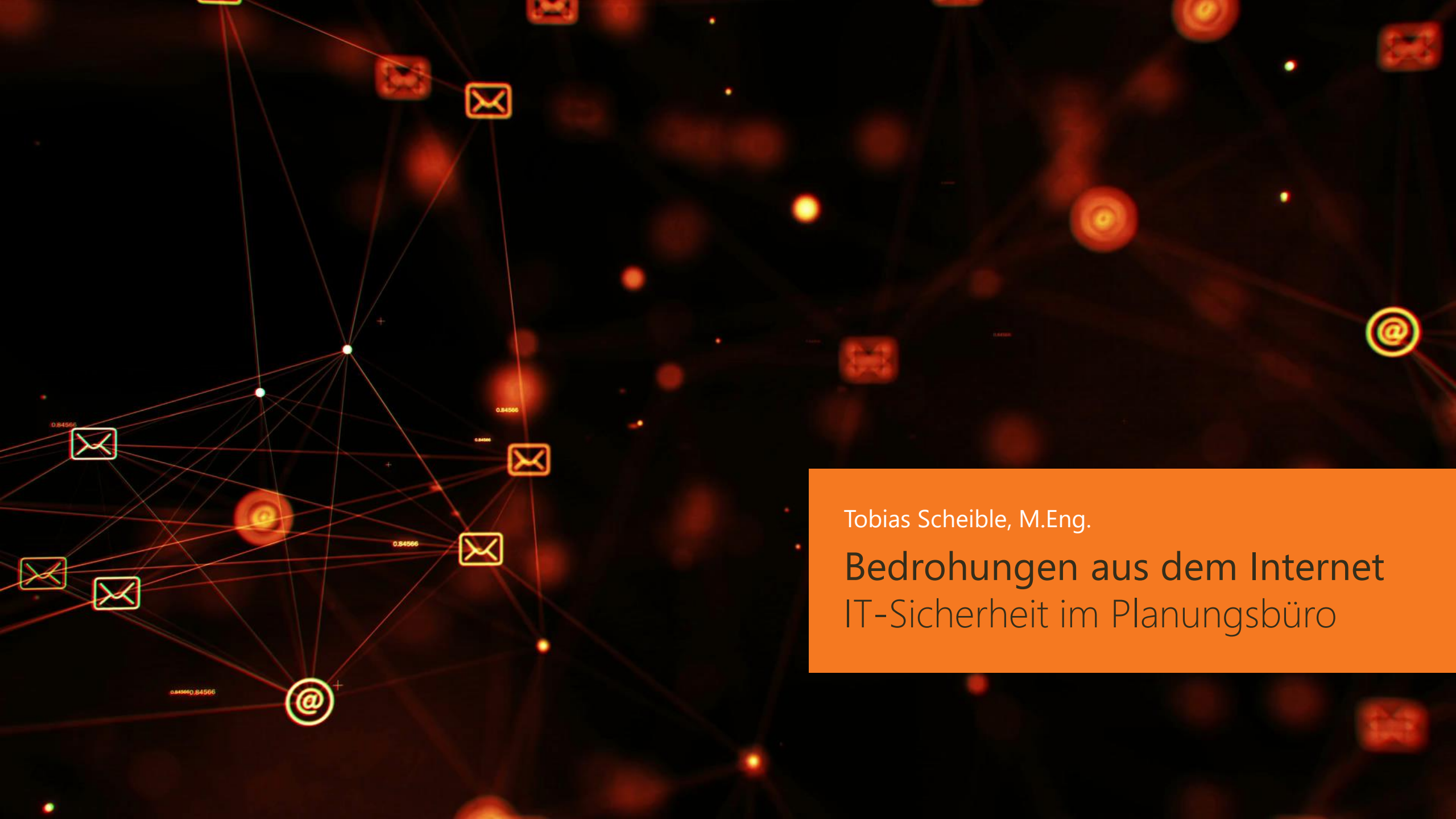


Tobias Scheible, M.Eng.

Bedrohungen aus dem Internet

IT-Sicherheit im Planungsbüro

Tobias Scheible, M.Eng.

Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

- 1999 GeoCities Website, 2000 eigene Domain, 2001 erste Projekte
- 2009 bis 2012: Softwareingenieur im Bereich Web Development
- Seit 2012: Wissenschaftlicher Mitarbeiter an der Hochschule Albstadt-Sigmaringen
  - BMBF gefördertes 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
    - IT Security 2 Bachelorstudiengang IT Security
    - Informationssicherheit Bachelorstudiengang Wirtschaftsinformatik
    - Internettechnologien Hochschulzertifikatsprogramm
    - Cloud Technologies and Cloud Security Architectures Masterstudiengang IT GRC

Agenda

- Cyber Security
  - Pin Code Beispiel
  - IoT Beispielprodukt
  - Spezialisierte Suchmaschine
  - Cybercrime as a Service
- Social Engineering
  - Moderner Gefängnisausbruch
  - CEO Fraud
  - E-Mails fälschen
  - Ransomware
  - AIDS – Erste Ransomware
  - Fallbeispiel Locky
- Passwortsicherheit
  - Faktor Mensch
  - Bekannte Passwörter
  - Gehackte Accounts
  - Passwörter verraten
  - Zwei-Faktor-Authentisierung
  - Passwortmanager
- Hacking Hardware
  - Hardware Tools
  - BadUSB

Cyber Security

000000000

?

Quelle: heise.de (1)

00000000

Launch-Code für die in den USA stationierten Atomraketen

(1962 bis 1977)

Quelle: heise.de (1)

Pin Code Beispiel - Steuerungstechnik

Quelle: zeit.de (2)

IoT Beispielprodukt

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.

