Tobias Scheible, M.Eng.

Cyber Security Workshop

Praxisorientierte IT-Sicherheit

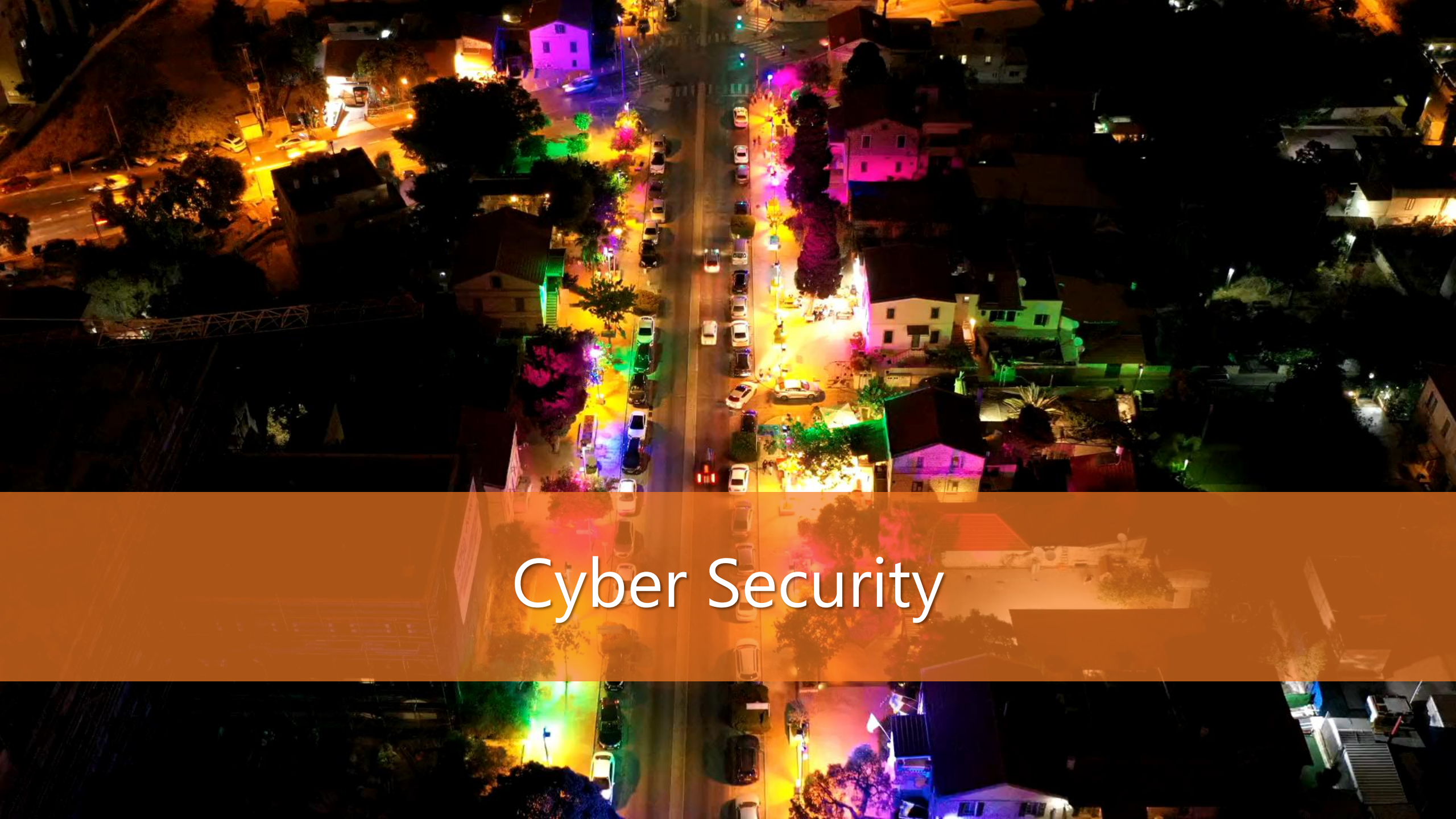
Tobias Scheible, M.Eng.

Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

- 2009 bis 2012: Softwareingenieur im Bereich Web Development
- Seit 2012: Wissenschaftlicher Mitarbeiter an der Hochschule Albstadt-Sigmaringen
  - Forschungsprojekt SEKT (IT Security & Smart Textiles)
  - Aktuelle & ehemalige Lehrmodule (Auswahl):
    - Grundlagen der digitalen Forensik Masterstudiengang IT GRC Management
    - Digitale Forensik Bachelorstudiengang IT Security
    - Internet Grundlagen Masterstudiengang Digitale Forensik
    - Betriebssystemforensik Masterstudiengang Digitale Forensik
    - IT Security 2 Bachelorstudiengang IT Security
    - Informationssicherheit Bachelorstudiengang Wirtschaftsinformatik
    - Internettechnologien Hochschulzertifikatsprogramm
    - Cloud Technologies and Cloud Security Architectures Masterstudiengang IT GRC

Agenda

- Cyber Security
  - Grundlagen
  - IT-Sicherheitsvorfälle
  - Cybercrime as a Service
- Social Engineering
  - Manipulation von Menschen
  - Social Engineering Beispiele
- Passwortsicherheit
  - Angriffe auf Passwörter
  - Sicherer Umgang mit Passwörtern
- Datenschutz
  - Versteckte Informationen
  - Sicher im Web
- IT Security Hardware
  - Hardware Tools



Cyber Security

000000000

?

Quelle: heise.de (1)

Cyber Security
Grundlagen
IT-Sicherheitsvorfälle
Cybercrime as a Service

Social Engineering

Passwortsicherheit

Datenschutz

IT Security Hardware

Cyber Security
Grundlagen
IT-Sicherheitsvorfälle
Cybercrime as a Service
Social Engineering
Passwortsicherheit
Datenschutz
IT Security Hardware

00000000

Launch-Code für die in den USA stationierten Atomraketen

(1962 bis 1977)

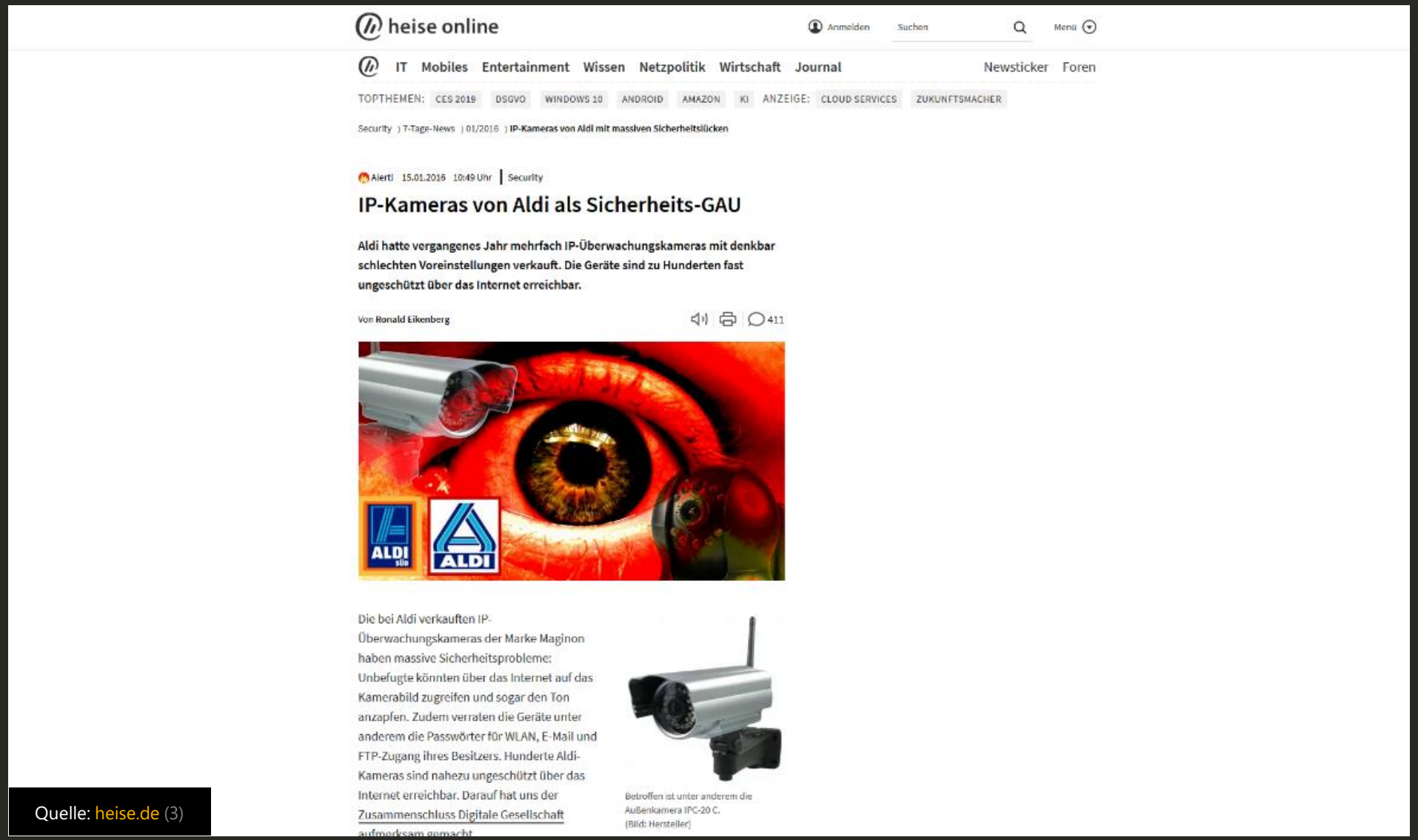
Quelle: heise.de (1)

Pin Code Beispiel

Quelle: zeit.de (2)

Cyber Security
Cyber Security
Grundlagen
IT-Sicherheitsvorfälle
IT-Sicherheitsvorfälle
Cybercrime as a Service
Cybercrime as a Service
Social Engineering
Social Engineering
Passwortsicherheit
Passwortsicherheit
Datenschutz
Datenschutz
IT Security Hardware
IT Security Hardware

Verwundbare Webcam



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)

Quelle: heise.de (3)

Cyber Security
Grundlagen
IT-Sicherheitsvorfälle
Cybercrime as a Service

Social Engineering

Passwortsicherheit

Datenschutz

IT Security Hardware

Webcams einfach finden

Quelle: google.de (4)

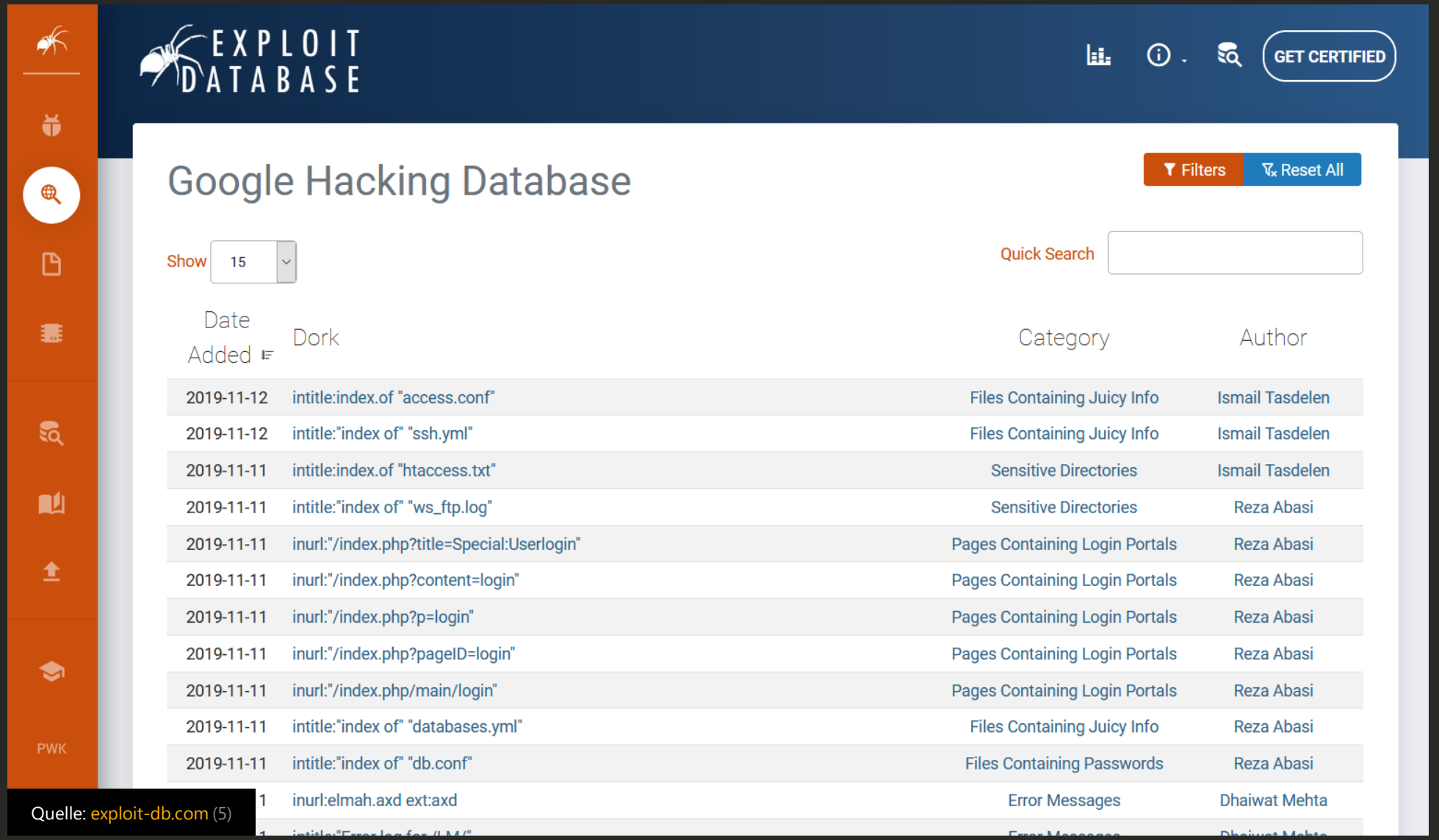
Webcams einfach finden

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 enthalten. 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"*

