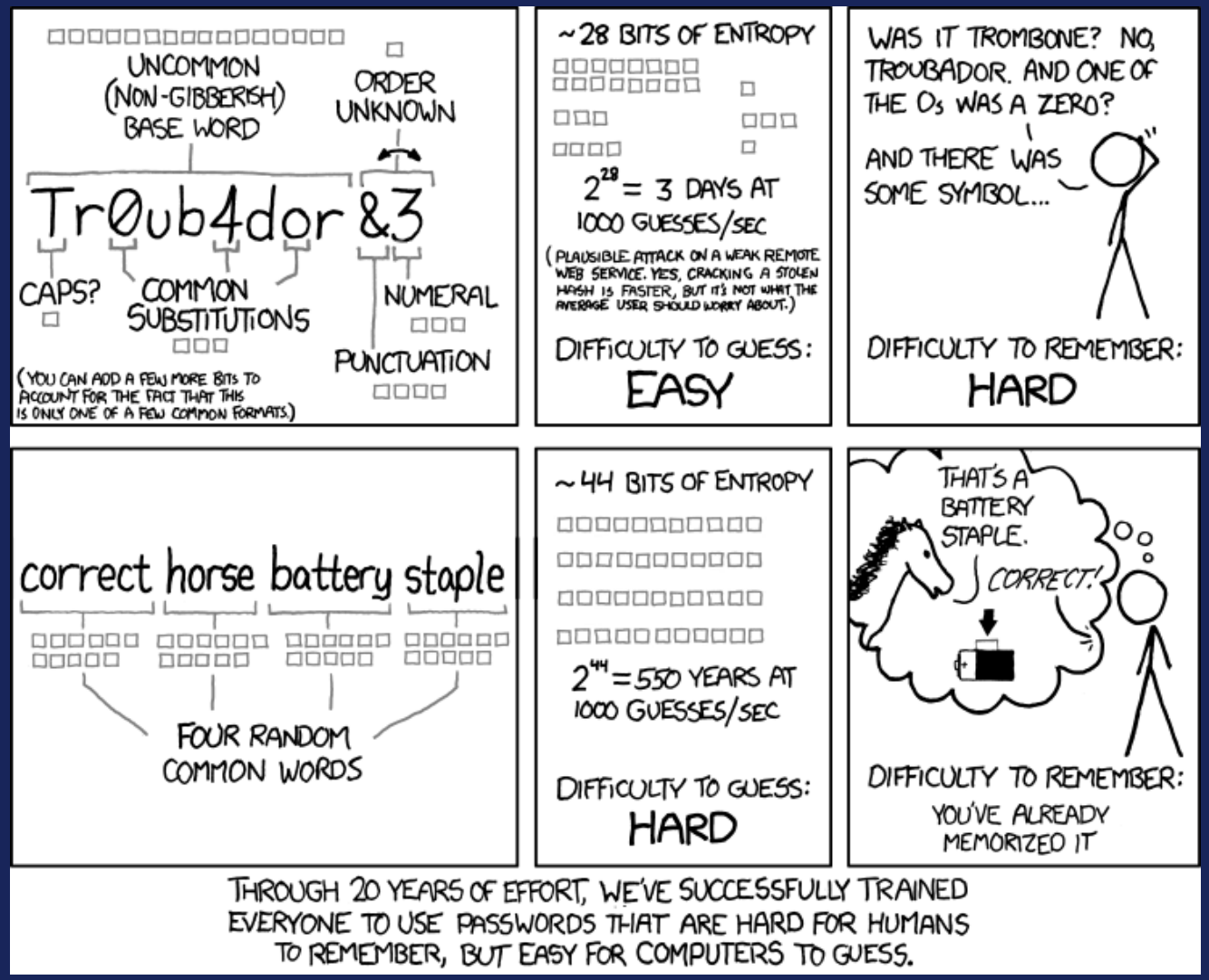
Brute-Force Methode

- 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

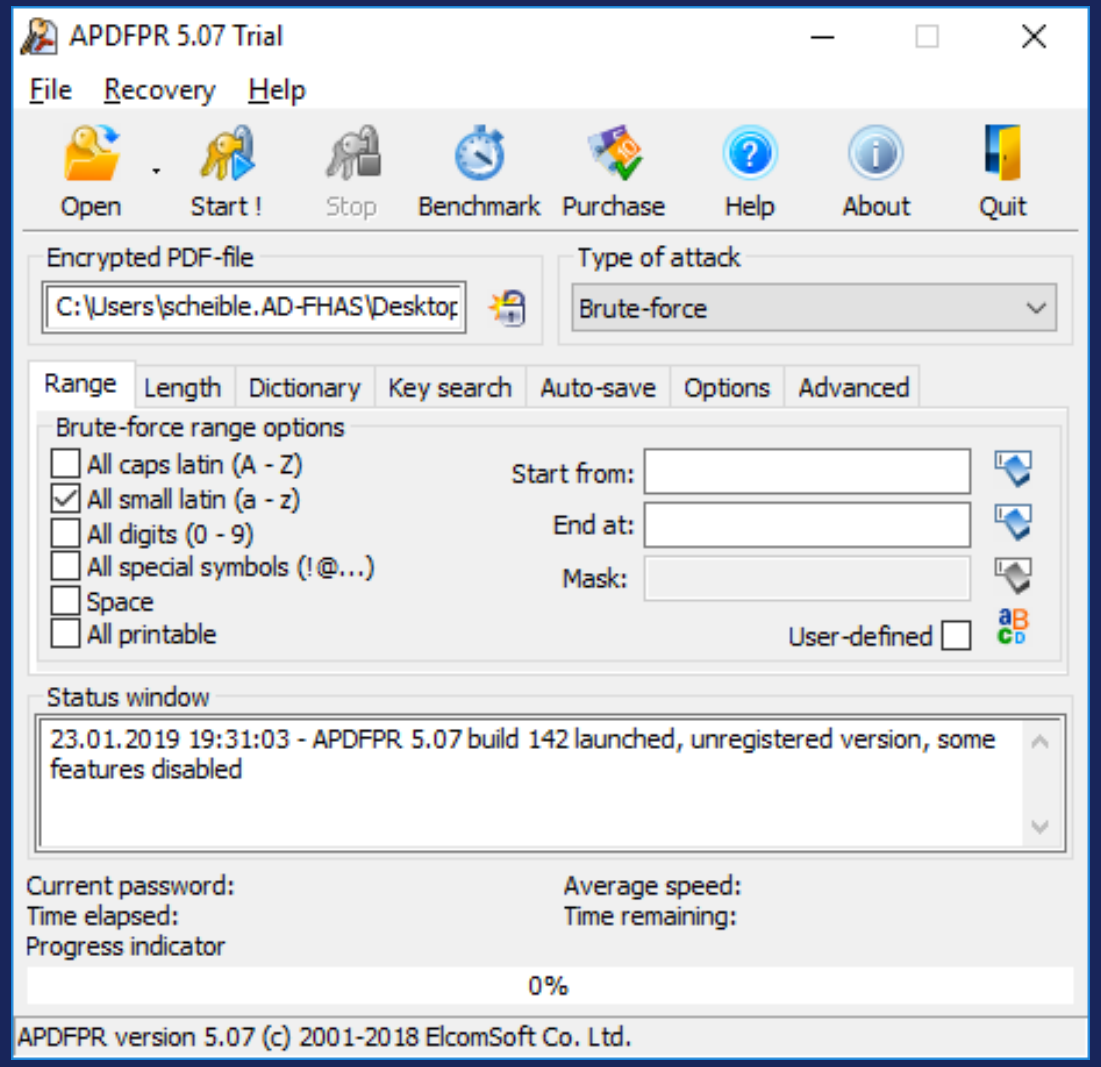
- Komplexität von Passwörtern: Zeichenanzahl $^{\text{Passwortlänge}}$ = Kombinationen
  - Zeichenanzahl
    - Alphabet = 26 Zeichen
      - Mit Groß- und Kleinschreibung = 52 Zeichen
      - Mit den Umlauten = 59 Zeichen