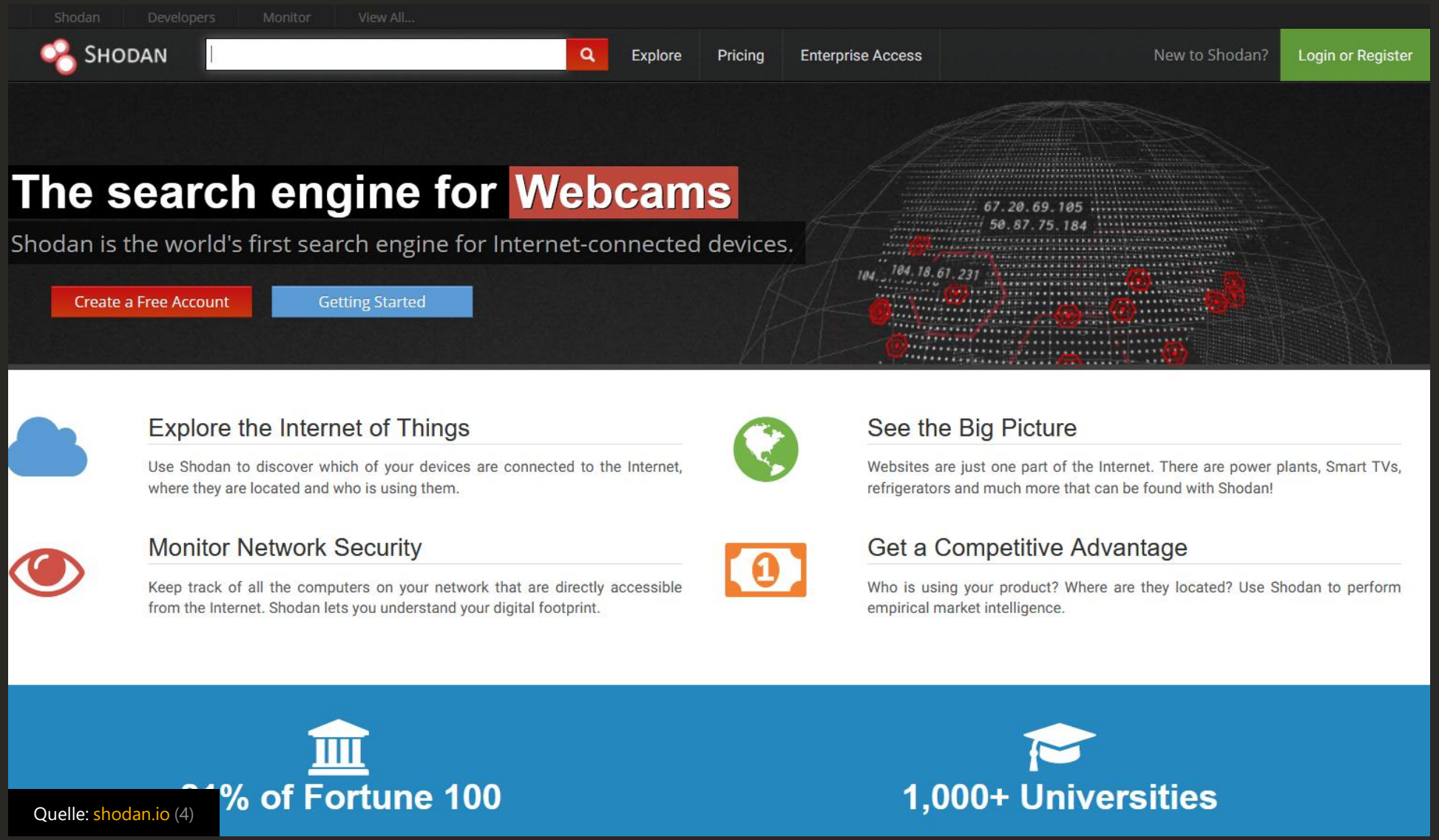
Von Ronald Eikenberg 411

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)

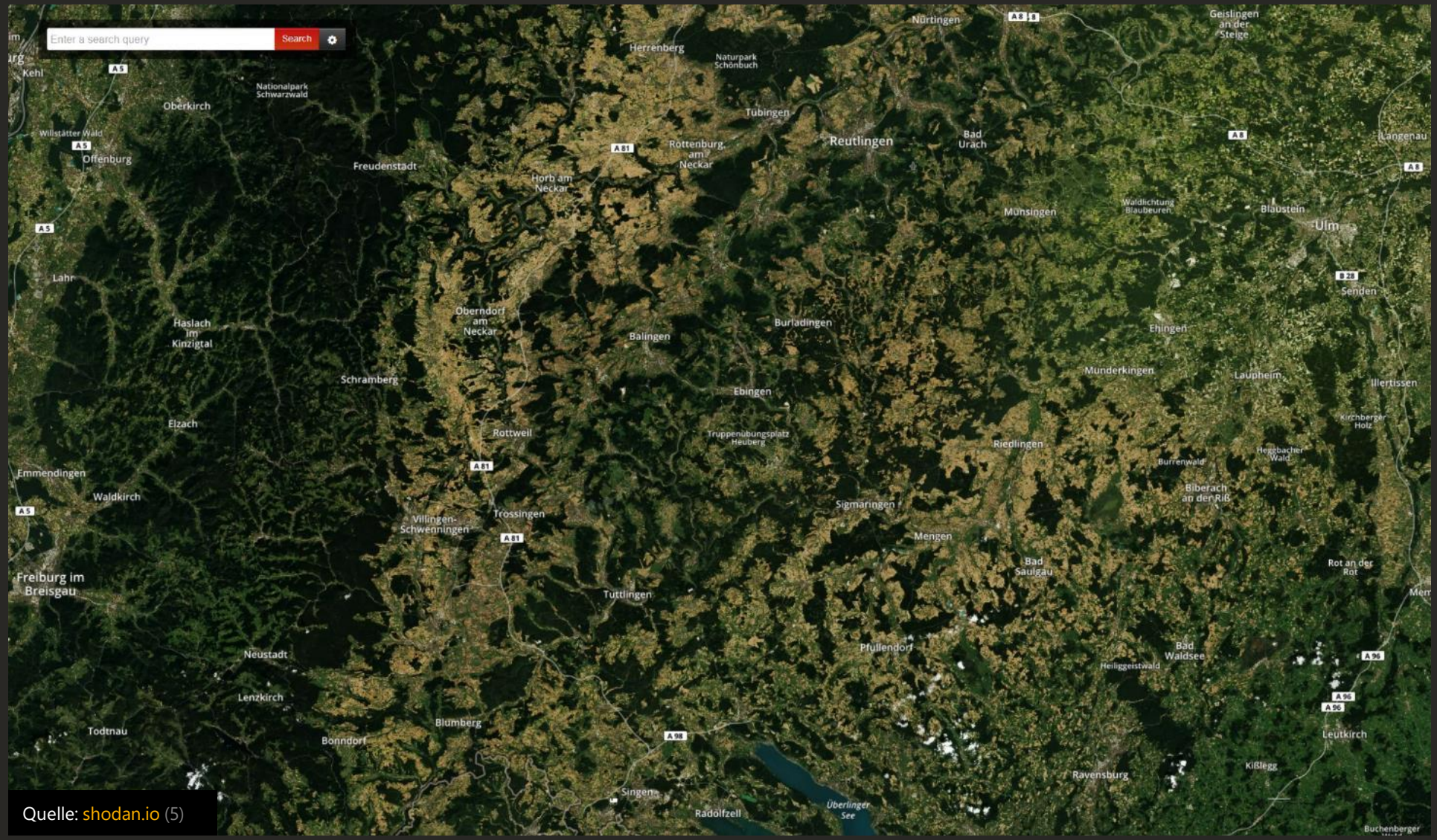
Quelle: heise.de (3)

Spezialisierte Suchmaschine



Quelle: shodan.io (4)

LIVE Spezialisierte Suchmaschine



Quelle: shodan.io (5)