PRAXIS Webcams einfach finden

- 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"

Webcams einfach finden - GHDB



Quelle: exploit-db.com (5)

Cyber Security
- Grundlagen
- IT-Sicherheitsvorfälle
- Cybercrime as a Service

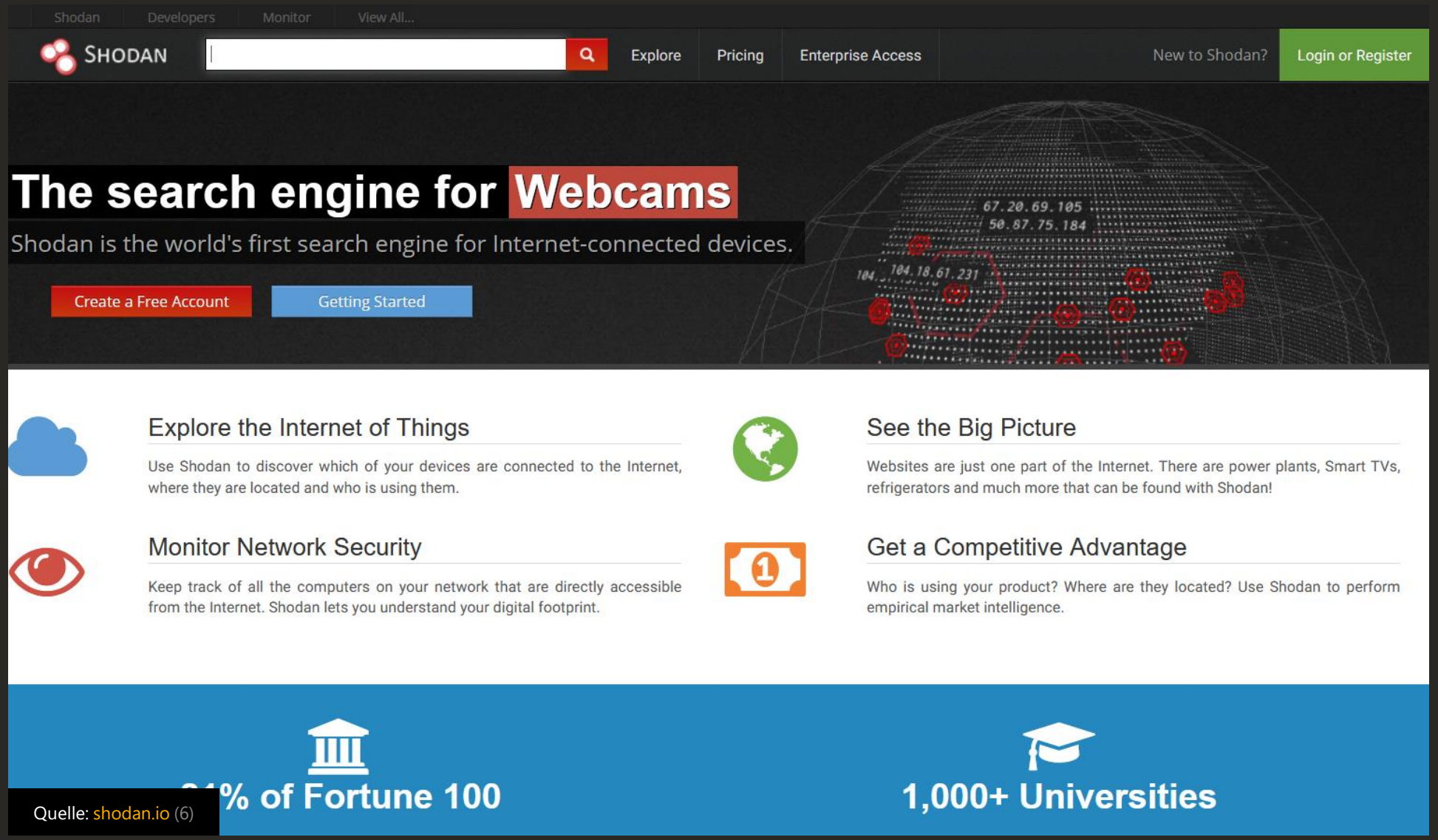
Social Engineering

Passwortsicherheit

Datenschutz

IT Security Hardware

Webcams einfach finden - Shodan



Quelle: shodan.io (6)

Cyber Security
- Grundlagen
- IT-Sicherheitsvorfälle
- Cybercrime as a Service

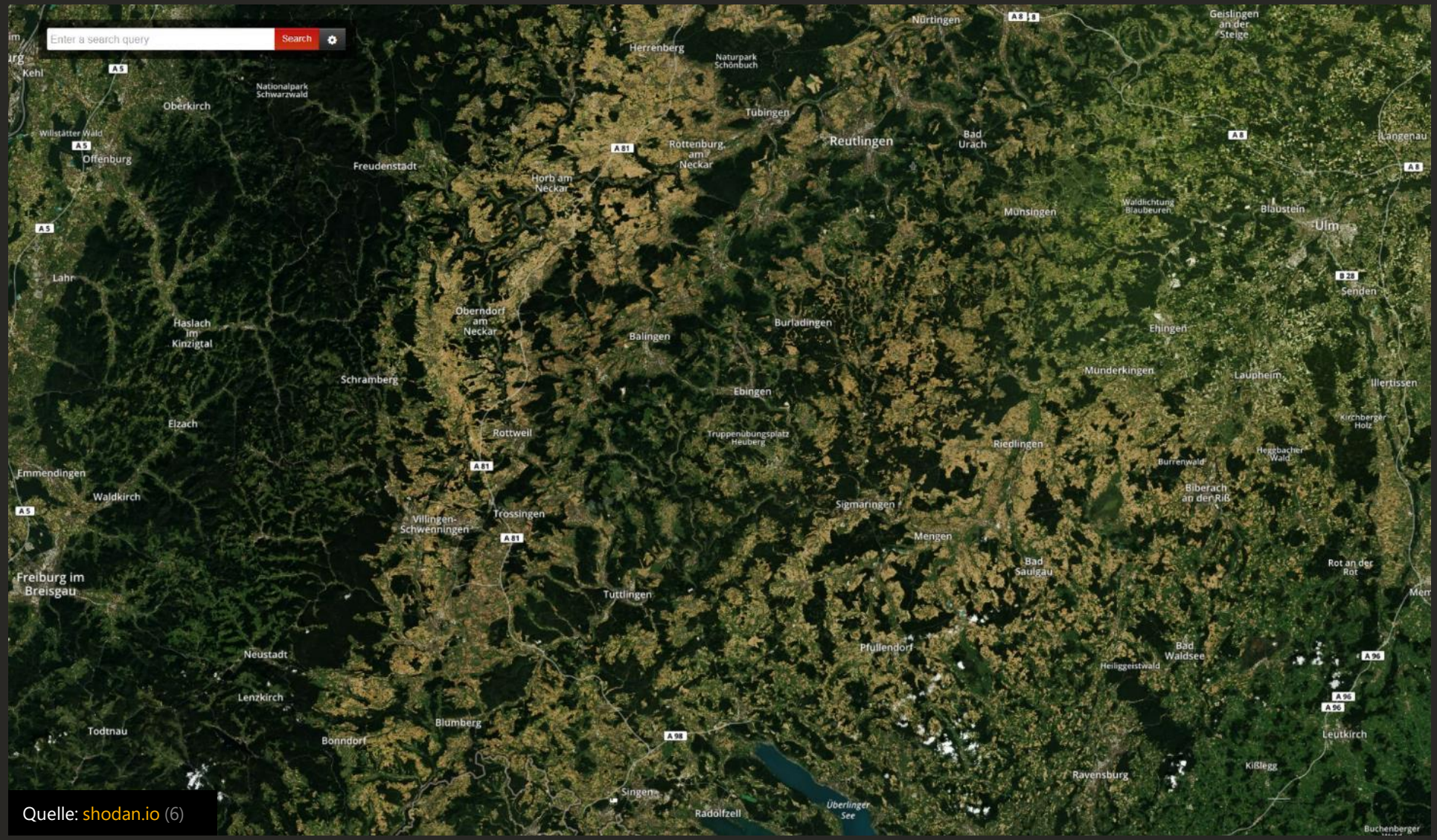
Social Engineering

Passwortsicherheit

Datenschutz

IT Security Hardware

LIVE Webcams einfach finden - Shodan



Quelle: shodan.io (6)

Cyber Security
- Grundlagen
- IT-Sicherheitsvorfälle
- Cybercrime as a Service

Social Engineering

Passwortsicherheit

Datenschutz

IT Security Hardware

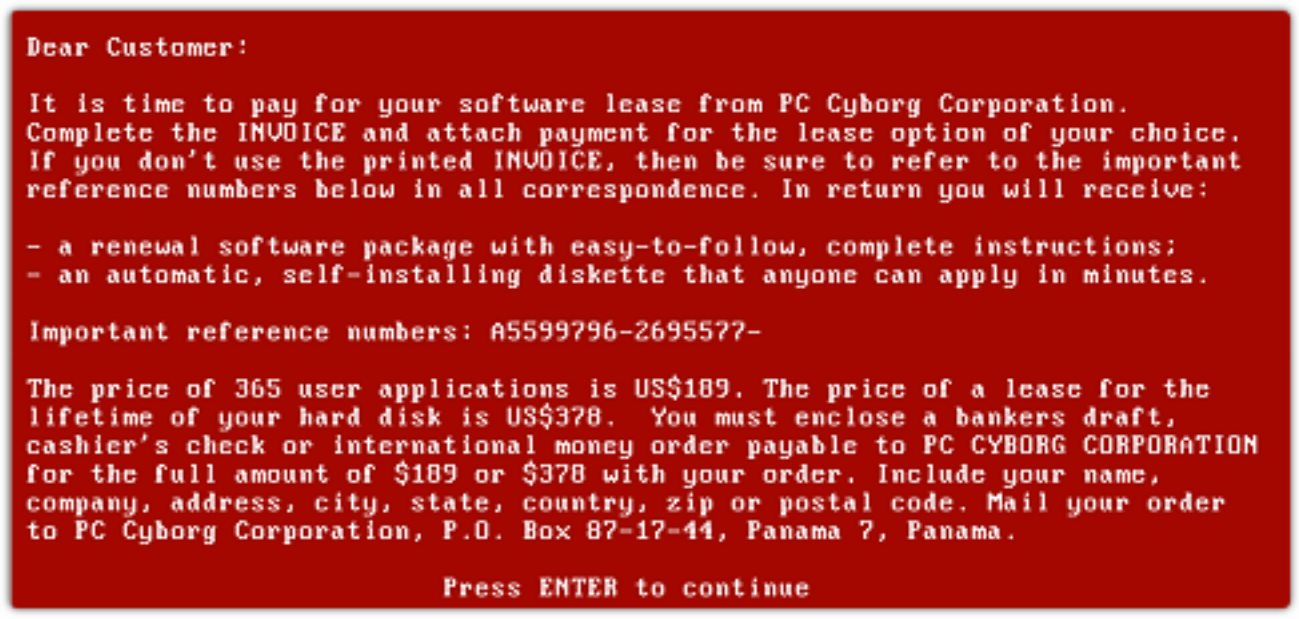
Geschichte der Schadsoftware

- Nutzung von Standardfunktionen
  - 80er Jahre: Der Begriff Computervirus wird zum ersten Mal verwendet
  - 1985: Über Computerviren wird in Deutschland berichtet
  - 1988: Zum ersten Mal wird das Konzept „Würmer“ bekannt

Quelle: gdata.de (7)