    - Zahlen = 10 Zeichen
    - Sonderzeichen = 32 Zeichen
    - 101 verschiedene 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 (28)

DEMO Brute-Force Methode



Bekannte Passwörter

124 lines (115 sloc) | 6.67 KB

Raw Blame History

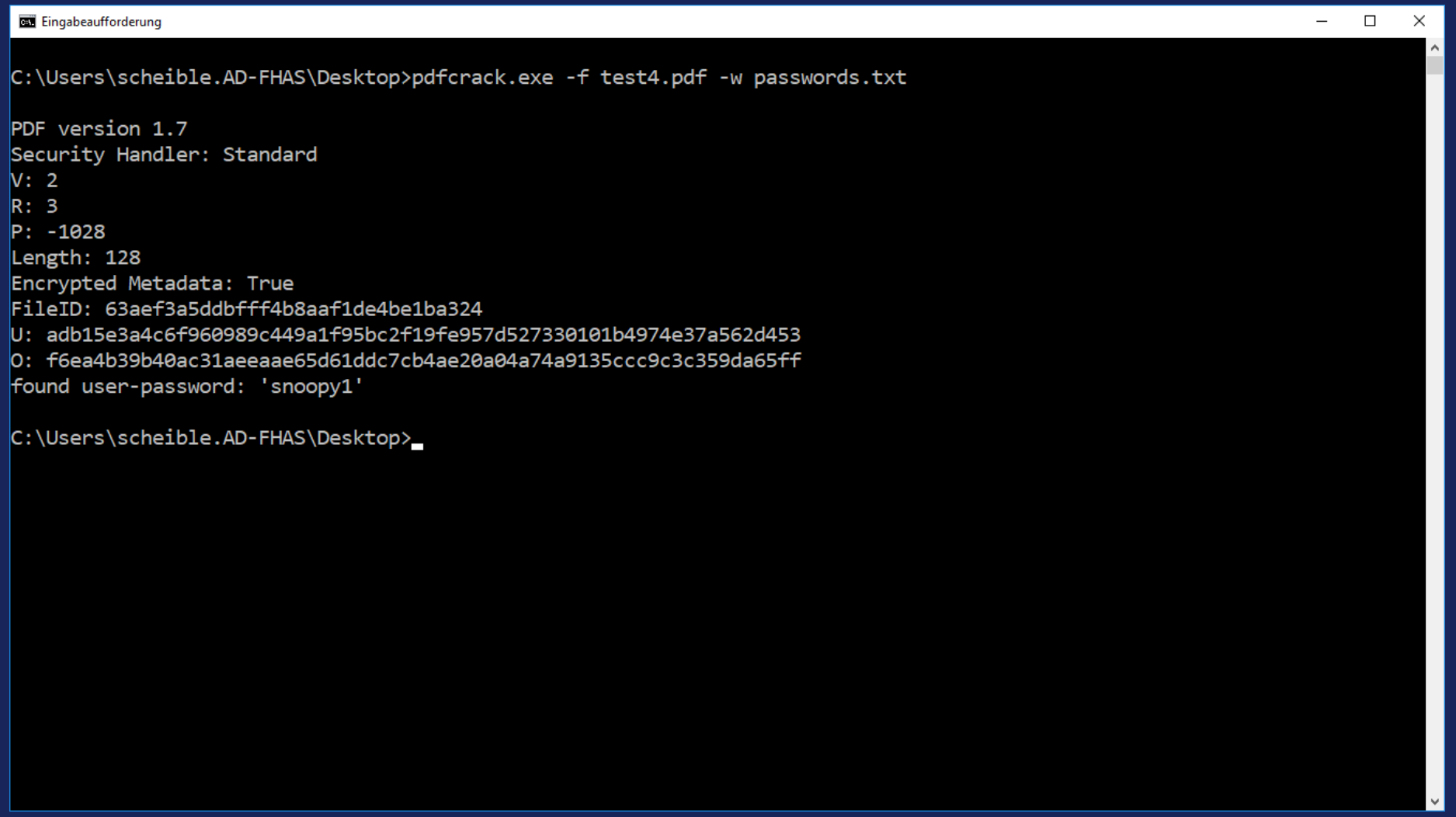
```
Top 100 Adobe Passwords with Count

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.
```