Bedrohungen aus dem Internet
IT-Sicherheit im Planungsbüro

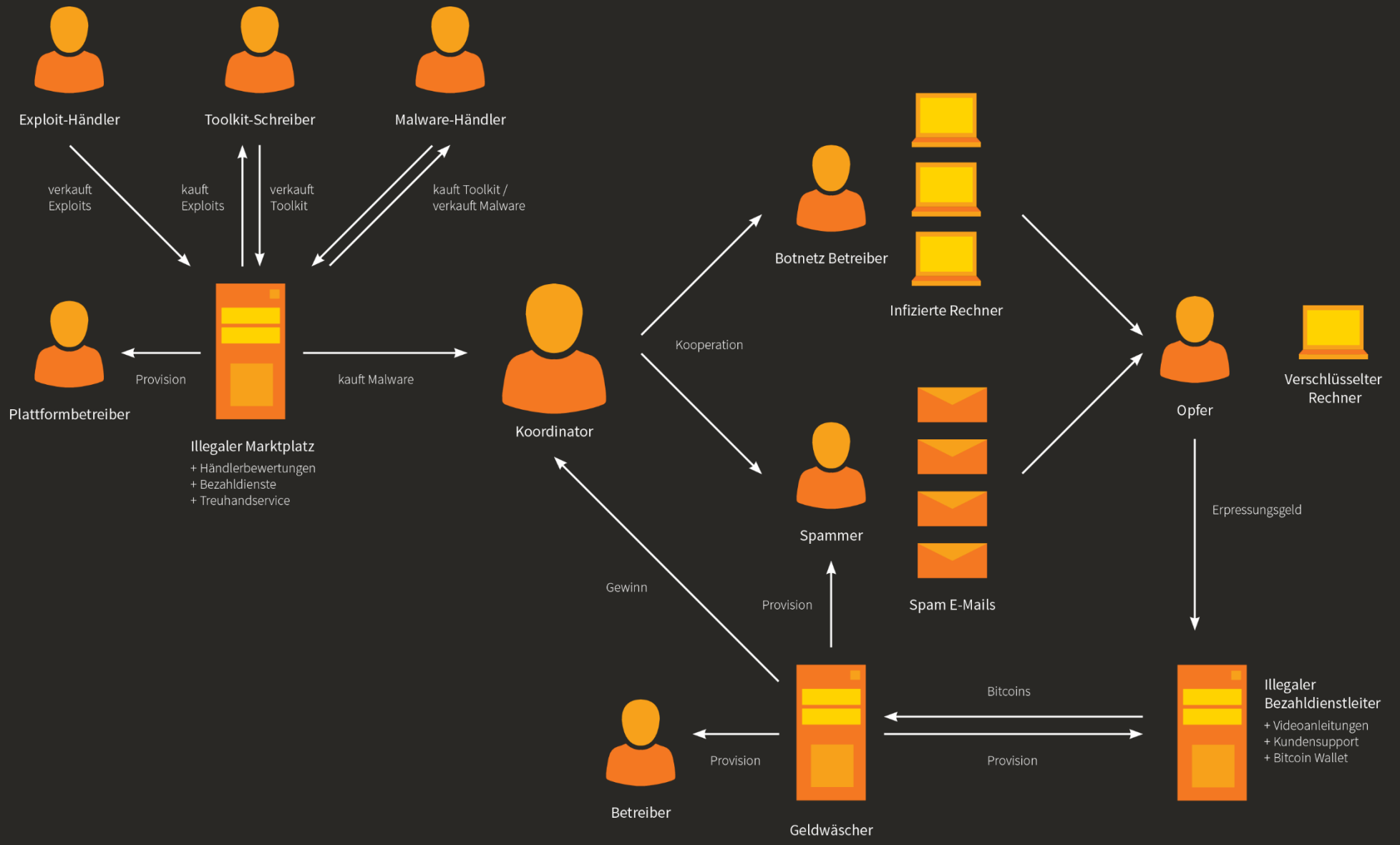
Cyber Security
- Pin Code Beispiel
- IoT Beispielprodukt
- Spezialisierte Suchmaschine
- Cybercrime as a Service

Social Engineering

Passwortsicherheit

Hacking Hardware

Cybercrime as a Service



Cybercrime as a Service

Quelle: youtube.com (6)

Zusatzfolie

Fazit Cyber Security

- Alle Systeme, die online erreichbar sind, können auch gefunden werden. Verschleierung durch komplizierte Links oder Verschleierung der IP-Adresse sind kein Schutz.
- Die Standard-Passwörter von Geräten müssen immer geändert werden.
- Komponenten können sich auch selbstständig mit dem Internet verbinden, daher muss die Konfiguration immer geprüft werden.
- Updates sollten immer zeitnah installiert werden, um Sicherheitslücken schnell zu schließen.

Was ist die häufigste Angriffsmethode?

Ausnutzung von Schwachstellen

A

Physische Attacken

B

Manipulation von Personen

C

Ausnutzung von Fehlern

D

Social Engineering

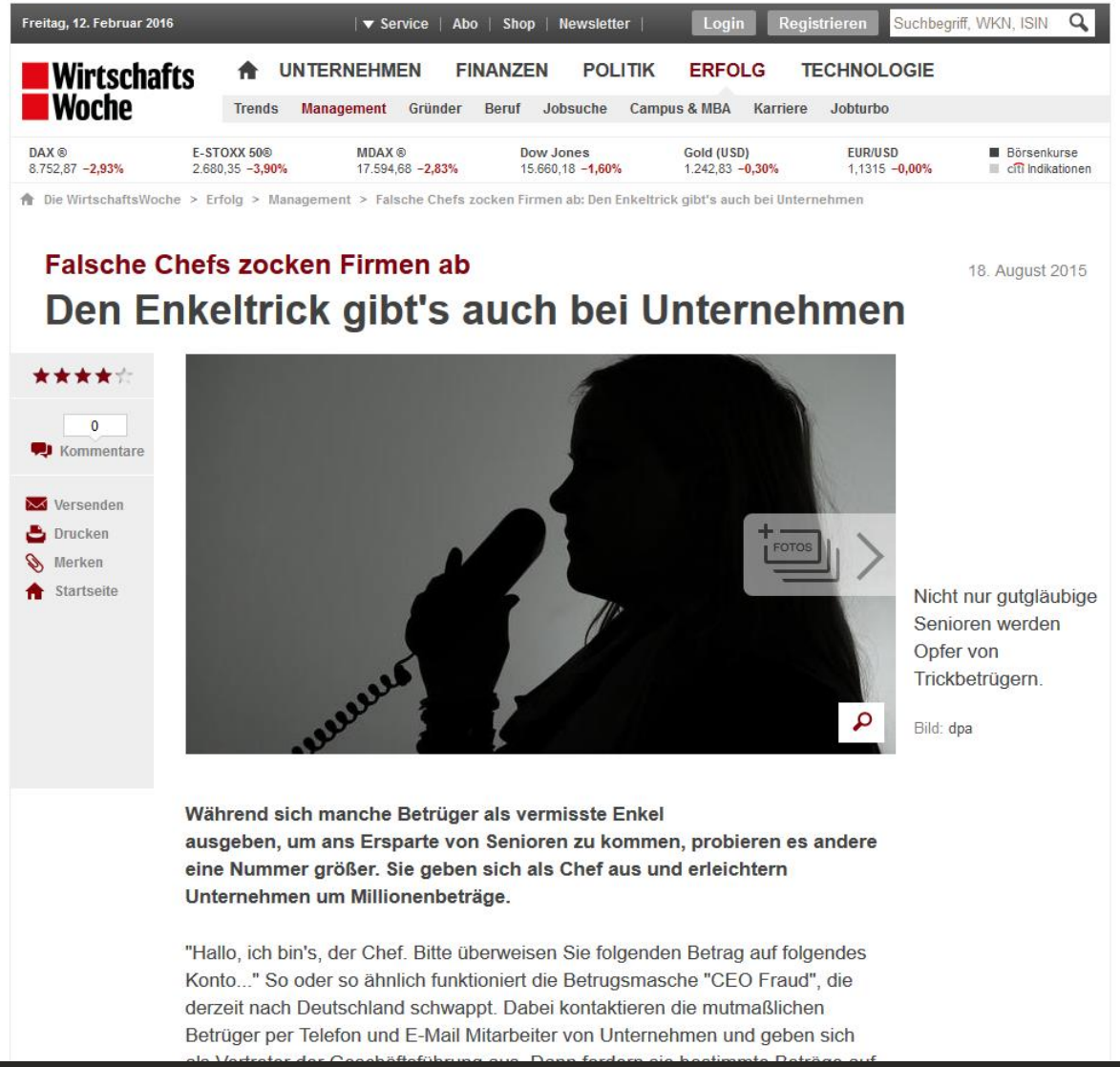
Moderner Gefängnisausbruch

- 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 (7)

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%	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.