Geschichte der Schadsoftware - AIDS

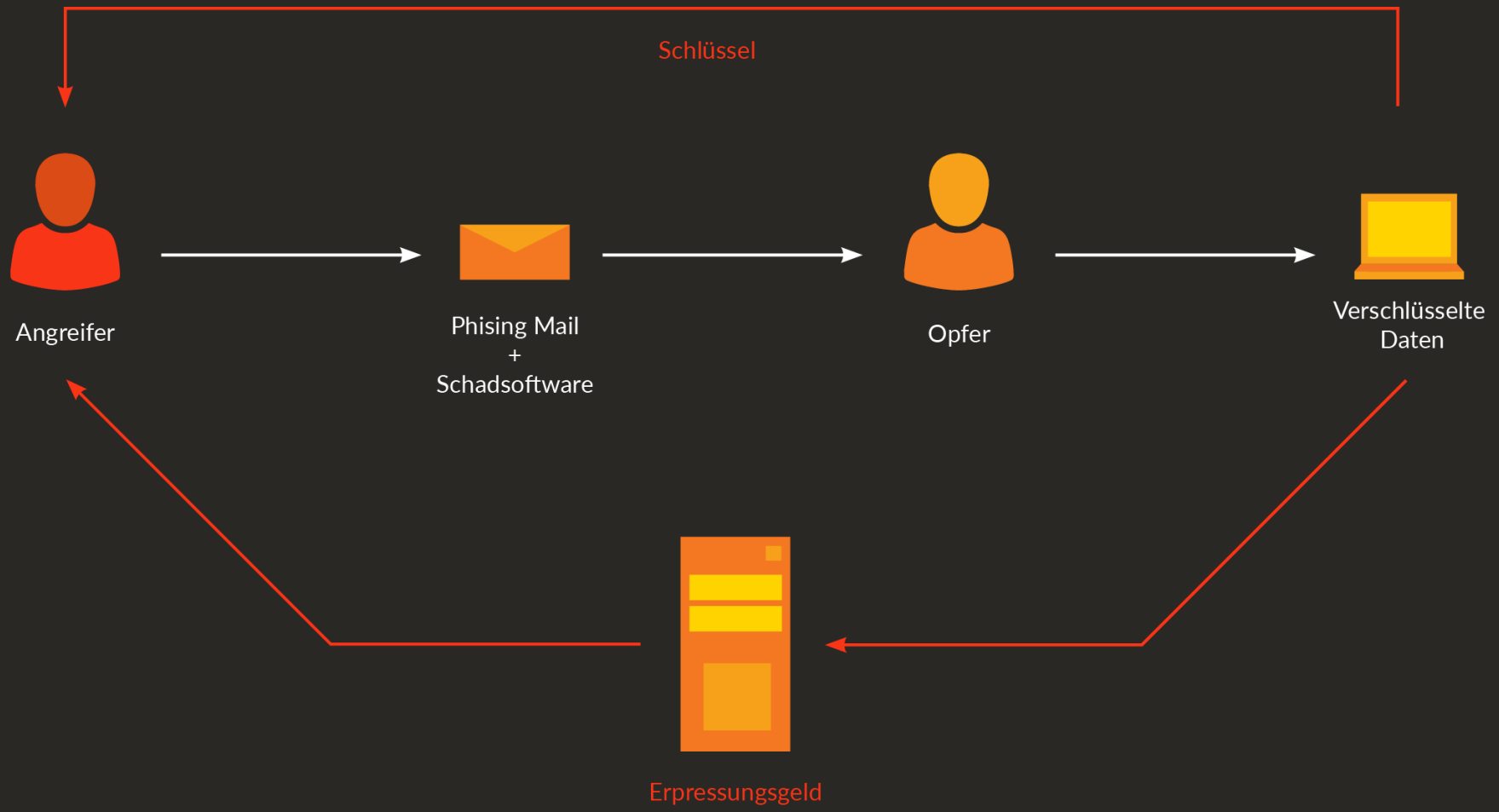
- Erste Angriffe mit Ransomware bereits 1989
- Schadsoftware wurde per 5,25“ Diskette mit der Post verschickt
- Nach 90 Starts wurden die Dateinamen verschlüsselt
  - Eine italienische AIDS Organisation verlor Forschungsergebnisse aus 10 Jahren
  - Ersteller der Ransomware wurde 1990 verhaftet



Quelle: wikipedia.org (8)

Cyber Security
Grundlagen
IT-Sicherheitsvorfälle
Cybercrime as a Service
Social Engineering
Passwortsicherheit
Datenschutz
IT Security Hardware

Ransomware



Cyber Security
Grundlagen
IT-Sicherheitsvorfälle
Cybercrime as a Service

Social Engineering

Passwortsicherheit

Datenschutz

IT Security Hardware

Geschichte der Schadsoftware

- Nutzung von Standardfunktionen
  - 80er Jahre: Der Begriff Computervirus wird zum ersten Mal verwendet
  - 1985: Über Computerviren wird in Deutschland berichtet
  - 1988: Zum ersten Mal wird das Konzept „Würmer“ bekannt
- Ausnutzung von Schwachstellen
  - 1997: Schadsoftware nutzt nun gezielt Schwachstellen aus
  - 2000: „I love you” Virus findet in Deutschland große Verbreitung
  - 2000: Erster Trojaner für mobile Endgeräte (PDAs)
- Krimineller Hintergrund
  - 2004: Schadsoftware wird von organisierten Kriminellen eingesetzt
  - 2005: „Wurm“ verbreitet sich automatisch auf Symbian Smartphones per MMS

Quelle: gdata.de (9)

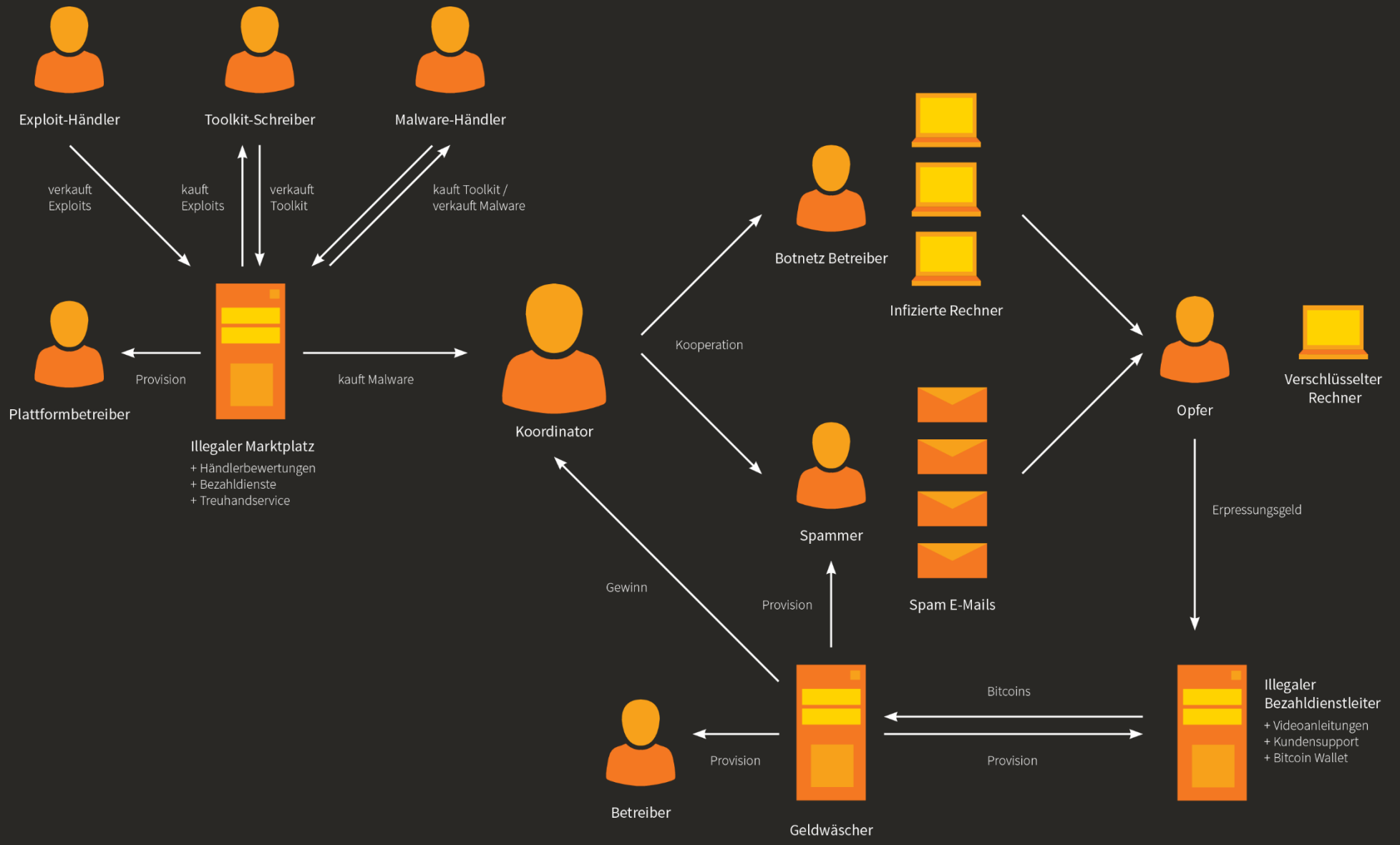
Geschichte der Schadsoftware - Locky

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

- 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 (10)

Cybercrime as a Service - CaaS



Cyber Security
- Grundlagen
- IT-Sicherheitsvorfälle
- Cybercrime as a Service

Social Engineering

Passwortsicherheit

Datenschutz

IT Security Hardware

Cybercrime as a Service - Werbevideo

Quelle: youtube.com (11)

Cyber Security
Grundlagen
IT-Sicherheitsvorfälle
Cybercrime as a Service

Social Engineering

Passwortsicherheit

Datenschutz

IT Security Hardware

Cybercrime as a Service - IoT

- 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

Cyber Security
Grundlagen
IT-Sicherheitsvorfälle
Cybercrime as a Service
Social Engineering
Passwortsicherheit
Datenschutz
IT Security Hardware

Social Engineering

Was ist die häufigste Angriffsmethode?

Ausnutzung von Schwachstellen

A

Physische Attacken

B

Manipulation von Personen

C

Ausnutzung von Fehlern

D

Faktor Mensch

Quelle: pics-for-fun.com (13)

Quelle: de.pinterest.com (14)

Cyber Security

Social Engineering
Manipulation von Menschen
Social Engineering Beispiele

Passwortsicherheit

Datenschutz

IT Security Hardware

Schulfrei ermogelt

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)

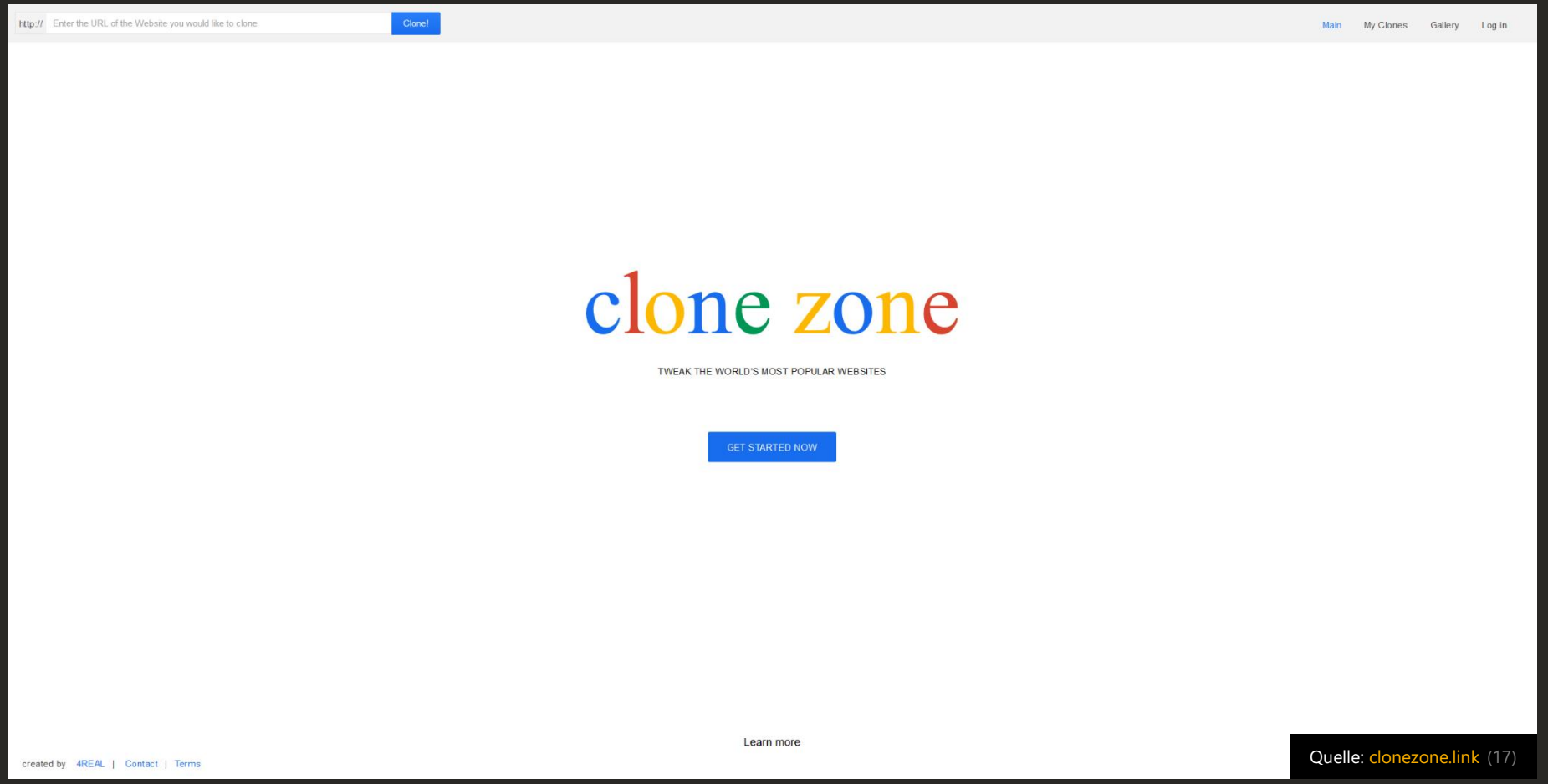
Moderner Gefängnisausbruch

- Moderner Ausbruch aus einem britischen Gefängnis (März 2015)
- SocialEngineering 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)

PRAXIS Gefälschte Websites



Quelle: clonezone.link (17)