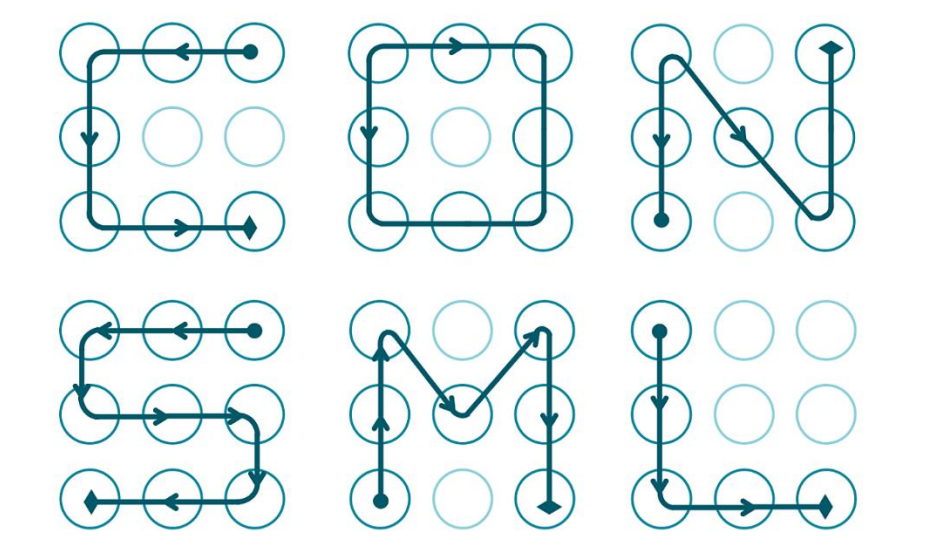
Quelle: github.com (29)

DEMO Bekannte Passwörter



Sperrmuster

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



Quelle: arstechnica.com (30)

Sperrmuster vs. PIN

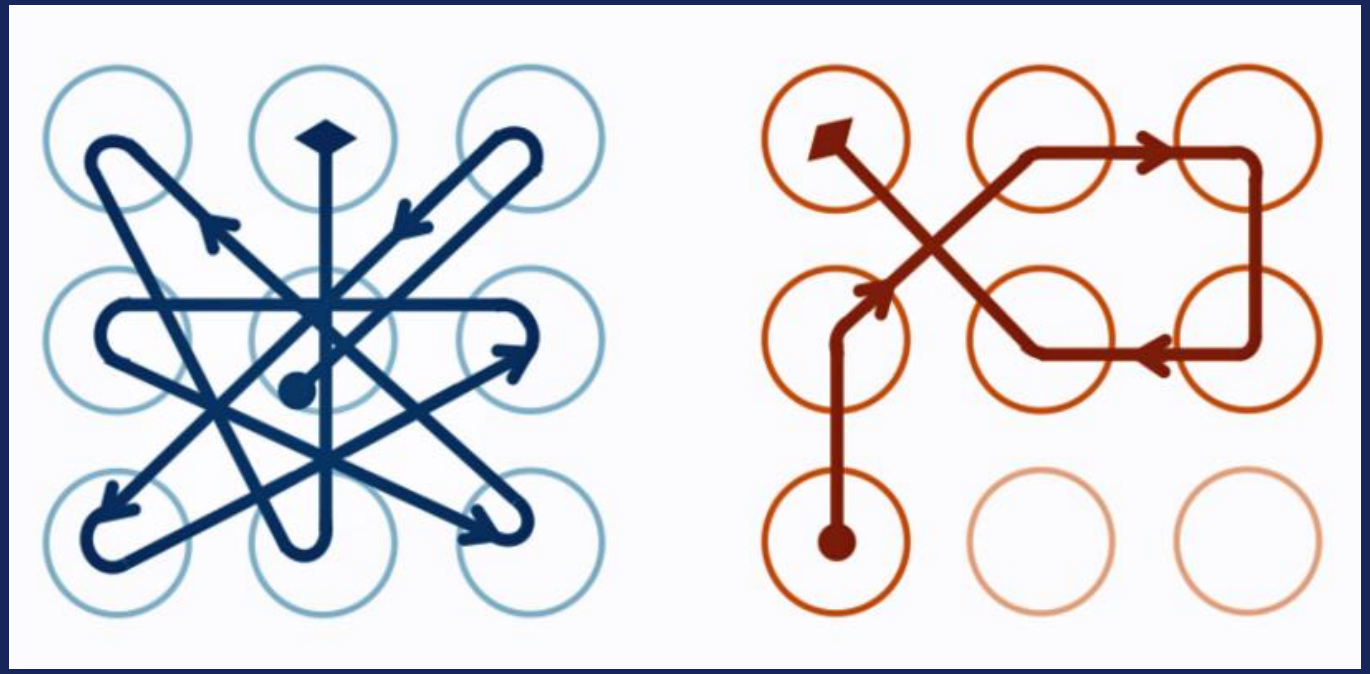
Länge	Wischmuster Kombinationen	PIN Kombinationen
4	1624	10^4 = 10000
5	7152	10^5 = 100000
6	26016	10^6 = 1000000
7	72912	10^7 = 10000000
8	140704	10^8 = 100000000
9	140704	10^9 = 1000000000