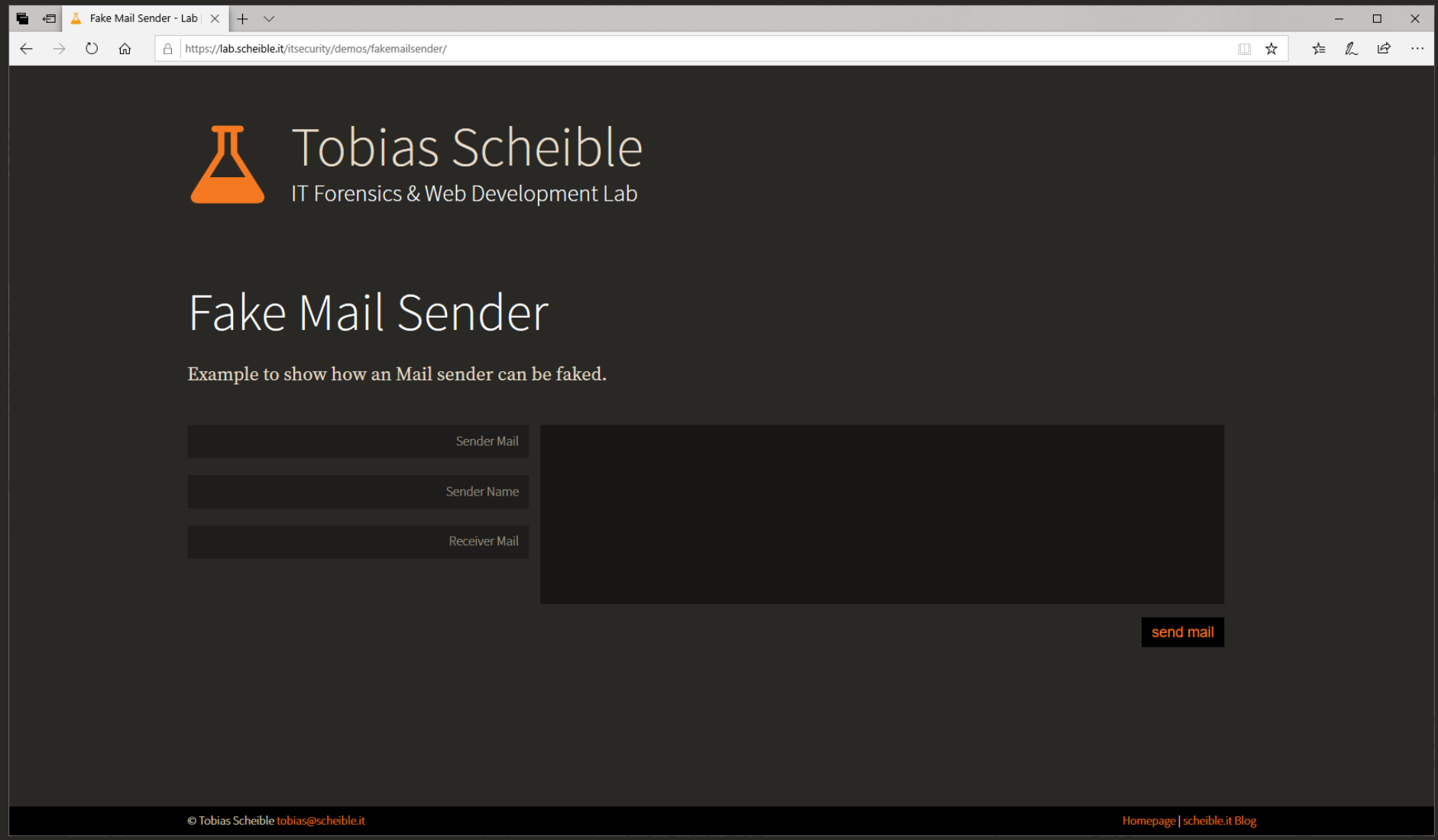
Bild: dpa

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.

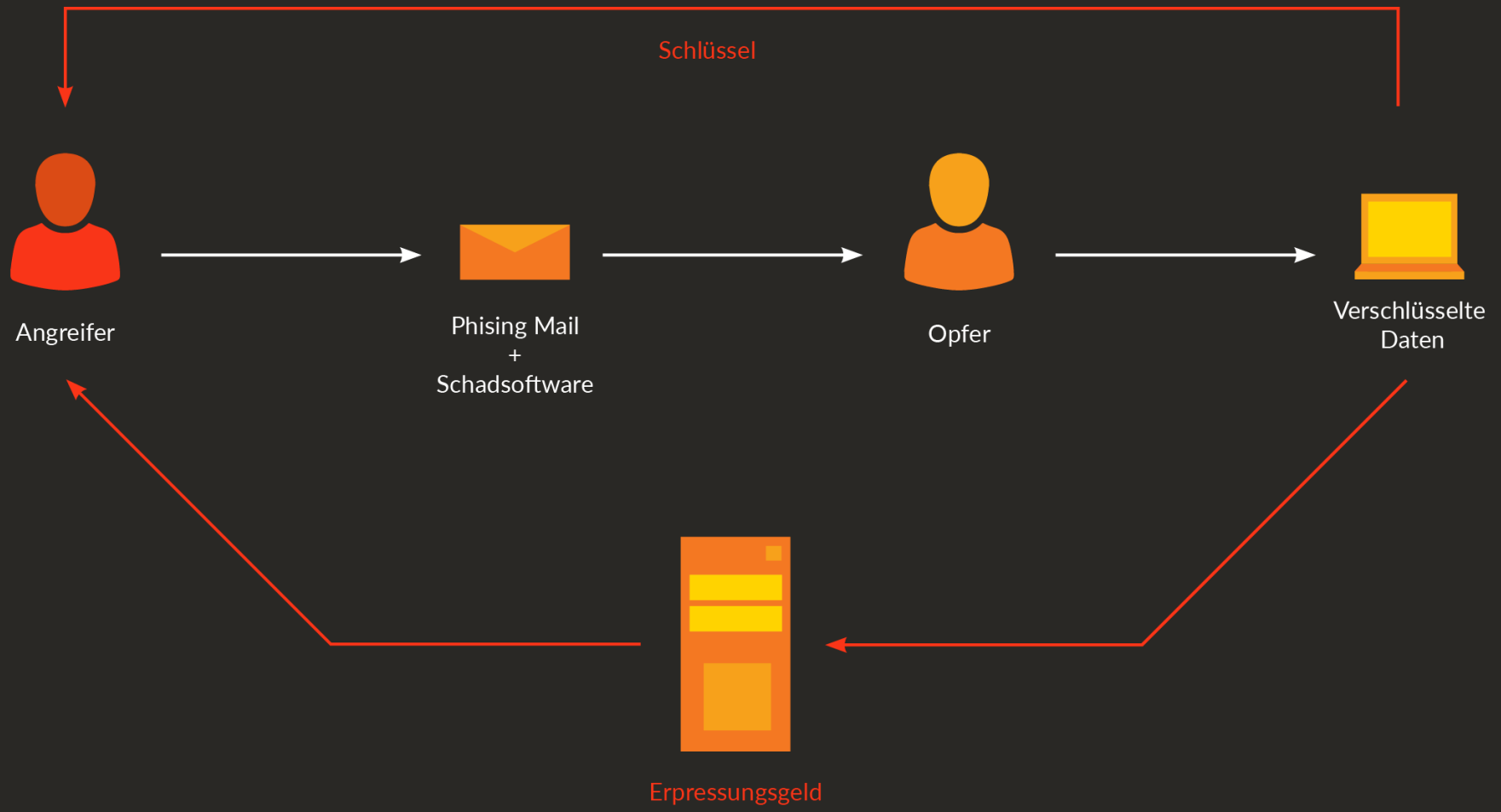
"Hallo, ich bin's, der Chef. Bitte überweisen Sie folgenden Betrag auf folgendes Konto..." So oder so ähnlich funktioniert die Betrugsmasche "CEO Fraud", die derzeit nach Deutschland schwappt. Dabei kontaktieren die mutmaßlichen Betrüger per Telefon und E-Mail Mitarbeiter von Unternehmen und geben sich

Quelle: wiwo.de (8)