Cyber Security

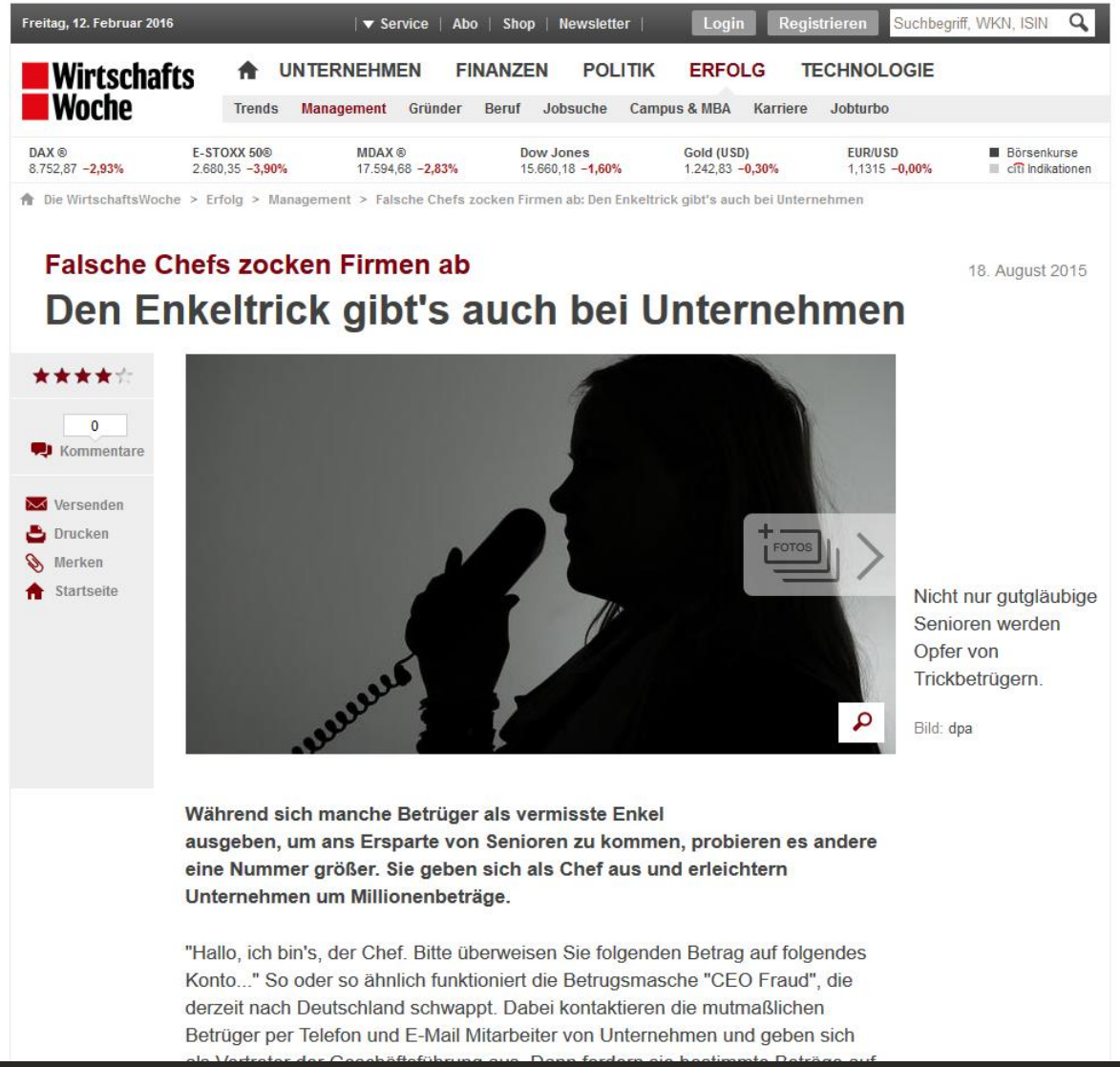
Social Engineering
Manipulation von Menschen
Social Engineering Beispiele

Passwortsicherheit

Datenschutz

IT Security Hardware

Enkeltrick bei Unternehmen - 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 ® 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 | citi 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 (18)

Cyber Security

Social Engineering
Manipulation von Menschen
Social Engineering Beispiele

Passwortsicherheit

Datenschutz

IT Security Hardware

Enkeltrick bei Unternehmen - CEO Fraud

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

Enkeltrick bei Unternehmen - CEO Fraud

..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. 21

Enkeltrick bei Unternehmen - CEO Fraud

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

Enkeltrick bei Unternehmen - CEO Fraud

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

Enkeltrick bei Unternehmen - CEO Fraud

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.

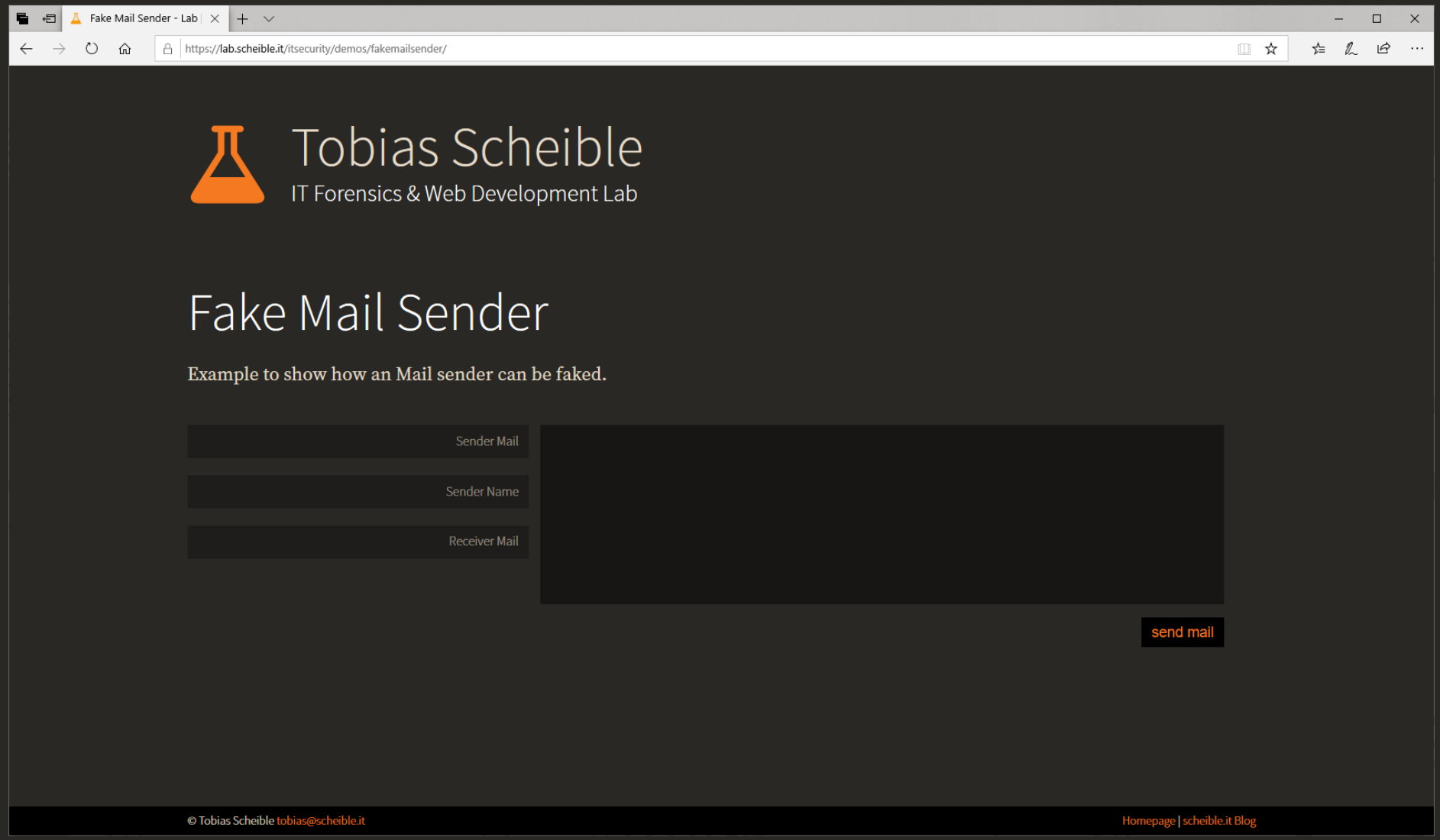
Best regards

B. Berater

BaFin /AMF Consultant

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

LIVE E-Mails fälschen



Cyber Security

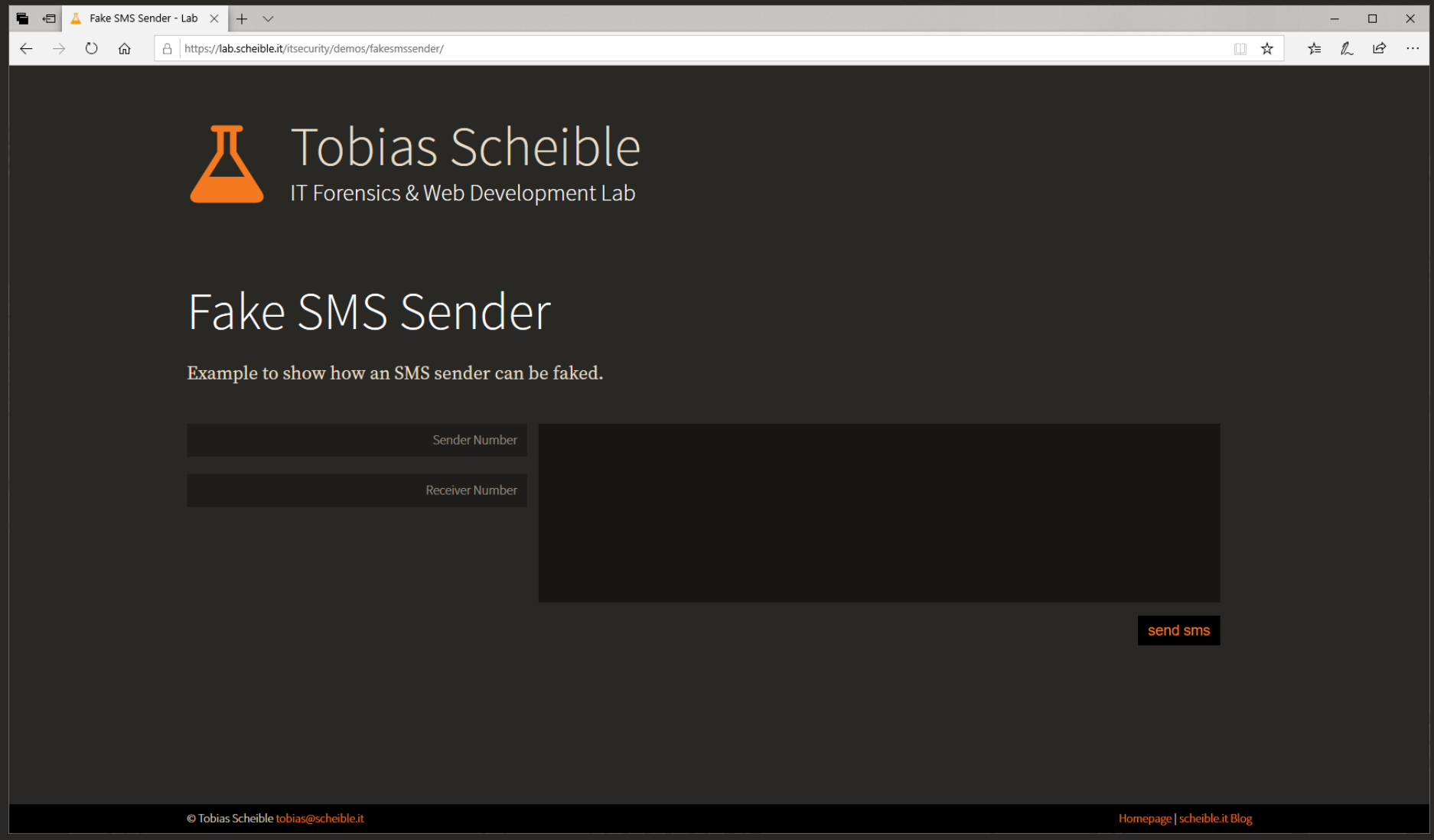
Social Engineering
Manipulation von Menschen
Social Engineering Beispiele

Passwortsicherheit

Datenschutz

IT Security Hardware

LIVE SMS-Versand manipulieren



Cyber Security

Social Engineering
Manipulation von Menschen
Social Engineering Beispiele

Passwortsicherheit

Datenschutz

IT Security Hardware

Passwortsicherheit

Öffentliche Passwörter

Quelle: heise.de (19)

Cyber Security

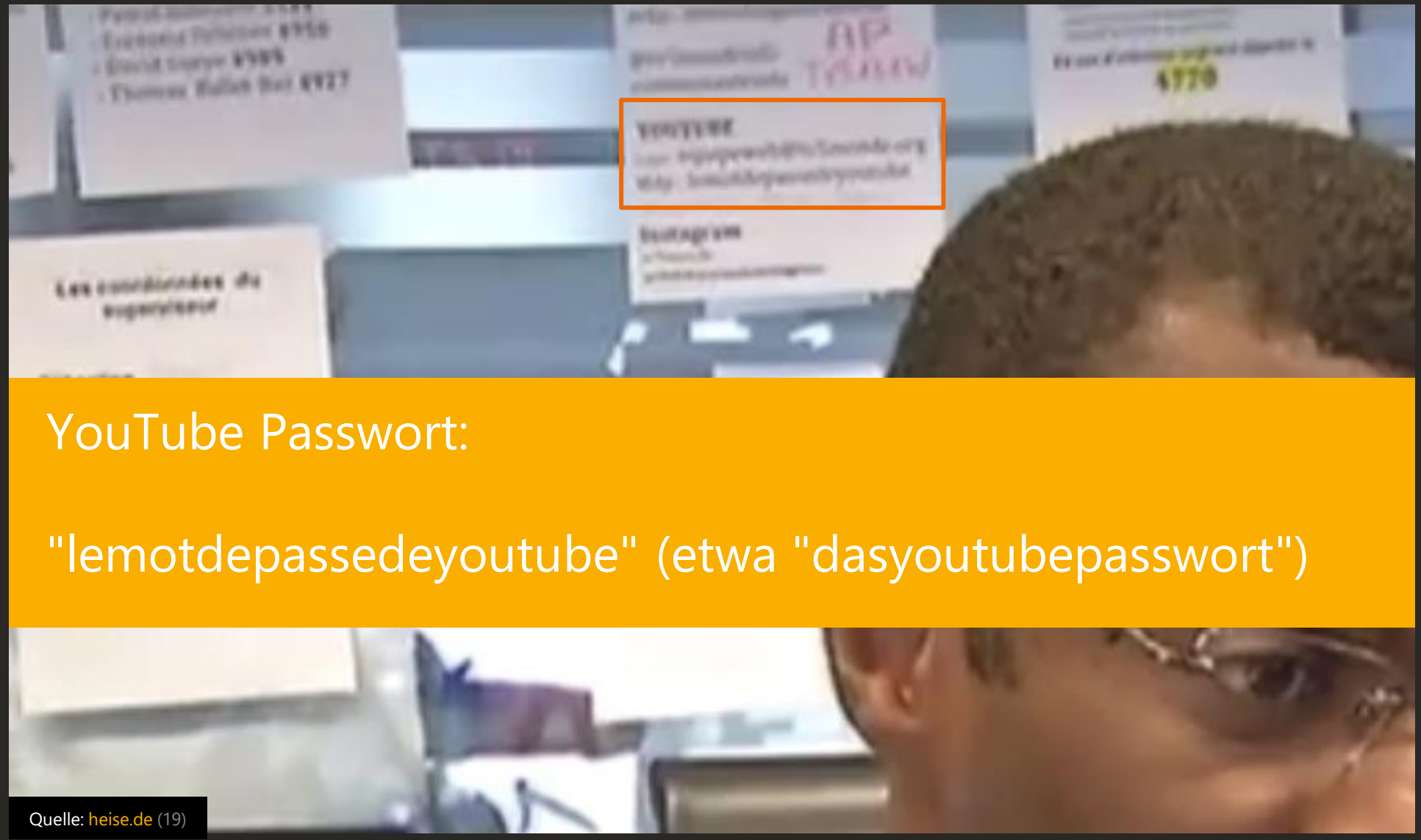
Social Engineering

Passwortsicherheit
- Öffentliche Passwörter
- Angriffe auf Passwörter
- Sicherer Umgang mit Passwörtern