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.

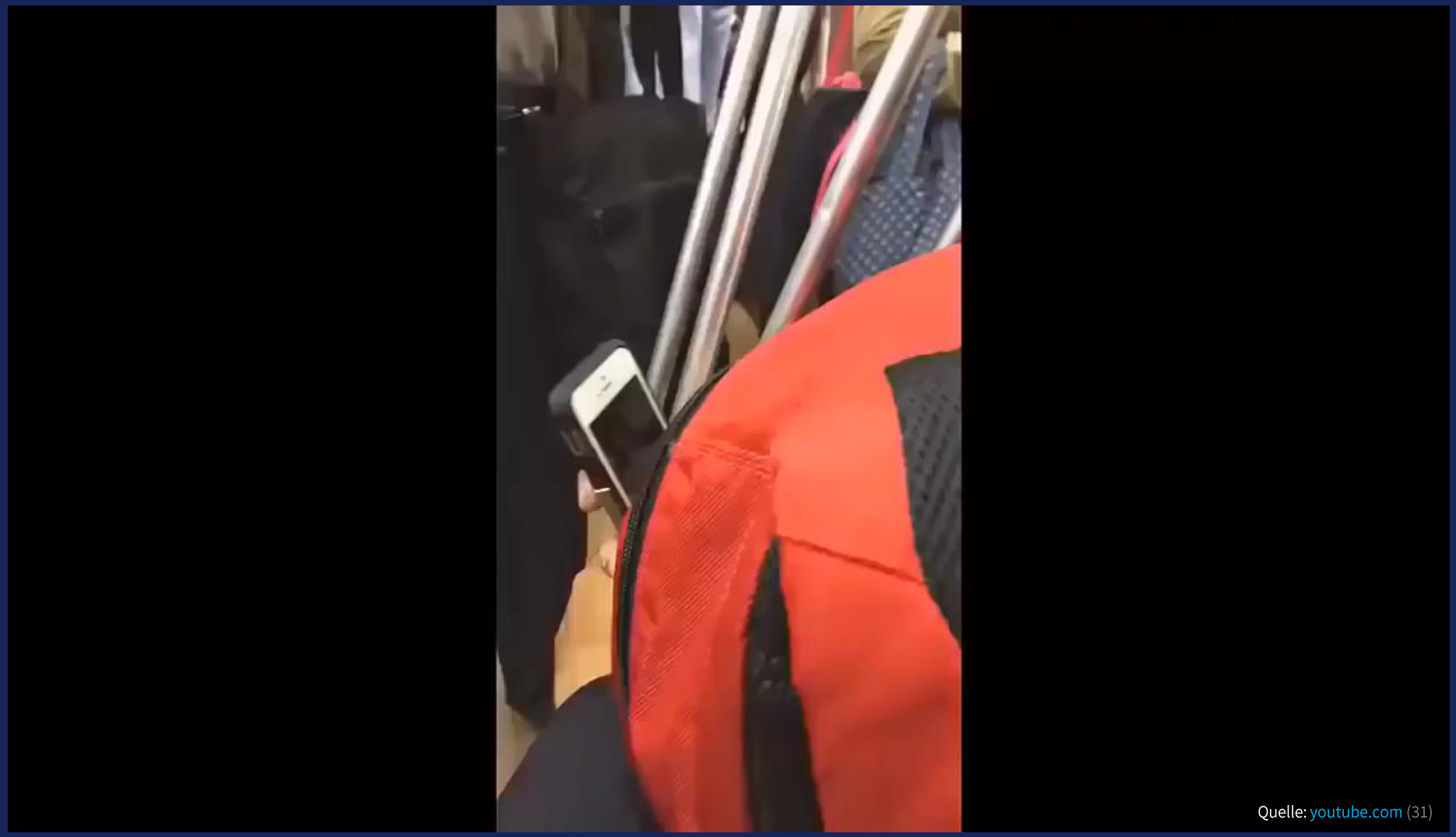
Sperrmuster- Gegenmaßnahmen

- Komplizierte Muster verwenden
- Lange PINs, besser Passwörter verwenden



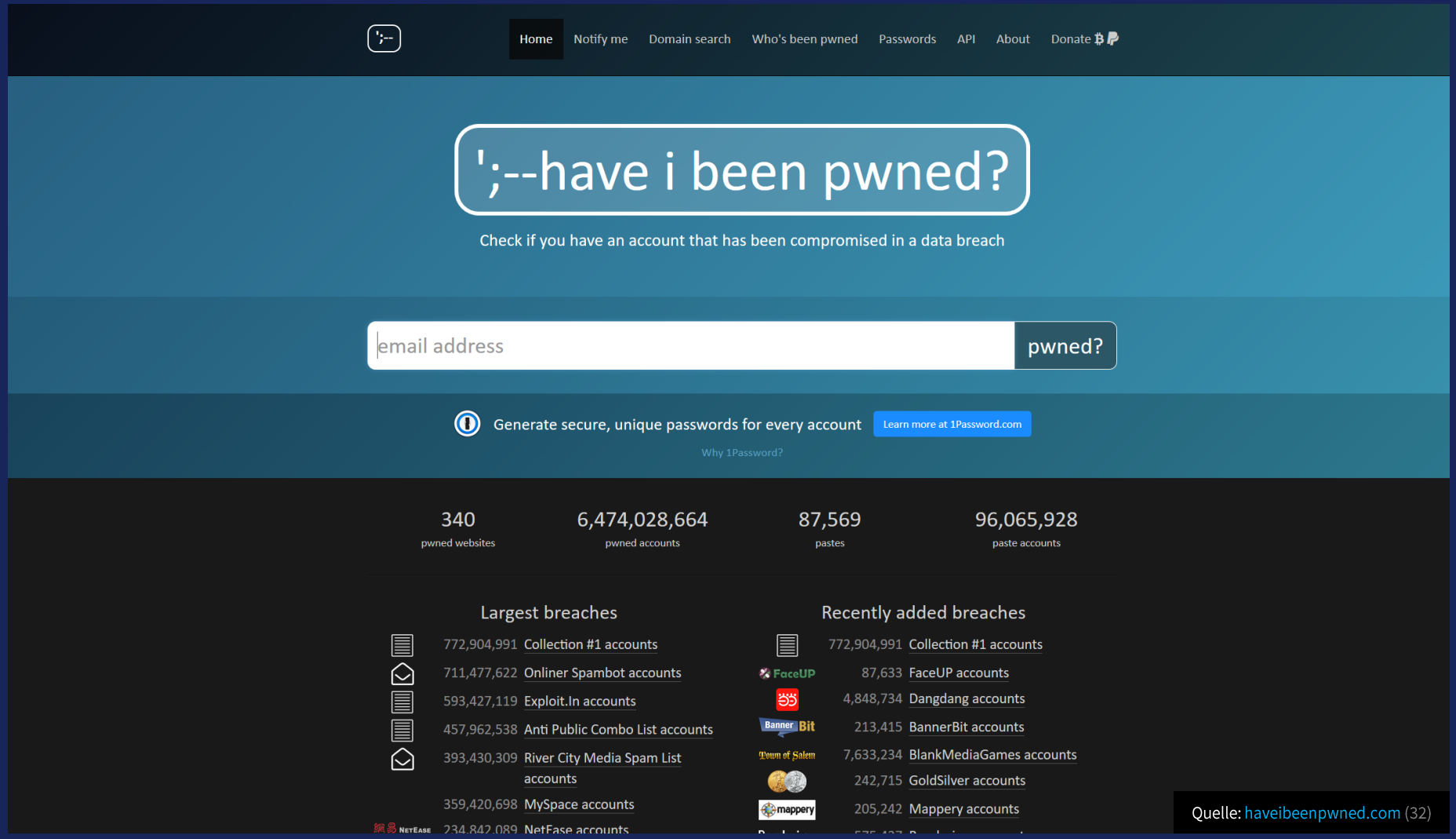
Quelle: arstechnica.com (30)

Sperrmuster – Pin Beispiel



Quelle: youtube.com (31)

DEMO Sichere Passwörter



Quelle: haveibeenpwned.com (32)

Sichere Passwörter

- Zwei-Faktor-Authentisierung
  - Login mit zwei Faktoren
    - Meistens Passwort + Code per SMS oder APP
  - Bei geklauten Login-Daten ist trotzdem keine Anmeldung möglich
  - Bekannt von der Bezahlung per EC-Karte (Pin + Karte)

- Passwortmanager
  - 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, …)

Sichere Passwörter - Passwortkarten

Nr: Kategorie:

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

Sichere Passwörter - 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,	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

Sichere Passwörter - 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

Sichere Passwörter - 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,	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

Sichere Passwörter - 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

Sichere Passwörter - 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

Sichere Passwörter - 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,	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