LIVE E-Mails fälschen

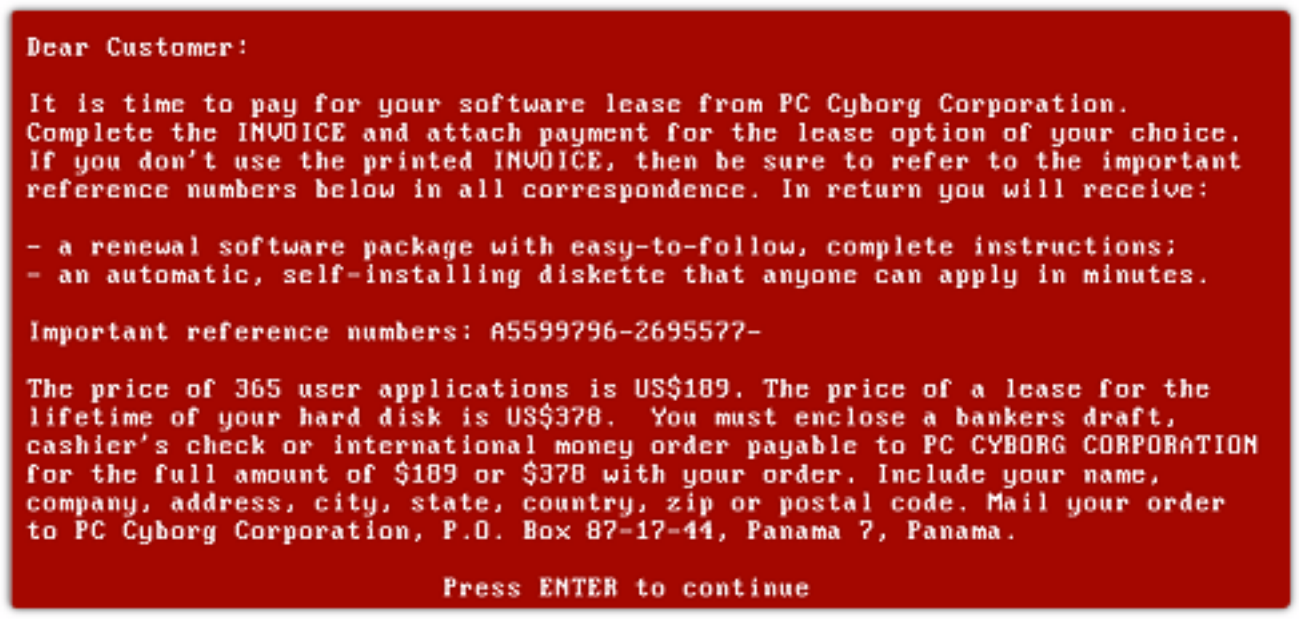


Ransomware



AIDS – Erste Ransomware

- 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 (9)

Fallbeispiel 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)

Zusatzfolie

FAZIT Social Engineering

- Informationen im Web, aber auch SMS-Nachrichten und Telefonnummern, können sehr einfach gefälscht werden.
- E-Mails können sehr einfach manipuliert werden und vorhandene Konversationen können von Angreifern aufgegriffen werden.
- Definierte Prozesse für alle Abteilungen, insbesondere mit Schnittstellen nach außen (Personalabteilung, Verkauf, etc.).
- Sensibilisierung der Mitarbeiter/innen mit Schulungen über Social Engineering-Strategien und –Methoden.

Passwortsicherheit

Faktor Mensch

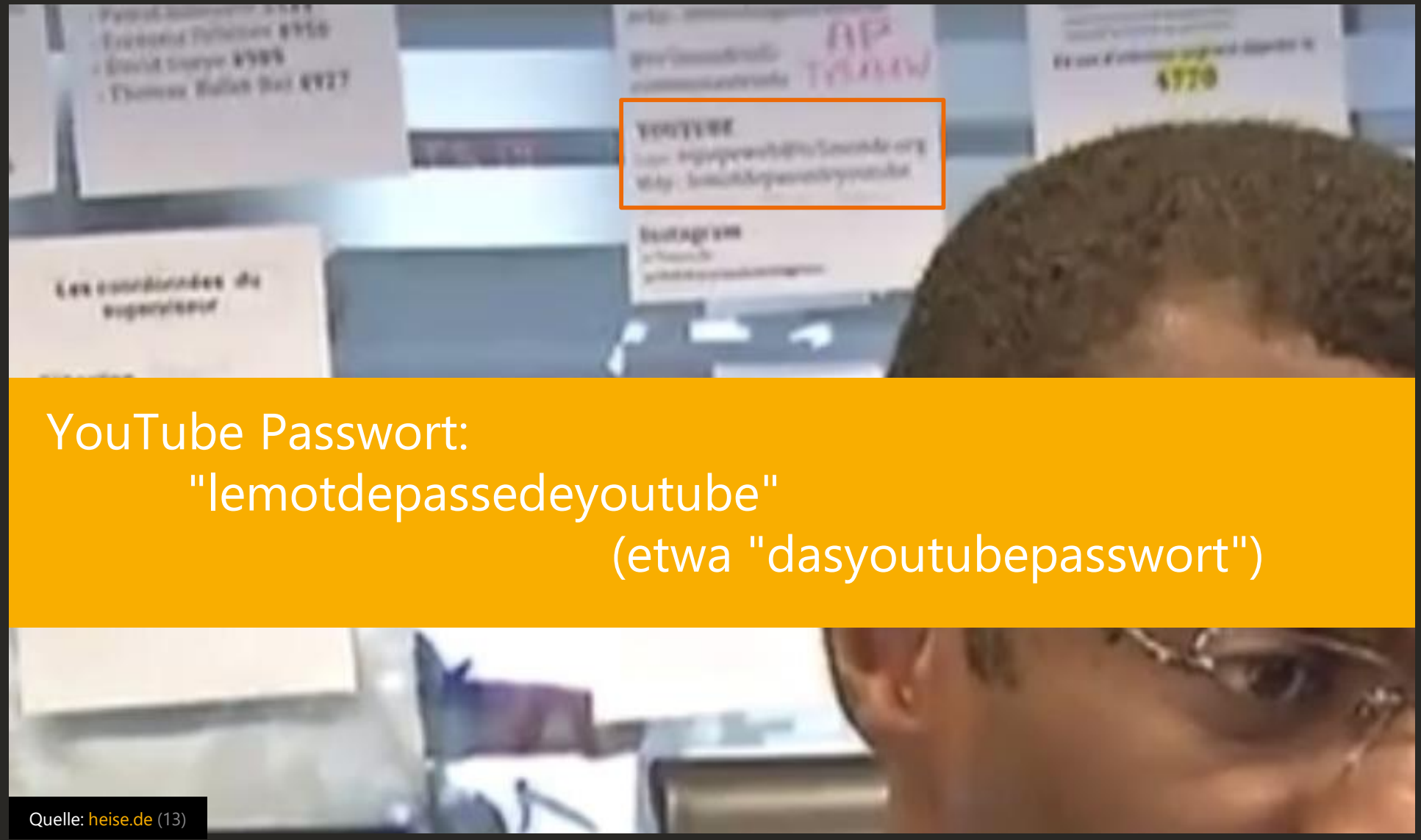
Quelle: pics-for-fun.com (11)

Quelle: de.pinterest.com (12)

Faktor Mensch

Quelle: heise.de (13)