Datenschutz

IT Security Hardware

Öffentliche Passwörter



YouTube Passwort:

"lemotdepassedeyoutube" (etwa "dasyoutubepasswort")

Quelle: heise.de (19)

Cyber Security

Social Engineering

Passwortsicherheit
Öffentliche Passwörter
Angriffe auf Passwörter
Sicherer Umgang mit Passwörtern

Datenschutz

IT Security Hardware

Öffentliche Passwörter

Quelle: vice.com (20)

Cyber Security

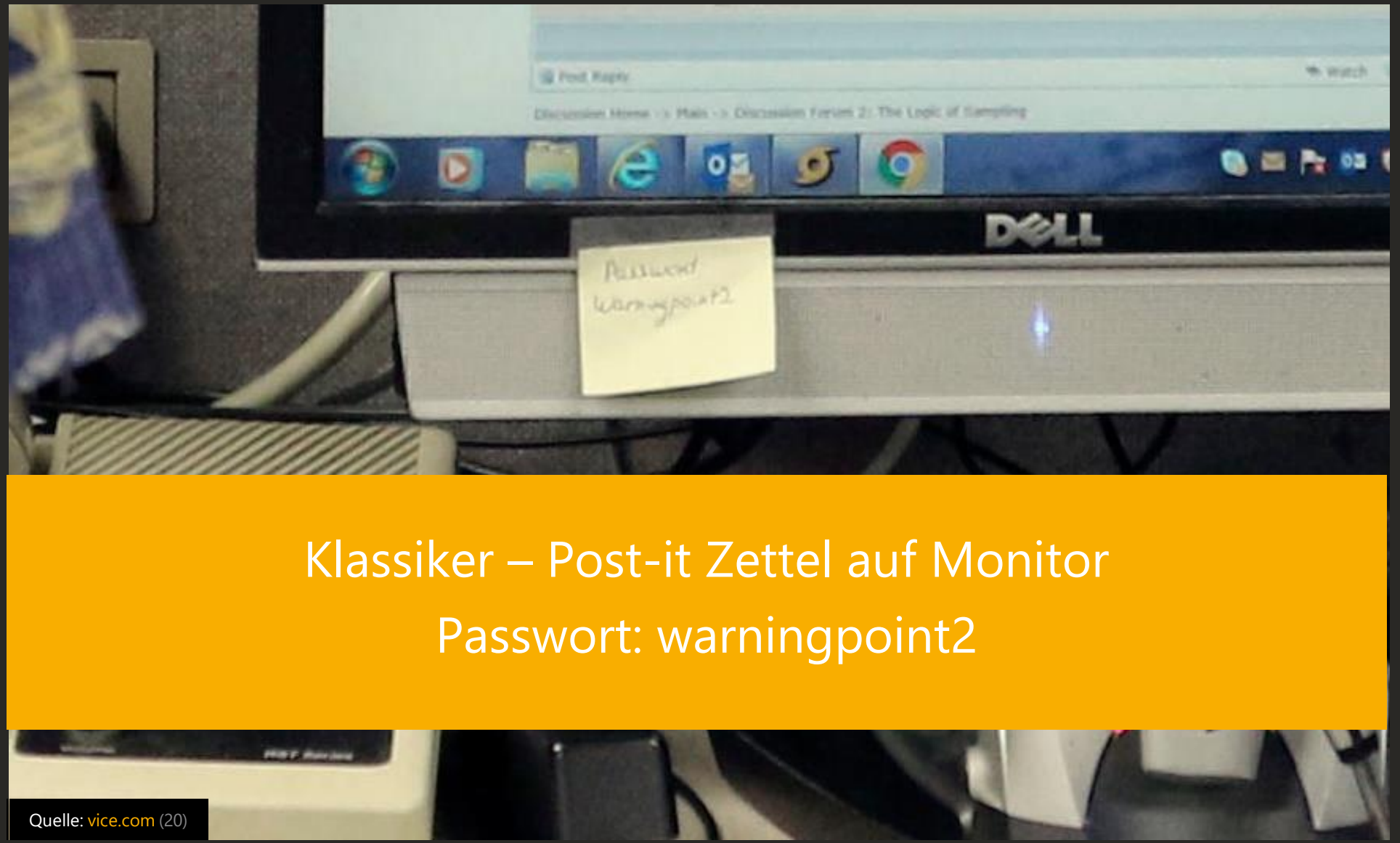
Social Engineering

Passwortsicherheit
- Öffentliche Passwörter
- Angriffe auf Passwörter
- Sicherer Umgang mit Passwörtern

Datenschutz

IT Security Hardware

Öffentliche Passwörter



Klassiker – Post-it Zettel auf Monitor

Passwort: warningpoint2

Quelle: vice.com (20)

Cyber Security

Social Engineering

Passwortsicherheit
Öffentliche Passwörter
Angriffe auf Passwörter
Sicherer Umgang mit Passwörtern

Datenschutz

IT Security Hardware

Passwortsicherheit

Quelle: youtube.com (21)

Cyber Security

Social Engineering

Passwortsicherheit
- Öffentliche Passwörter
- Angriffe auf Passwörter
- Sicherer Umgang mit Passwörtern

Datenschutz

IT Security Hardware

Passwörter erraten

Passwörter erraten

Angreifer analysieren das Umfeld eines Opfers, um auf potentielle Passwörter schließen zu können und so diese zu erraten.

- Alle Seiten bzw. Profile des Opfers werden analysiert.
- Social Media Seiten werden automatisch gescannt
- Auch Fotos werden ausgewertet

Cyber Security

Social Engineering

Passwortsicherheit
Öffentliche Passwörter
Angriffe auf Passwörter
Sicherer Umgang mit Passwörtern

Datenschutz

IT Security Hardware

Passwörter erraten

- Angreifer analysieren das Umfeld eines Opfers, um auf potentielle Passwörter schließen zu können und so diese zu erraten.
  - Alle Seiten bzw. Profile werden von einem Opfer 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
  - Analysieren Sie den Lebenslauf und leiten Sie davon Passwörter ab
  - Versuchen Sie, die PDF-Dateien zu öffnen
  - Probieren Sie verschiedene Passwortkombinationen aus

Wie lauten die Passwörter zum Öffnen der PDF-Dateien?

Bekannte Passwörter

Passwörter erraten

Angreifer analysieren das Umfeld eines Opfers, um auf potentielle Passwörter schließen zu können und so diese zu erraten.

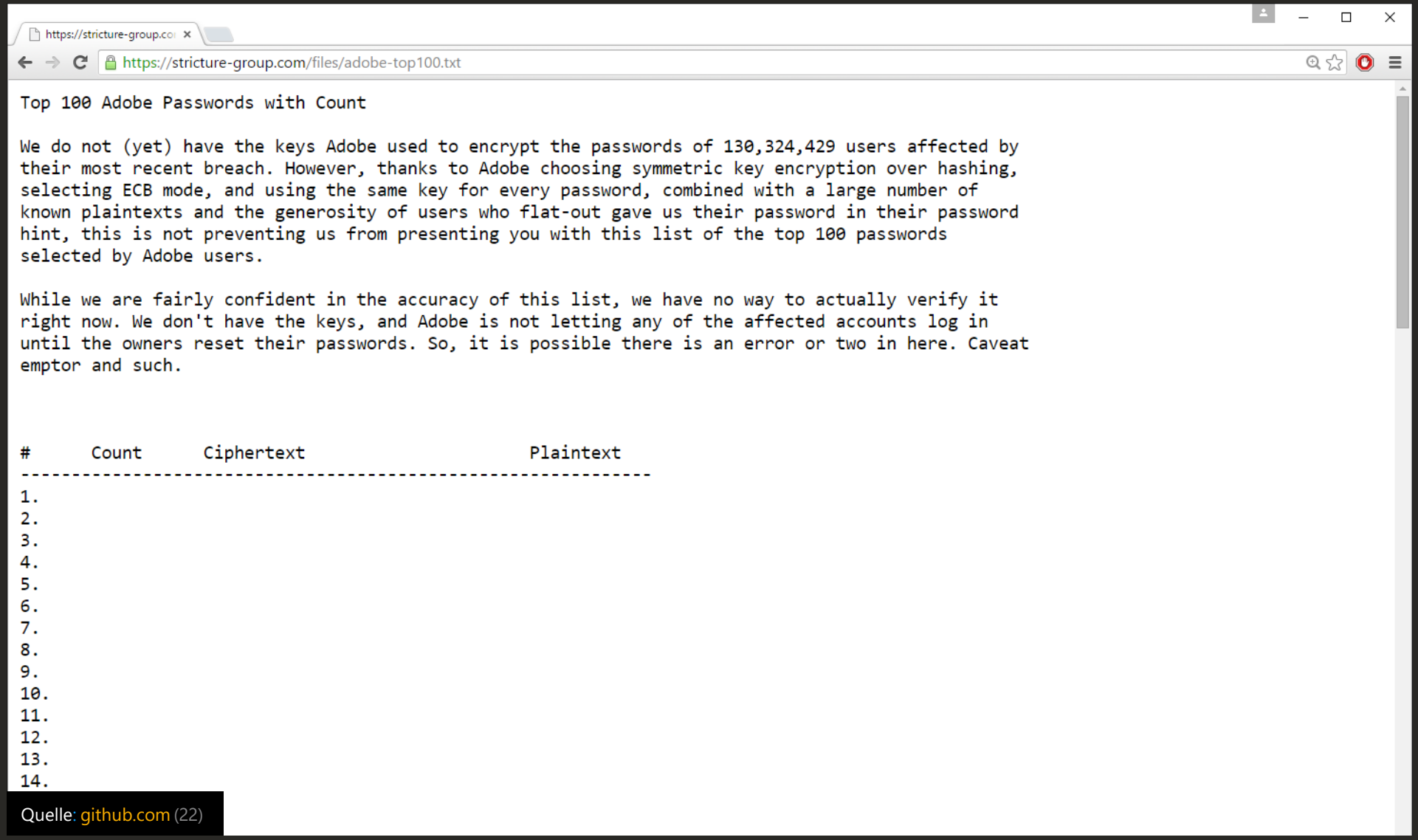
- Alle Seiten bzw. Profile des Opfers werden analysiert.
- Social Media Seiten werden automatisch gescannt.
- Auch Fotos werden ausgewertet.

Bekannte Passwörter

Durch Hacks werden immer wieder Passwörter geklaut und in Listen veröffentlicht.

- Diese werden nach Häufigkeit sortiert gespeichert.
- Sobald ein neues Passwort erbeutet wird, werden andere Dienste angegriffen.
- Daher sollte immer pro Dienst ein anderes Passwort verwendet werden.

Bekannte Passwörter



Quelle: github.com (22)

Cyber Security

Social Engineering

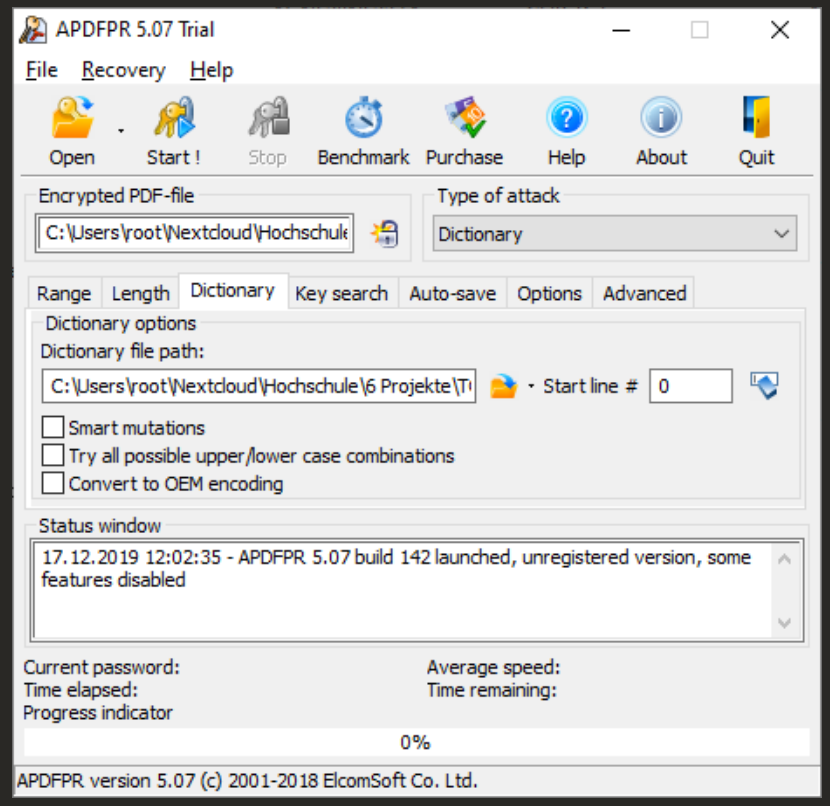
Passwortsicherheit
- Öffentliche Passwörter
- Angriffe auf Passwörter
- Sicherer Umgang mit Passwörtern

Datenschutz

IT Security Hardware

PRAXIS Bekannte Passwörter

Öffnen Sie wieder die das Programm „APDFPR.exe“ und knacken Sie die PDF-Dateien mit der Angriffsmethode „Dictionary“.