Sichere Passwörter - Passwortkarten

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

Nr: 1 Kategorie: Online-Banking

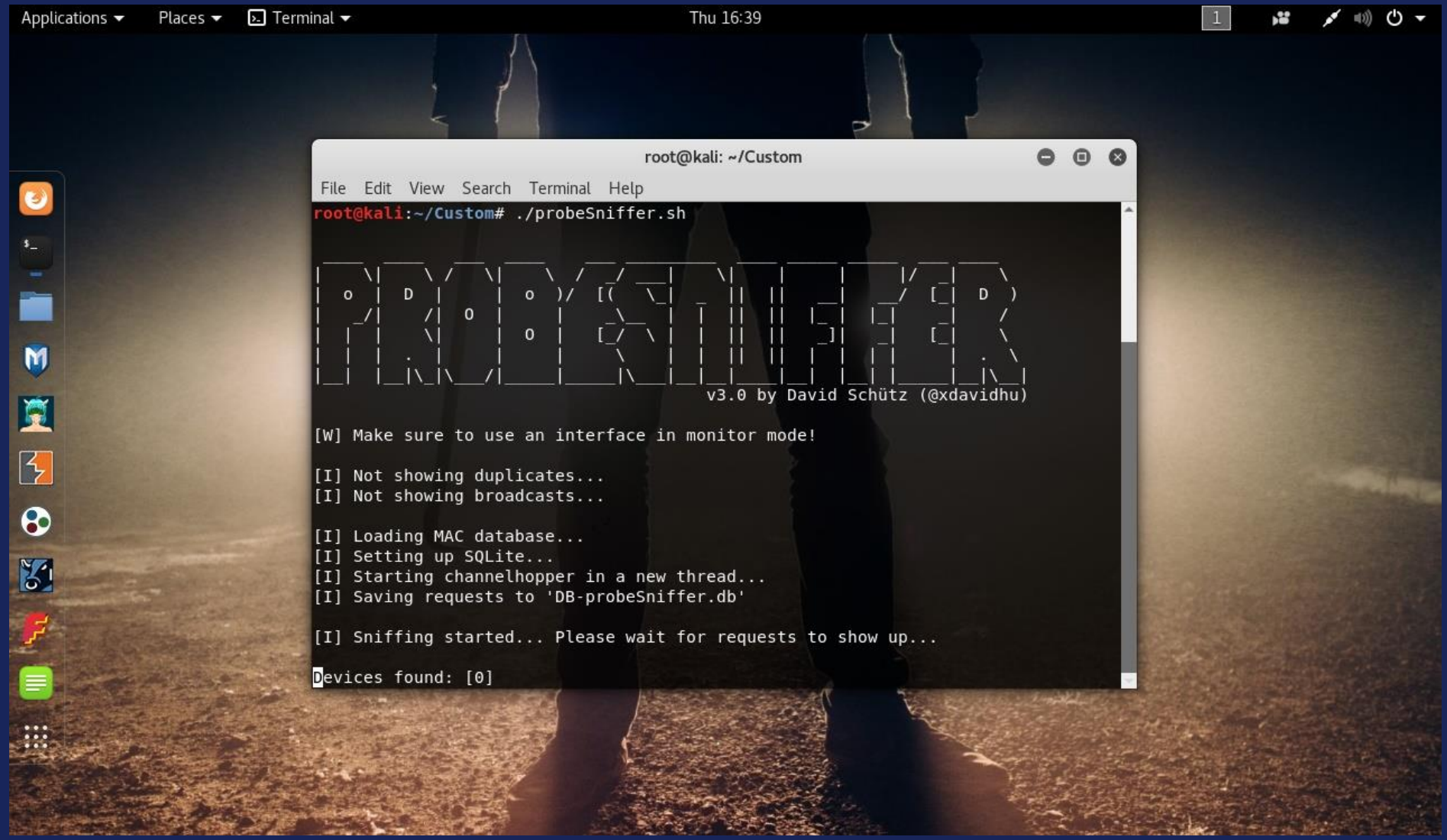
	abc	def	ghi	jkl	mno	pqr	stu	vwx	yz	#
1	x!	Q*	S<	bL	Pn	X:	V=	dd	n3	9K
2	T8	wb	eT	98	C,	6<	ff	aO	X>	Hm
3	Bd	dD	C)	7c	gz	er	q]	p=	t&	1P
4	ne	a@	e-	W8	k-	G2	>d	PE	z3	z:
5	V·	H>	d*	W-	Wl	J8	Qi	U,	ld	7R
6	5=	mF	2n	XY	m:	f<	YH	mo	h4	7-
7	vT	ej	R:	+<	Vg	Nh	a9	6;	dJ	N{
8	d6	G7	p)	ek	pJ	mb	y2	e?	Jm	Rv

Fazit Passwortsicherheit

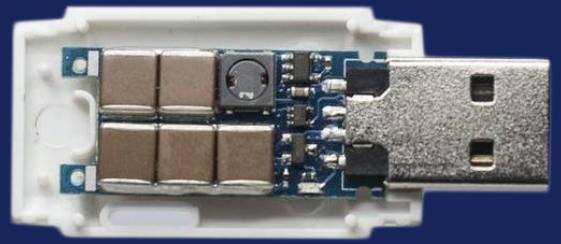
- Die Länge eines Passwortes ist ein entscheidender Faktor. Lange Passwörter sind, pauschal gesagt, sicherer als kurze.
- Das Passwort darf nicht mit Ihrem persönlichen Umfeld in Verbindung stehen.
- Nutzen Sie für jeden Dienst verschiedene Passwörter, damit nach einem Angriff nicht auch andere Accounts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

Hardware Hacks

DEMO Probe Requests Scanner



Hardware Tools



Quelle: amazon.com (33)