Faktor Mensch

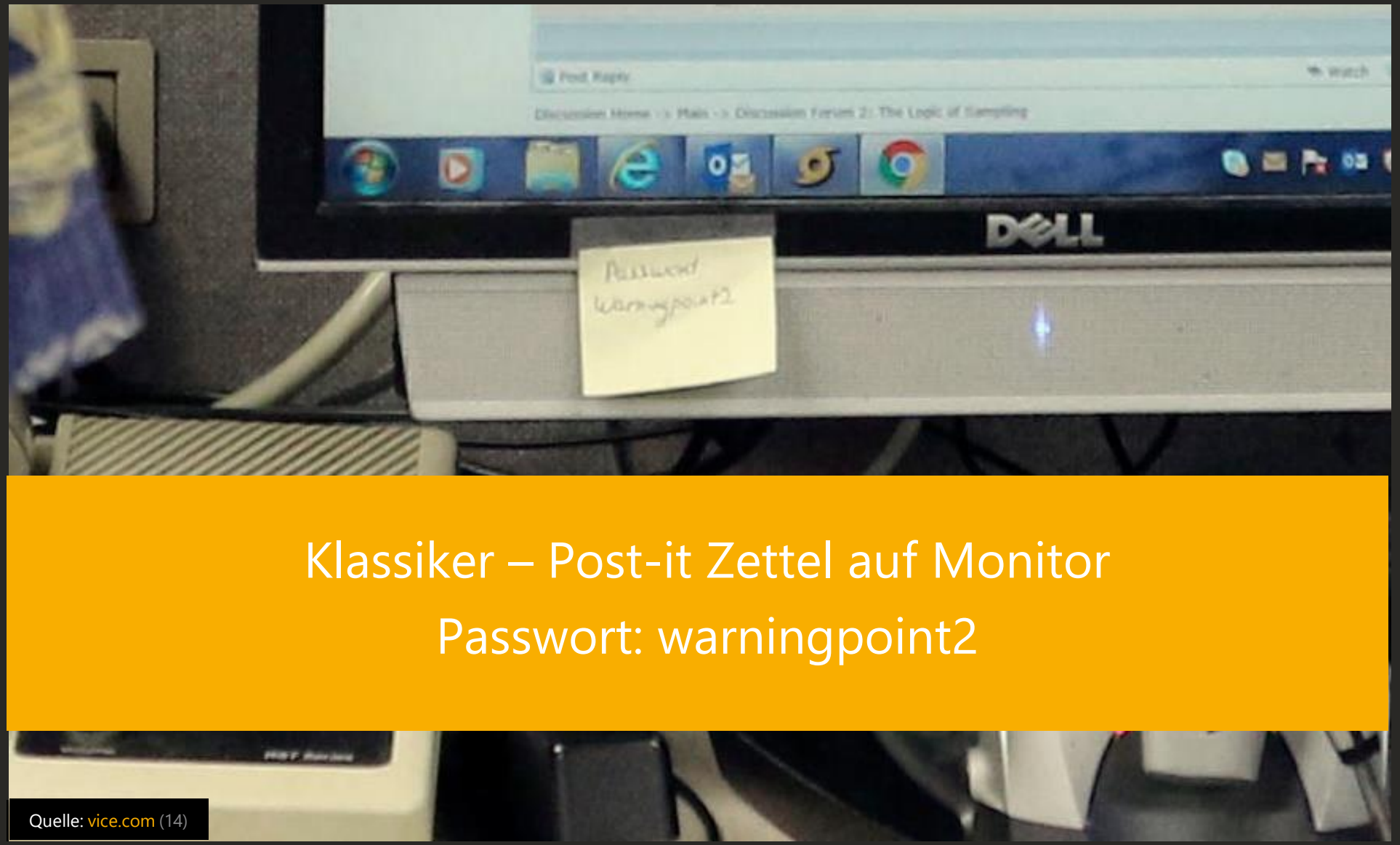


Quelle: heise.de (13)

Faktor Mensch

Quelle: vice.com (14)