Brute-Force-Angriff

Passwörter erraten

Angreifer analysieren das Umfeld eines Opfers, um auf potentielle Passwörter schließen zu können und so diese zu erraten.

- Alle Seiten bzw. Profile des Opfers werden analysiert.
- Social Media Seiten werden automatisch gescannt.
- Auch Fotos werden ausgewertet.

Bekannte Passwörter

Durch Hacks werden immer wieder Passwörter geklaut und in Listen veröffentlicht.

- Diese werden nach Häufigkeit sortiert gespeichert.
- Sobald ein neues Passwort erbeutet wird, werden andere Dienste angegriffen.
- Daher sollte immer pro Dienst ein anderes Passwort verwendet werden.

Brute-Force-Angriff

Angreifer analysieren das Umfeld eines Opfers, um auf potentielle Passwörter schließen zu können und so diese zu erraten.

- Geschwindigkeit abhängig von der verfügbaren Rechenleistung.
- Algorithmus beeinflusst auch die Geschwindigkeit.
- Länge des Passwortes ist für die Sicherheit wichtig.

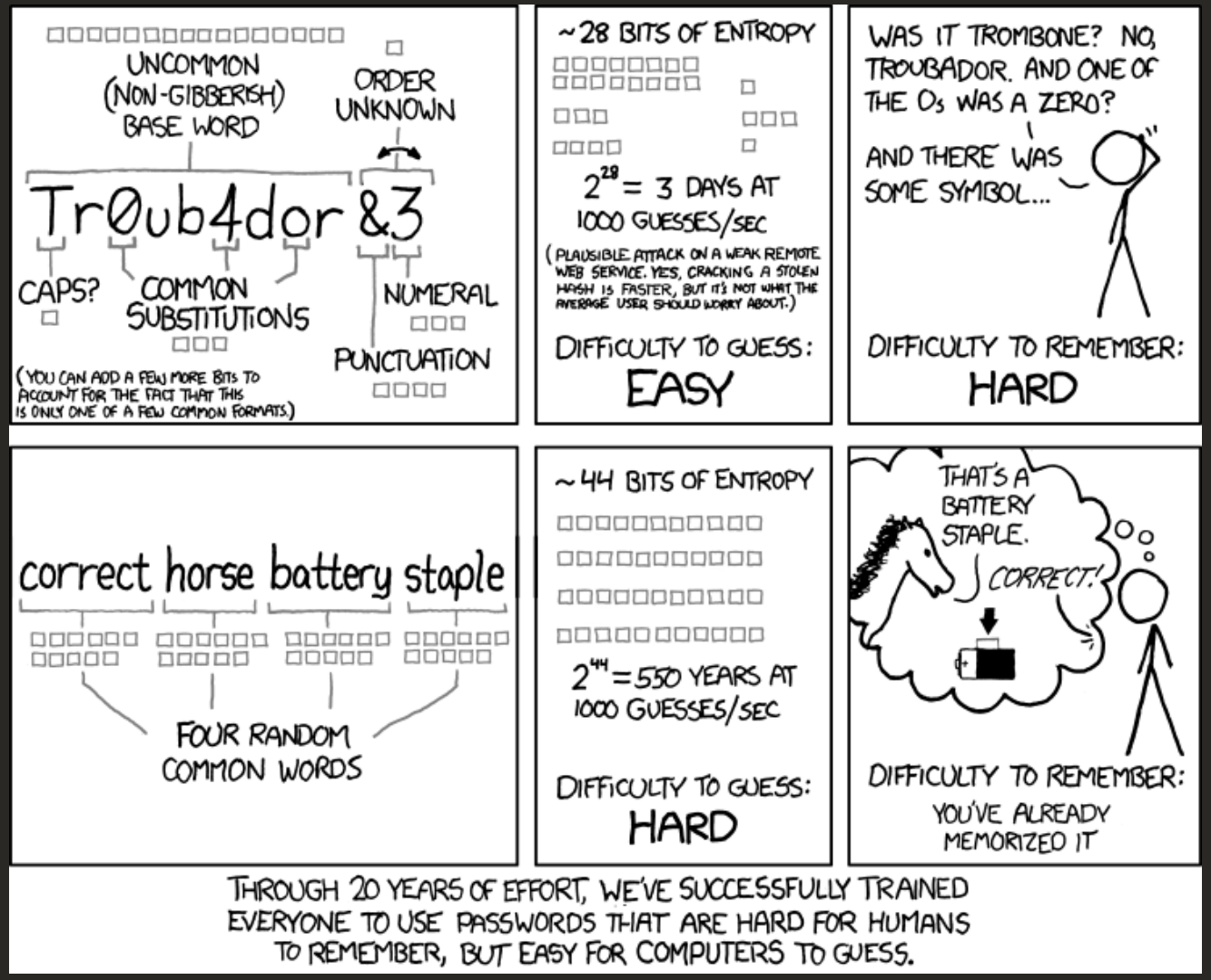
Brute-Force-Angriff

- 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-Angriff

- 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-Angriff



Quelle: xkcd.com (23)

Cyber Security

Social Engineering

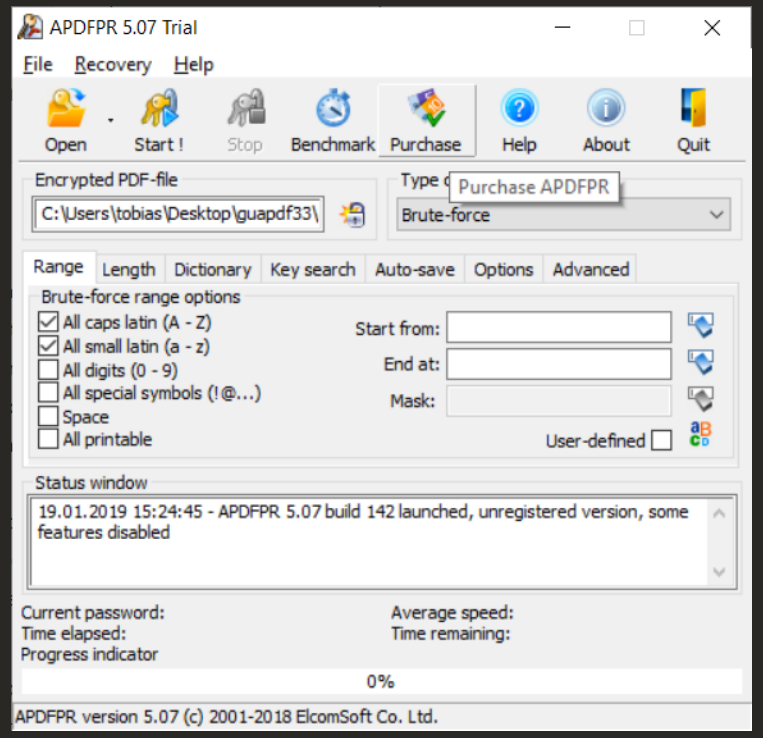
Passwortsicherheit
Öffentliche Passwörter
Angriffe auf Passwörter
Sicherer Umgang mit Passwörtern

Datenschutz

IT Security Hardware

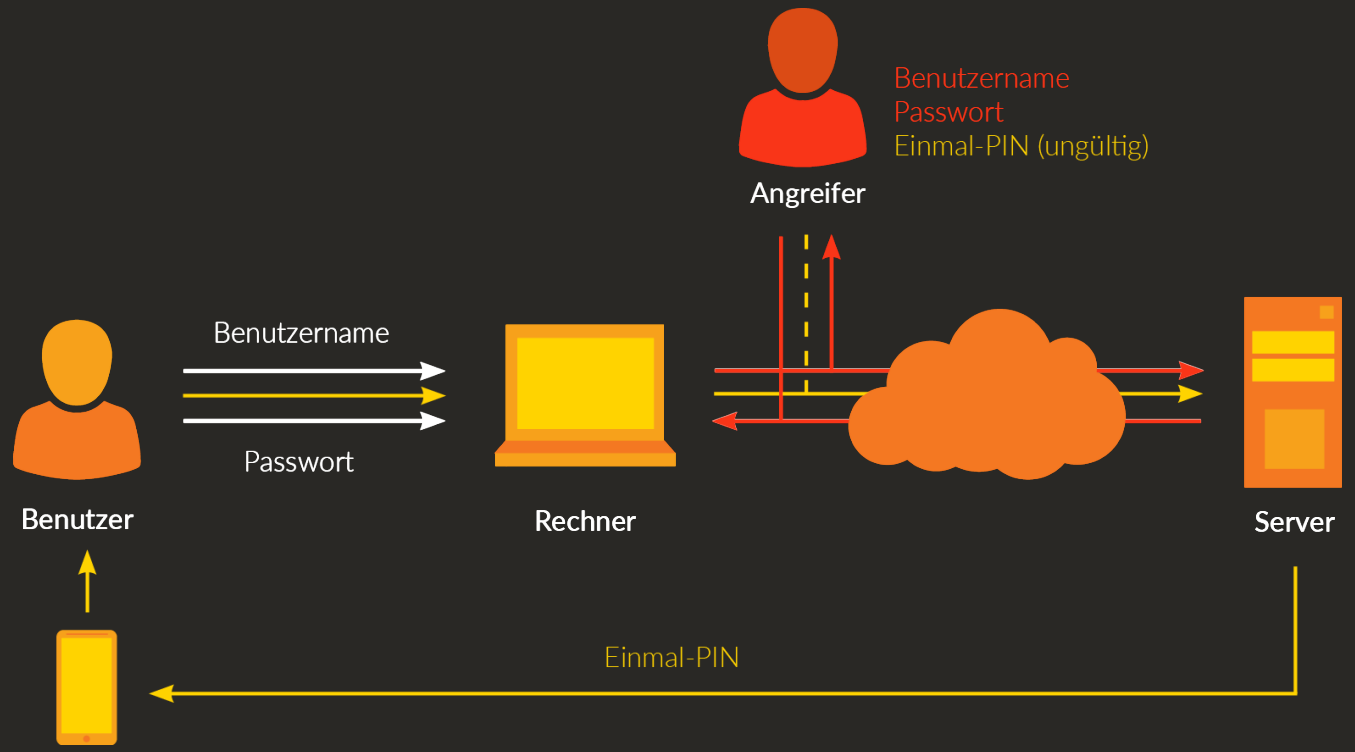
PRAXIS Brute-Force-Angriff

Öffnen Sie die das Programm „APDFPR.exe“ und knacken Sie die PDF-Dateien. Notieren Sie jeweils die benötigte Zeit für die unterschiedlichen Dateien.