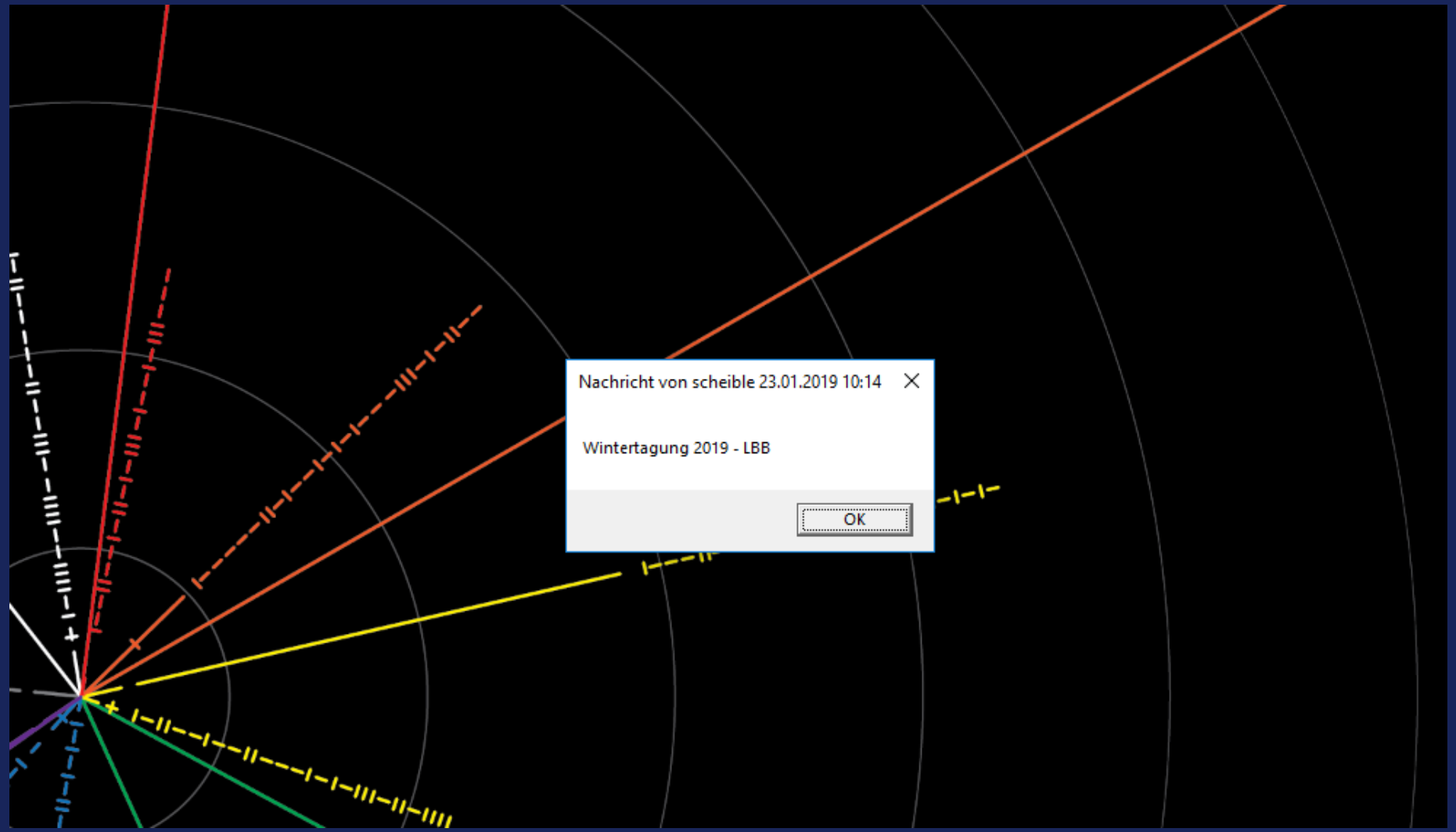
Quelle: hachshop.com (34)

Quelle: amazon.de (35)

Quelle: quora.com (36)

Quelle: pki-electronic.com (37)

DEMO BadUSB



FAZIT Hardware Hacks

- Rechner, die sich in einem frei zugänglichen Bereich befinden, sollten durch bauliche Maßnahmen vor Manipulationen geschützt werden.
- Jede Hardware sollte kontinuierlich auf Veränderungen automatisch überprüft und Vorkommnisse gemeldet werden.
- Mitarbeiter müssen sensibilisiert werden, damit unbekannte Geräte oder abweichende Verhaltensweisen sofort gemeldet werden.
- Ein Ausfall einer Sicherheitskomponente soll gleichgesetzt werden wie ein Alarm.

Zukünftige Entwicklung

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 (38)

IoT – Ransomware

Quelle: computerworld.com (39)

Vielen Dank für Ihre Aufmerksamkeit

Hochschule
Albstadt-Sigmaringen
University of Applied Sciences

Fakultät Informatik

Noch Fragen?

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

Quellen

(1) 00000000: Passwort für US-Atomraketen, http://www.heise.de/security/meldung/00000000-Passwort-fuer-US-Atomraketen-2060077.html, abgerufen am 23.01.2019

(2) Mit Floppy Disks Atombomben überwachen, http://www.zeit.de/politik/ausland/2016-05/us-militaer-pcs-technologie-veraltet-rechnungshof, abgerufen am 23.01.2019

(3) Was ist eigentlich die Geschichte der Malware?, https://www.gdata.de/ratgeber/was-ist-eigentlich-die-geschichte-der-malware, abgerufen am 23.01.2019

(4) AIDS (Schadprogramm), https://de.wikipedia.org/wiki/AIDS_(Schadprogramm), abgerufen am 23.01.2019

(5) Doxing - eine alte Hacker-Waffe trifft den deutschen Mainstream , https://www.sueddeutsche.de/digital/hack-doxing-privatsphaere-1.4278901, abgerufen am 23.01.2019

(6) online metadata and exif viewer, http://metapicz.com, abgerufen am 23.01.2019

(7) Millionen Passwörter im Netz veröffentlicht, https://www.zeit.de/digital/datenschutz/2019-01/datenleak-email-passwoerter-internet-it-sicherheit, abgerufen am 23.01.2019