Faktor Mensch

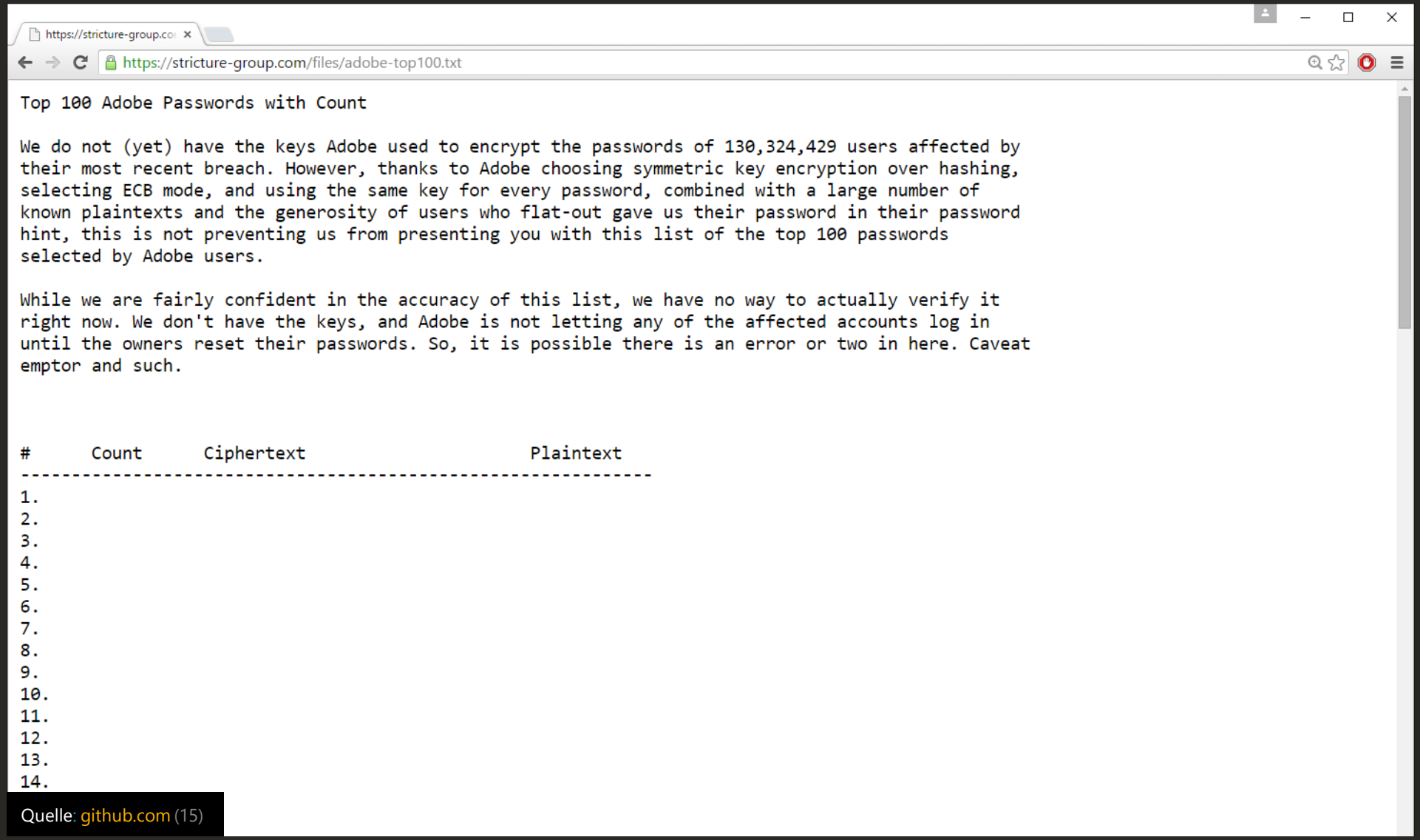


Klassiker – Post-it Zettel auf Monitor

Passwort: warningpoint2

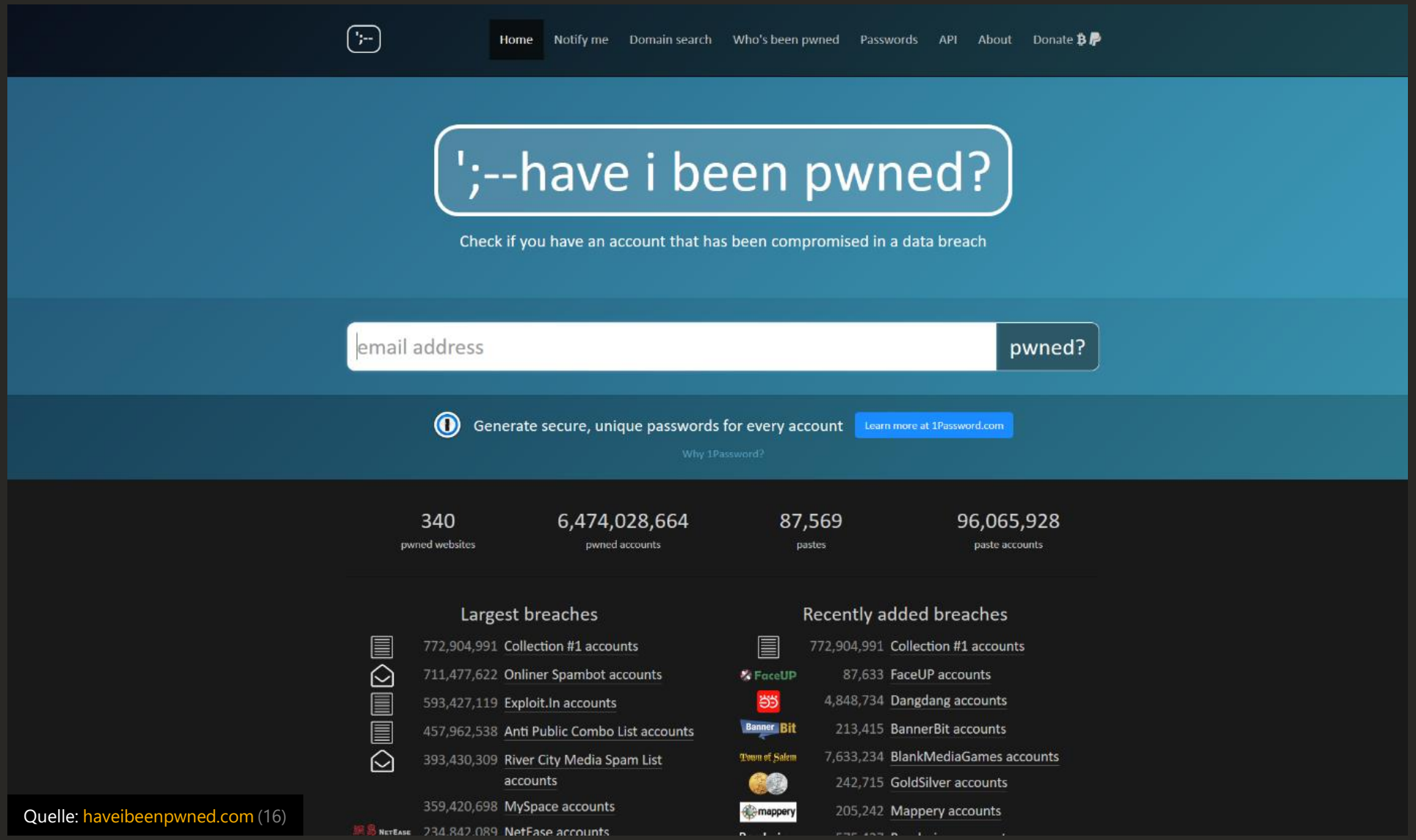
Quelle: vice.com (14)

Bekannte Passwörter



Quelle: github.com (15)

LIVE Gehackte Accounts



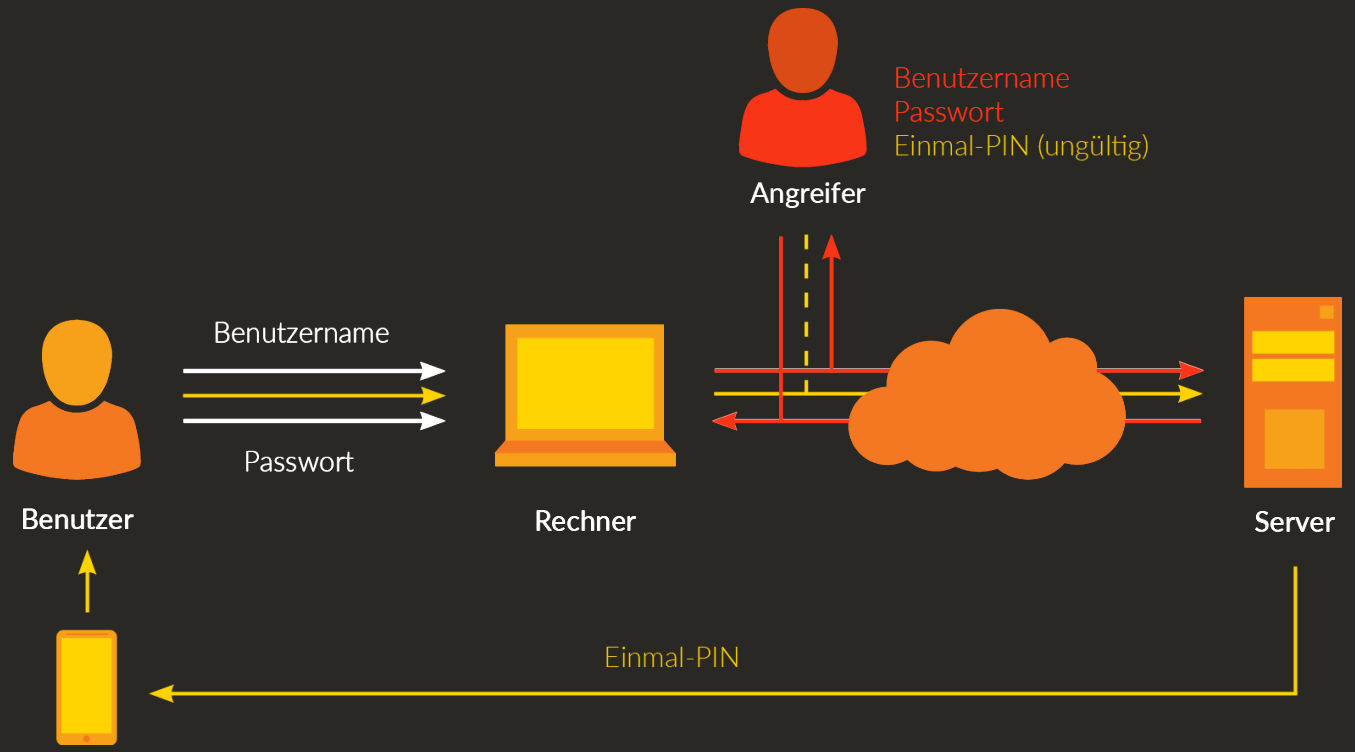
Quelle: haveibeenpwned.com (16)

Passwörter verraten

Quelle: youtube.com (17)