Sichere Passwörter

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



Cyber Security

Social Engineering

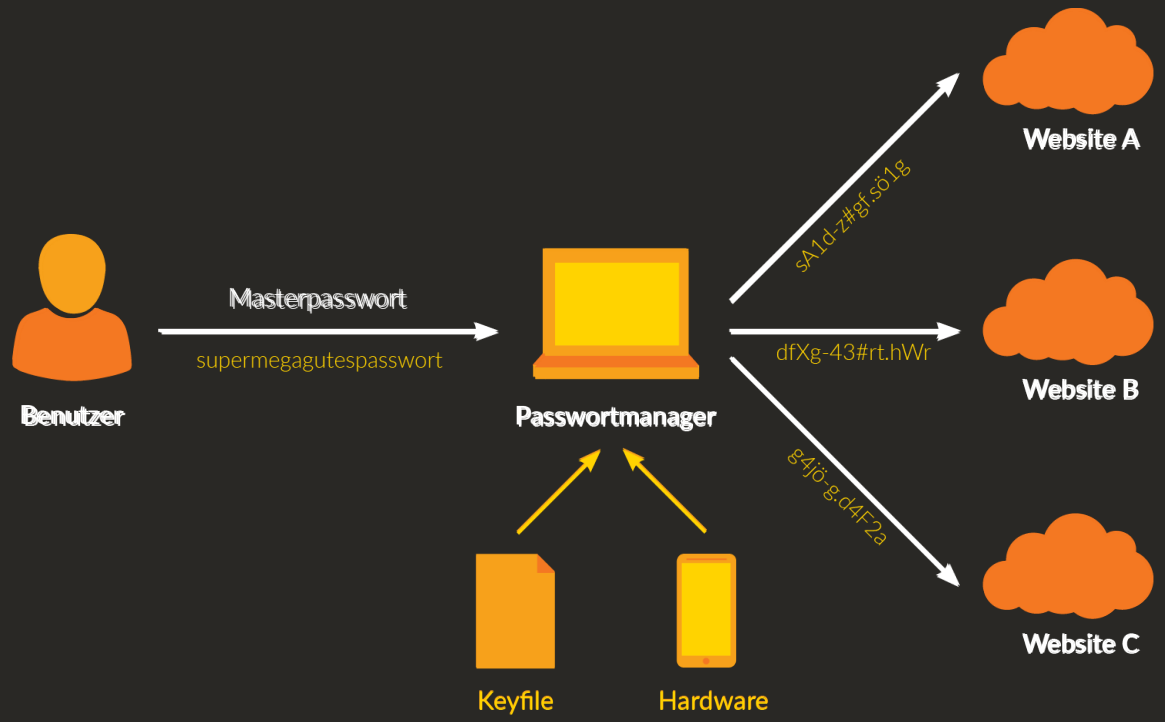
Passwortsicherheit
Öffentliche Passwörter
Angriffe auf Passwörter
Sicherer Umgang mit Passwörtern

Datenschutz

IT Security Hardware

Sichere Passwörter

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



Cyber Security

Social Engineering

Passwortsicherheit
Öffentliche Passwörter
Angriffe auf Passwörter
Sicherer Umgang mit Passwörtern

Datenschutz

IT Security Hardware

Sichere Passwörter - Passwortkarten

Nr: Kategorie:

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

Cyber Security

Social Engineering

Passwortsicherheit
Öffentliche Passwörter
Angriffe auf Passwörter
Sicherer Umgang mit Passwörtern

Datenschutz

IT Security Hardware

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,	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:

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

Cyber Security

Social Engineering

Passwortsicherheit
Öffentliche Passwörter
Angriffe auf Passwörter
Sicherer Umgang mit Passwörtern

Datenschutz

IT Security Hardware

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

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

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

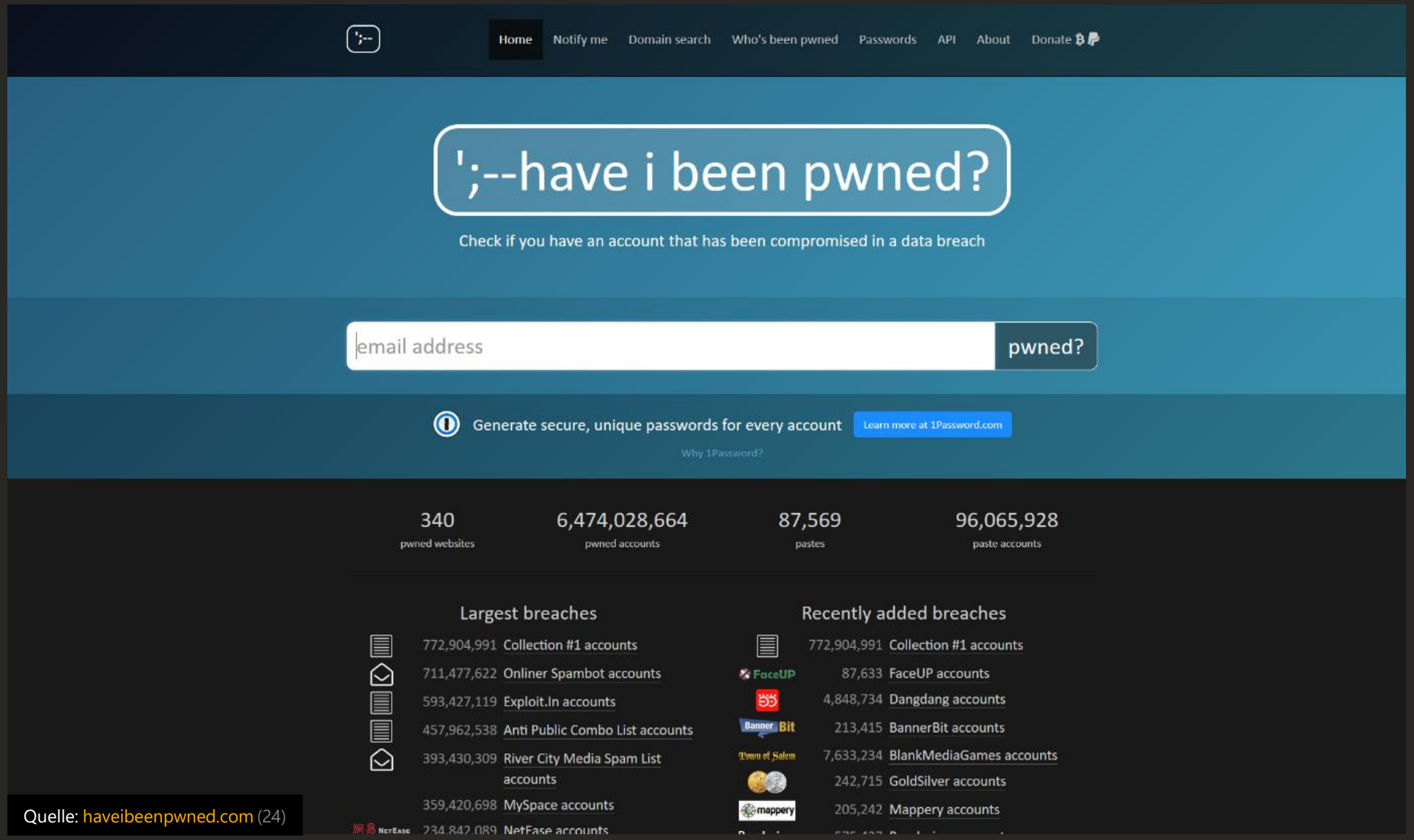
Sichere Passwörter - Passwortkarten

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

PRAXIS Passwortsicherheit



Quelle: haveibeenpwned.com (24)

Cyber Security

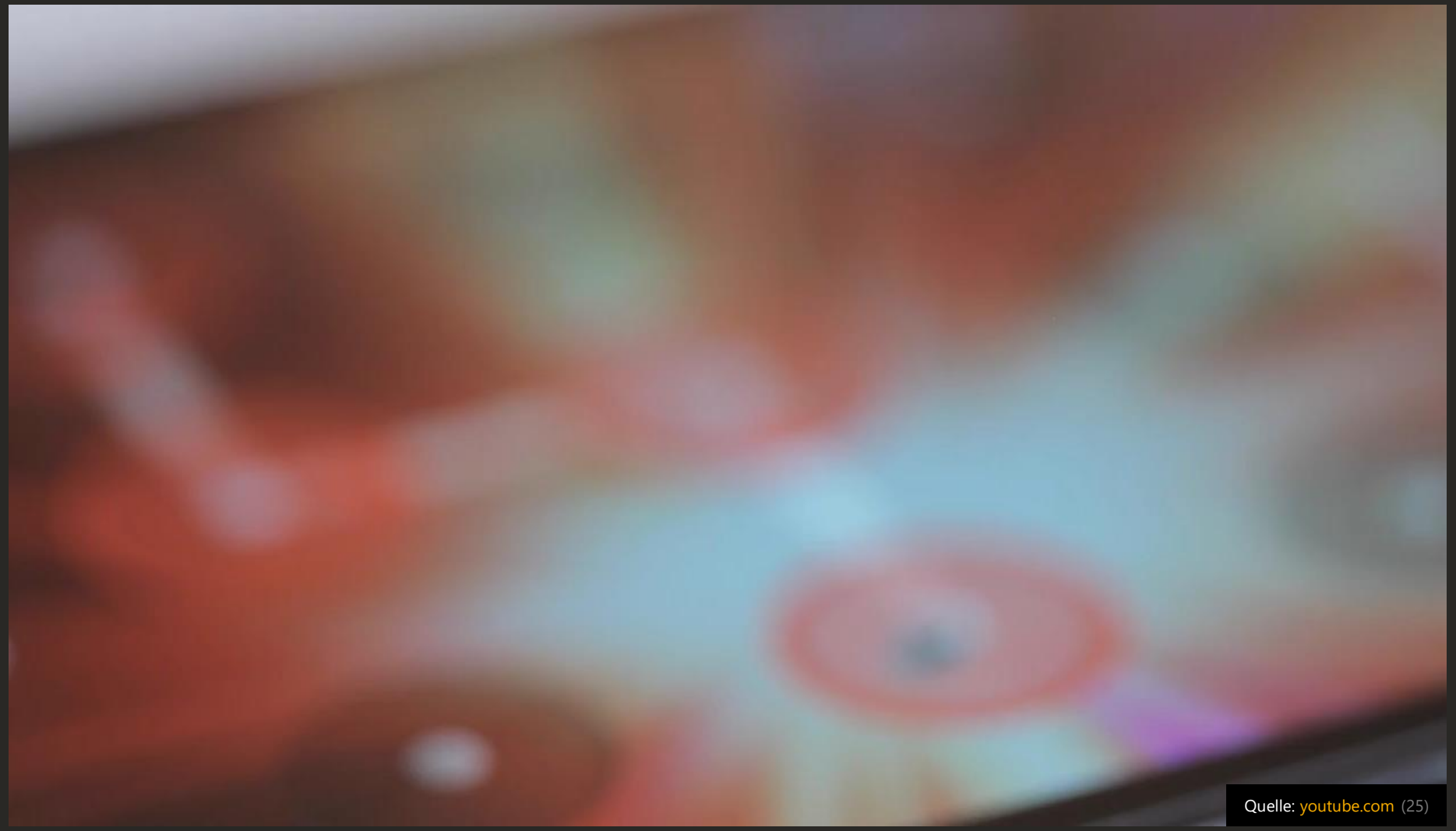
Social Engineering

Passwortsicherheit
- Öffentliche Passwörter
- Angriffe auf Passwörter
- Sicherer Umgang mit Passwörtern

Datenschutz

IT Security Hardware

Sperrmuster - Brute-Force



Quelle: youtube.com (25)

Cyber Security

Social Engineering

Passwortsicherheit
Öffentliche Passwörter
Angriffe auf Passwörter
Sicherer Umgang mit Passwörtern

Passwortsicherheit
Faktor Mensch
Passwörter erraten
Brute-Force Methode
Bekannte Passwörter
Komplexität von Passwörtern
Sperrmuster
Sichere Passwörter

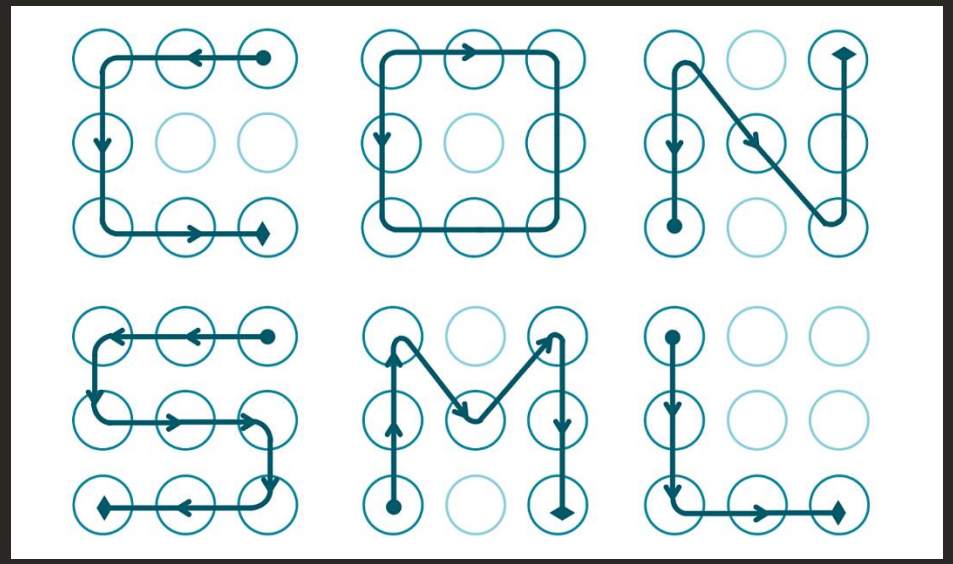
Datenschutz

IT Security Hardware

Web Application Security

Sperrmuster

- Studie von Marte Løge analysierte über 4000 Android Entsperrmuster im Rahmen ihrer Masterthesis.
  - 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 (26)

Sperrmuster – „Pin Code“

Quelle: youtube.com (27)