(8) iWebapp, http://www.shop.ledermode.tv, abgerufen am 23.01.2019

(9) Google, https://google.de, abgerufen am 23.01.2019

(10) Google Hacking Database, https://www.exploit-db.com/google-hacking-database, abgerufen am 23.01.2019

(11) IP-Kameras von Aldi als Sicherheits-GAU, http://www.heise.de/security/meldung/IP-Kameras-von-Aldi-als-Sicherheits-GAU-3069735.html, abgerufen am 23.01.2019

(12) Shodan, https://www.shodan.io, abgerufen am 23.01.2019

(13) Shodan, https://www.shodan.io, abgerufen am 23.01.2019

Quellen

(14) Low Orbit Ion Cannon (LOIC), https://en.wikipedia.org/wiki/Low_Orbit_Ion_Cannon#/media/File:LOIC-0.png, abgerufen am 23.01.2019

(15) LOIC - Low Orbit Ion Cannon, http://m.1mobile.com/genius.mohammad.loic.html, abgerufen am 23.01.2019

(16) Anuncio - gwapo‘s, https://www.youtube.com/watch?v=5M9k7wfiWiI, abgerufen am 23.01.2019

(17) Locky, https://de.wikipedia.org/wiki/Locky, abgerufen am 23.01.2019

(18) Gefälschte E-Mail - Schulfrei ermogelt, http://www.spiegel.de/schulspiegel/schulfrei-in-niedersachsen-wegen-gefaelschter-e-mail-a-1071105.html, abgerufen am 23.01.2019

(19) Legisdigit@ - Groupe Mutuel Versicherungen - https://www.youtube.com/watch?v=WvRL5I1eU3E, abgerufen am 23.01.2019

(20) Gefängnisausbruch mittels E-Mail-Betrug, http://www.heise.de/newsticker/meldung/Gefaengnisausbruch-mittels-E-Mail-Betrug-2587303.html, abgerufen am 23.01.2019

(21) Clone Zone, http://clonezone.link, abgerufen am 23.01.2019

(22) Den Enkeltrick gibt's auch bei Unternehmen, https://www.wiwo.de/erfolg/management/falsche-chefs-zocken-firmen-ab-den-enkeltrick-gibts-auch-bei-unternehmen/12201572.html, abgerufen am 23.01.2019

(23) Code, http://pics-for-fun.com/wonder-what-the-code-could-be/, abgerufen am 23.01.2019

(24) And the valuables are in the closet on the top shelf in a box marked, https://de.pinterest.com/pin/3025924727584002/, abgerufen am 23.01.2019

(25) What is Your Password?, https://www.youtube.com/watch?v=opRMrEfAIiI, abgerufen am 23.01.2019

(26) Passwörter im TV-Bild: Spekulationen zu TV5-Attacke, http://www.heise.de/newsticker/meldung/Passwoerter-im-TV-Bild-Spekulationen-zu-TV5-Attacke-2598298.html, abgerufen am 23.01.2019

Quellen

(27) The Agency That Messed Up Hawaii's Nuclear Alert Keeps Passwords on Post-Its, https://www.vice.com/en_us/article/qvwmx5/the-agency-that-messed-up-hawaiis-nuclear-alert-keeps-passwords-on-post-its-vgtrn, abgerufen am 23.01.2019

(28) Password Strength, https://xkcd.com/936/, abgerufen am 23.01.2019

(29) Top 100 Adobe Passwords with Count, https://github.com/morontt/symfobrute/blob/master/adobe-top100.txt, abgerufen am 23.01.2019

(30) New data uncovers the surprising predictability of Android lock patterns, https://arstechnica.com/information-technology/2015/08/new-data-uncovers-the-surprising-predictability-of-android-lock-patterns/, abgerufen am 23.01.2019

(31) The Longest iPhone 6 Unlock Code In History (He Gotta Be Cheating), https://www.youtube.com/watch?v=brzU7i2sAcY, abgerufen am 23.01.2019

(32) Have I Been Pwned: Check if your email has been compromised in a data breach, https://haveibeenpwned.com, abgerufen am 23.01.2019

(33) The Original USB KeyLogger 8MB Black, http://www.amazon.com/KeyGrabber-USB-KeyLogger-8MB-Black/dp/B004TUBOKW, abgerufen am 23.01.2019

(34) Pocket Jammer, http://www.pki-electronic.com/products/jamming-systems/pocket-jammer/, abgerufen am 23.01.2019

(35) Mobile Mini GSM Alarmanlage Quadband mit Rückruffunktion, https://www.amazon.de/Mobile-Alarmanlage-Quadband-Rückruffunktion-Geräuschaktivierungs-Lautstärke-Schwarz/dp/B00RC7SF8S, abgerufen am 23.01.2019

(36) USB Rubber Ducky, https://hakshop.com/products/usb-rubber-ducky-deluxe, abgerufen am 23.01.2019

(37) How do USB killers work?, https://www.quora.com/How-do-USB-killers-work, abgerufen am 23.01.2019

(38) UK police arrested the alleged mastermind of the MIRAI attack on Deutsche Telekom, http://securityaffairs.co/wordpress/56604/cyber-crime/mirai-attack-deutsche-telekom.html, abgerufen am 23.01.2019

(39) Hackers demonstrated first ransomware for IoT thermostats at DEF CON, https://www.computerworld.com/article/3105001/security/hackers-demonstrated-first-ransomware-for-iot-thermostats-at-def-con.html, abgerufen am 23.01.2019