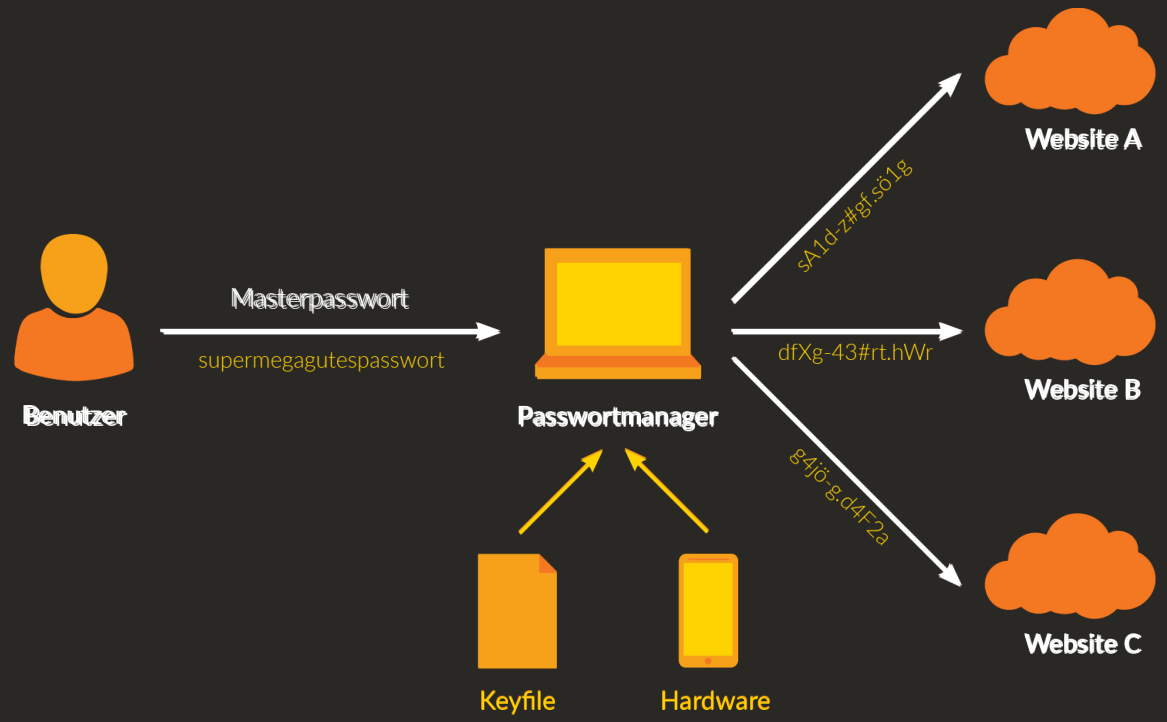
Zwei-Faktor-Authentisierung

- 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)



Passwortmanager

- 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, …)



Zusatzfolie

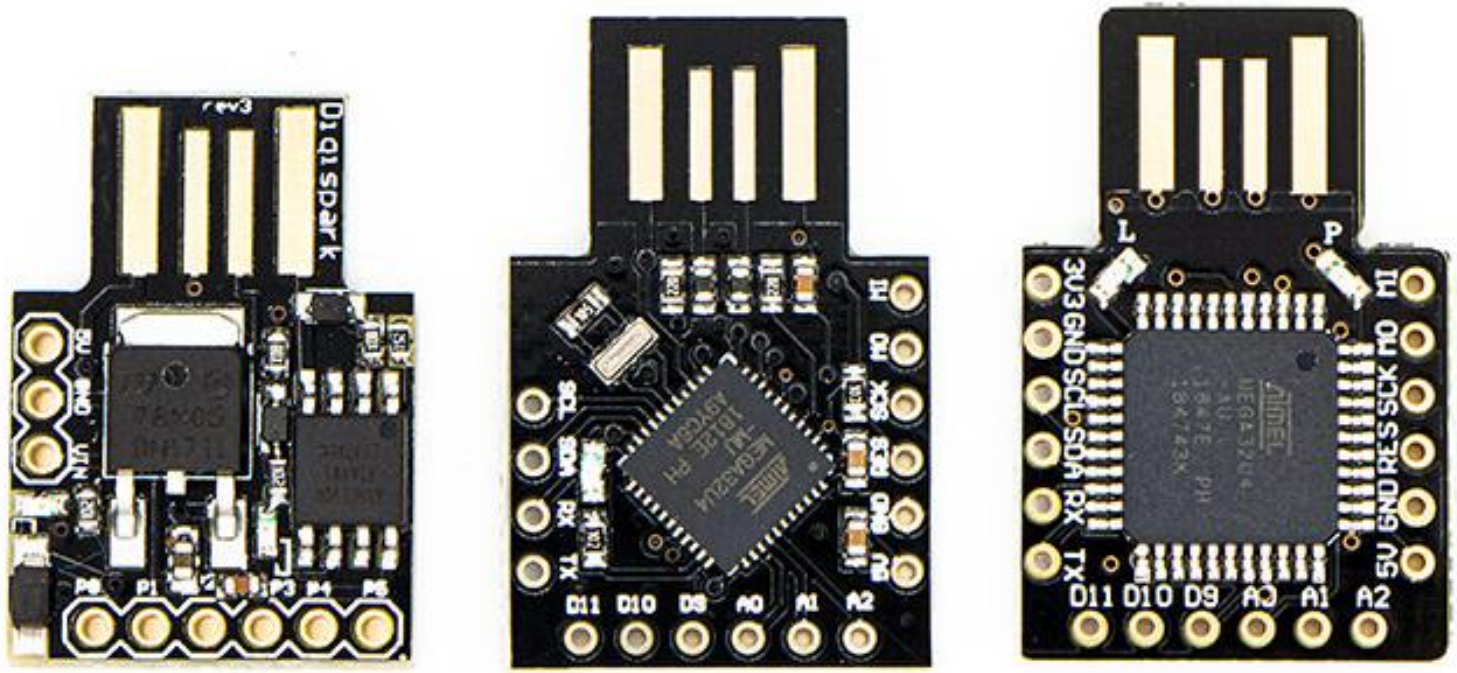
Fazit Passwortsicherheit

- 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, wenn möglich, eine Zwei-Faktor-Authentifizierung.

Hacking Hardware

Hardware Tools

LIVE BadUSB



Zusatzfolie

FAZIT Hacking Hardware

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


Fragen?
Präsentation 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 19.11.2019

2) Mit Floppy Disks Atombomben überwachen, http://www.zeit.de/politik/ausland/2016-05/us-militaer-pcs-technologie-veraltet-rechnungshof, abgerufen am 19.11.2019

3) IP-Kameras von Aldi als Sicherheits-GAU , http://www.heise.de/security/meldung/IP-Kameras-von-Aldi-als-Sicherheits-GAU-3069735.html, abgerufen am 19.11.2019

4) Shodan, https://shodan.io/, abgerufen am 19.11.2019

5) Shodan Maps, https://maps.shodan.io, abgerufen am 19.11.2019

6) Anuncio - gwapo's, https://www.youtube.com/watch?v=5M9k7wfiWiI, abgerufen am 19.11.2019

7) Gefängnisausbruch mittels E-Mail-Betrug, http://www.heise.de/newsticker/meldung/Gefaengnisausbruch-mittels-E-Mail-Betrug-2587303.html, abgerufen am 19.11.2019

8) 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 19.11.2019

9) AIDS (Schadprogramm), https://de.wikipedia.org/wiki/AIDS_(Schadprogramm), abgerufen am 19.11.2019

10) Locky, https://de.wikipedia.org/wiki/Locky, abgerufen am 19.11.2019

11) Code, http://pics-for-fun.com/wonder-what-the-code-could-be/, abgerufen am 19.11.2019

12) And the valuables are in the closet on the top shelf in a box marked, https://de.pinterest.com/pin/302592472758400 2/, abgerufen am 19.11.2019

13) 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 19.11.2019

Quellen

14) 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 19.11.2019

15) Top 100 Adobe Passwords with Count, https://github.com/morontt/symfobrute/blob/master/adobe-top100.txt, abgerufen am 02.03.2020

16) Have I Been Pwned, https://haveibeenpwned.com, abgerufen am 19.11.2019

17) What is Your Password?, https://www.youtube.com/watch?v=opRMrEfAIiI, abgerufen am 19.11.2019