Cyber Security

Social Engineering

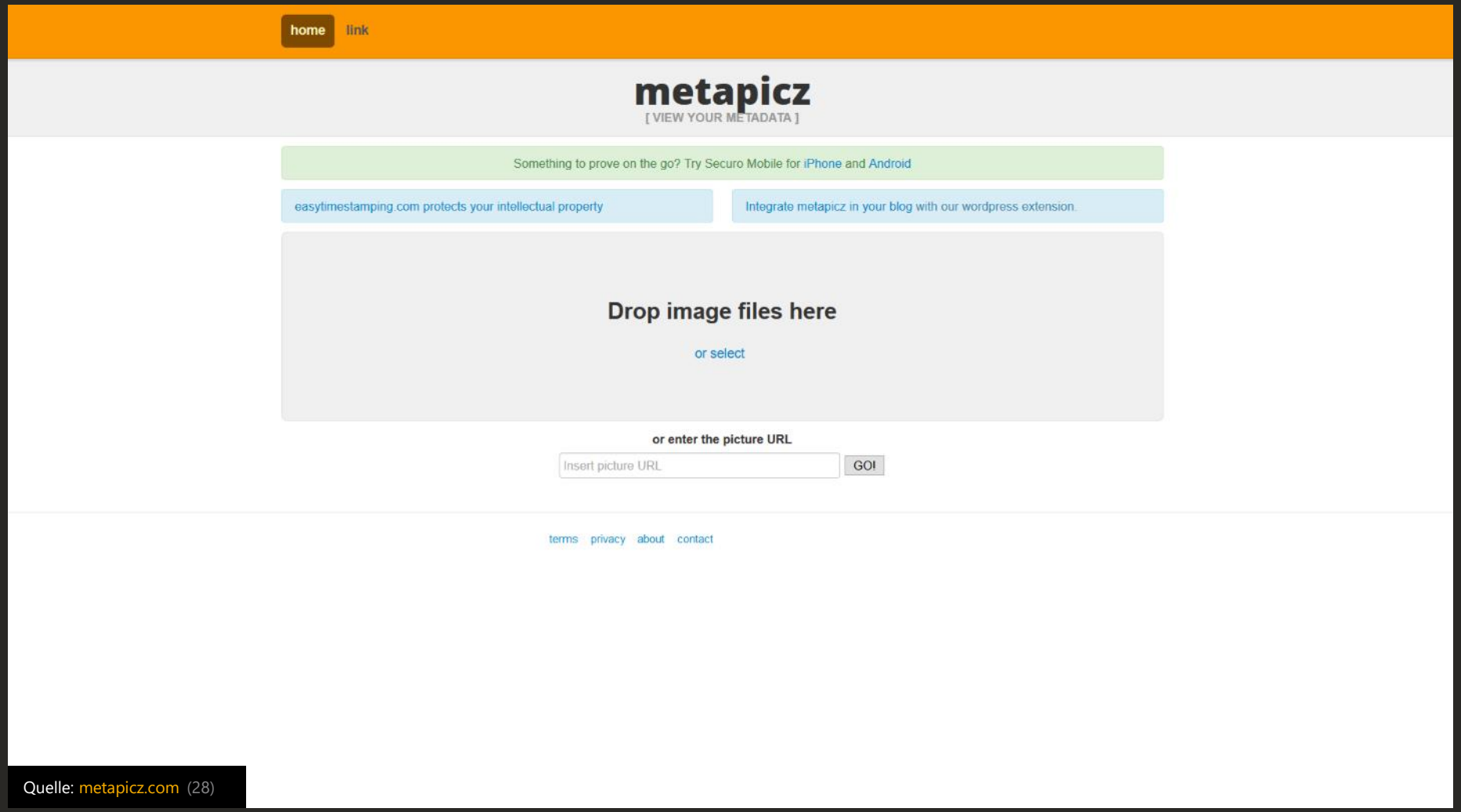
Passwortsicherheit
- Öffentliche Passwörter
- Angriffe auf Passwörter
- Sicherer Umgang mit Passwörtern

Datenschutz

IT Security Hardware

Datenschutz

Versteckte Informationen auslesen



Quelle: metapicz.com (28)

Cyber Security

Social Engineering

Passwortsicherheit

Datenschutz
Versteckte Informationen
Sicher im Web

IT Security Hardware

PRAXIS Positionsdaten von Fotos

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

http://metapicz.com

Datenschutz & Privatsphäre

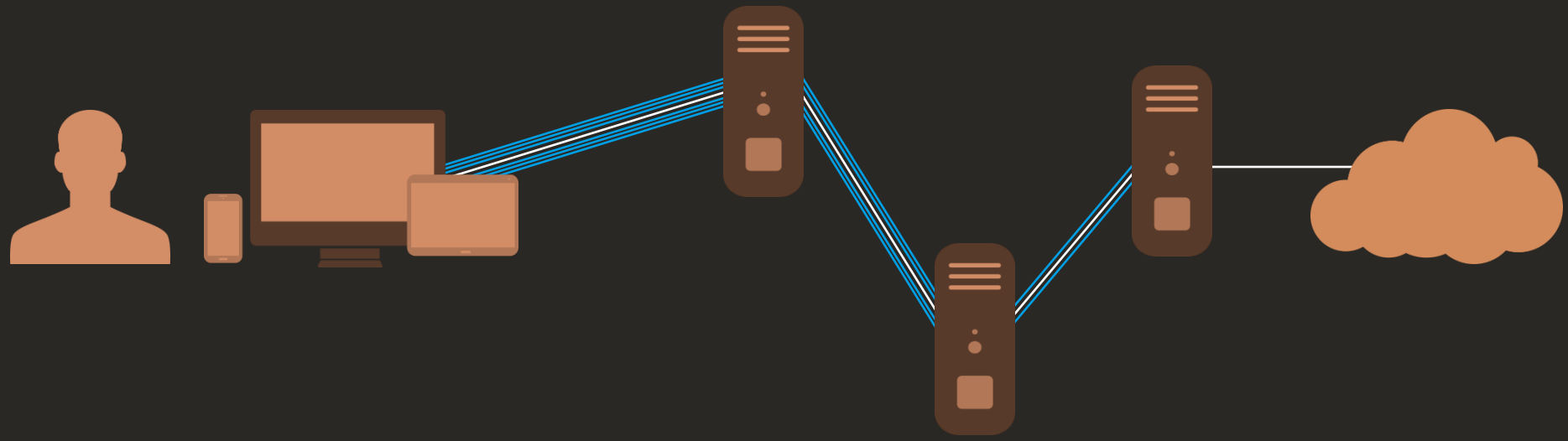
- Das Nutzerverhalten von Internetnutzern wird gezielt und möglichst seitenübergreifend aufgezeichnet.
- Gründe dafür sind die Optimierung von Dienstleitungen, zielgerichtetes Marketing sowie die Profildaten im Allgemeinen.
- Dies lässt sich nicht vollständig vermeiden, jedoch zumindest etwas einschränken,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

PRAXIS Web-Browser absichern

- Starten Sie den portablen Firefox und rufen Sie die Seite http://mybrowserinfo.com auf.
- Installieren Sie die foglenden AddOns:
  - uBlock Origin, Canvas Defender & Random User-Agent
- 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.

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

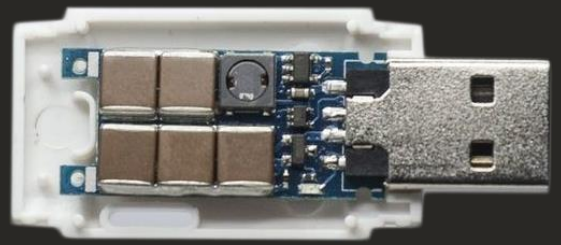


PRAXIS Tor Netzwerk - Darknet

- Starten Sie den TOR-Browser
- 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

IT Security Hardware

Hardware Tools



Quelle: amazon.com (29)

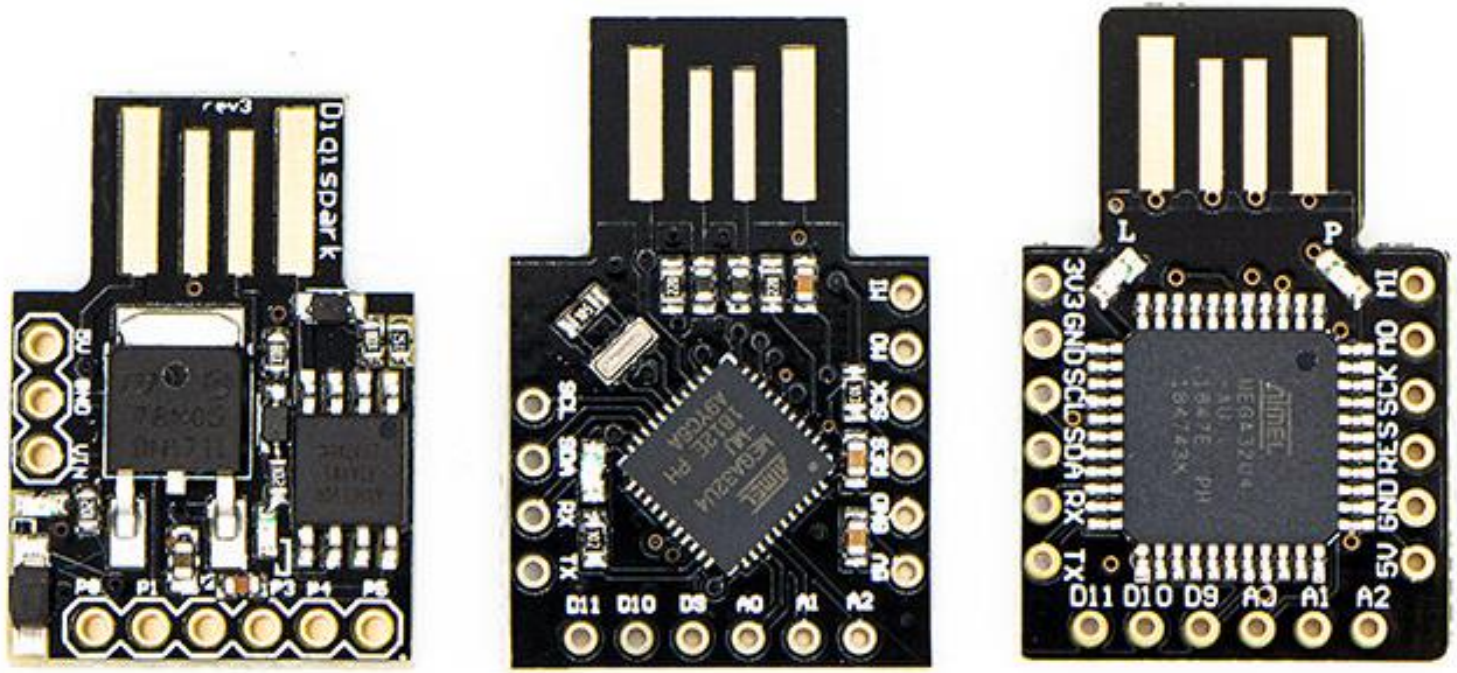
Quelle: hachshop.com (30)

Quelle: amazon.de (31)

Quelle: quora.com (32)

Quelle: pki-electronic.com (33)

LIVE Hardware Tools



Cyber Security

Social Engineering

Passwortsicherheit

Datenschutz

IT Security Hardware
Hardware Tools

Fragen?
Präsentation online unter: https://scheible.it

Quellen

(1) http://www.heise.de/security/meldung/00000000-Passwort-fuer-US-Atomraketen-2060077.html, abgerufen am 24.09.2020

(2) http://www.zeit.de/politik/ausland/2016-05/us-militaer-pcs-technologie-veraltet-rechnungshof, abgerufen am 24.09.2020

(3) http://www.heise.de/security/meldung/IP-Kameras-von-Aldi-als-Sicherheits-GAU-3069735.html, abgerufen am 24.09.2020

(4) http://google.de/, abgerufen am 24.09.2020

(5) https://www.exploit-db.com/google-hacking-database, abgerufen am 24.09.2020

(6) https://shodan.io/, abgerufen am 24.09.2020

(7) https://www.gdata.de/ratgeber/was-ist-eigentlich-die-geschichte-der-malware, abgerufen am 24.09.2020

(8) https://de.wikipedia.org/wiki/AIDS_(Schadprogramm), abgerufen am 24.09.2020

(9) https://www.gdata.de/ratgeber/was-ist-eigentlich-die-geschichte-der-malware, abgerufen am 24.09.2020

(10) https://de.wikipedia.org/wiki/Locky, abgerufen am 24.09.2020

(11) https://www.youtube.com/watch?v=5M9k7wfiWiI, abgerufen am 24.09.2020

(12) https://www.computerworld.com/article/3105001/security/hackers-demonstrated-first-ransomware-for-iot-thermostats-at-def-con.html, abgerufen am 24.09.2020

(13) http://pics-for-fun.com/wonder-what-the-code-could-be/, abgerufen am 24.09.2020

(14) https://de.pinterest.com/pin/3025924727584002/, abgerufen am 24.09.2020

(15) http://www.spiegel.de/schulspiegel/schulfrei-in-niedersachsen-wegen-gefaelschter-e-mail-a-1071105.html, abgerufen am 24.09.2020

(16) http://www.heise.de/newsticker/meldung/Gefaengnisausbruch-mittels-E-Mail-Betrug-2587303.html, abgerufen am 24.09.2020

(17) http://clonezone.link, abgerufen am 24.09.2020

Quellen

(18) https://www.wiwo.de/erfolg/management/falsche-chefs-zocken-firmen-ab-den-enkeltrick-gibts-auch-bei-unternehmen/12201572.html, abgerufen am 24.09.2020

(19) http://www.heise.de/newsticker/meldung/Passwoerter-im-TV-Bild-Spekulationen-zu-TV5-Attacke-2598298.html, abgerufen am 24.09.2020

(20) https://www.vice.com/en_us/article/qvwmx5/the-agency-that-messed-up-hawaiis-nuclear-alert-keeps-passwords-on-post-its-vgtrn, abgerufen am 24.09.2020

(21) https://www.youtube.com/watch?v=opRMrEfAIiI, abgerufen am 24.09.2020

(22) https://stricture-group.com/files/adobe-top100.txt, abgerufen am 24.09.2020

(23) https://xkcd.com/936/, abgerufen am 24.09.2020

(24) https://haveibeenpwned.com/, abgerufen am 24.09.2020

(25) https://www.youtube.com/watch?v=WFaFL4mAzpQ, abgerufen am 24.09.2020

(26) http://en.wikipedia.org/wiki/Google_hacking, abgerufen am 24.09.2020

(27) https://www.youtube.com/watch?v=brzU7i2sAcY, abgerufen am 24.09.2020

(28) http://metapicz.com/, abgerufen am 24.09.2020

(29) http://www.amazon.com/KeyGrabber-USB-KeyLogger-8MB-Black/dp/B004TUBOKW, abgerufen am 24.09.2020

(30) https://hakshop.com/products/usb-rubber-ducky-deluxe, abgerufen am 24.09.2020

(31) https://www.amazon.de/Mobile-Alarmanlage-Quadband-Rückruffunktion-Geräuschaktivierungs-Lautstärke-Schwarz/dp/B00RC7SF8S, abgerufen am 24.09.2020

(32) https://www.quora.com/How-do-USB-killers-work, abgerufen am 24.09.2020

(33) http://www.pki-electronic.com/products/jamming-systems/pocket-jammer/, abgerufen am 24.09.2020