Tobias Scheible, M.Eng.

IT Security für Handwerksbetriebe

Kreishandwerkerschaft Sigmaringen

Tobias Scheible, M.Eng.

Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

- 1999 GeoCities Website, 2000 eigene Domain, 2001 Kundenprojekte
- 2009 bis 2012: Softwareingenieur im Bereich Web Development
- Seit 2012: Wissenschaftlicher Mitarbeiter an der Hochschule Albstadt-Sigmaringen
  - Aktuelle & ehemalige Lehrmodule (Auswahl):
    - Netzsicherheit I: IT-Sicherheit von Netzwerken Hochschulzertifikatsprogramm
    - 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
  - E-Mails fälschen
  - Ransomware
  - AIDS – Erste Ransomware
  - Fallbeispiel Locky
- Passwortsicherheit
  - Faktor Mensch
  - Bekannte Passwörter
  - Gehackte Accounts
  - Zwei-Faktor-Authentisierung
  - Passwortmanager
- Hacking Hardware
  - Hardware Tools
  - BadUSB
- Zusammenfassung
  - Angriffsszenarien
  - Maßnahmen

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.

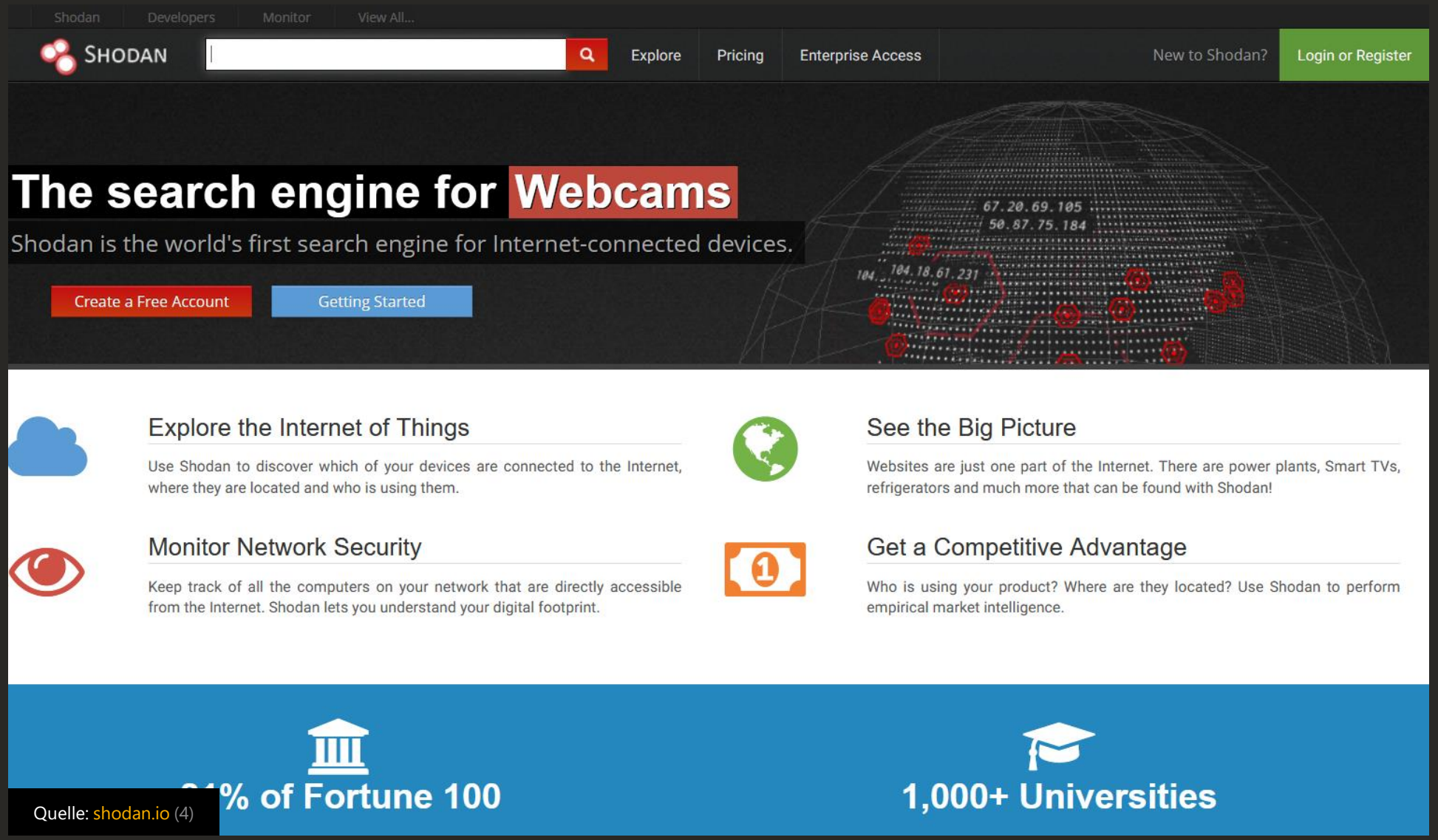
Von Ronald Eikenberg 411

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)

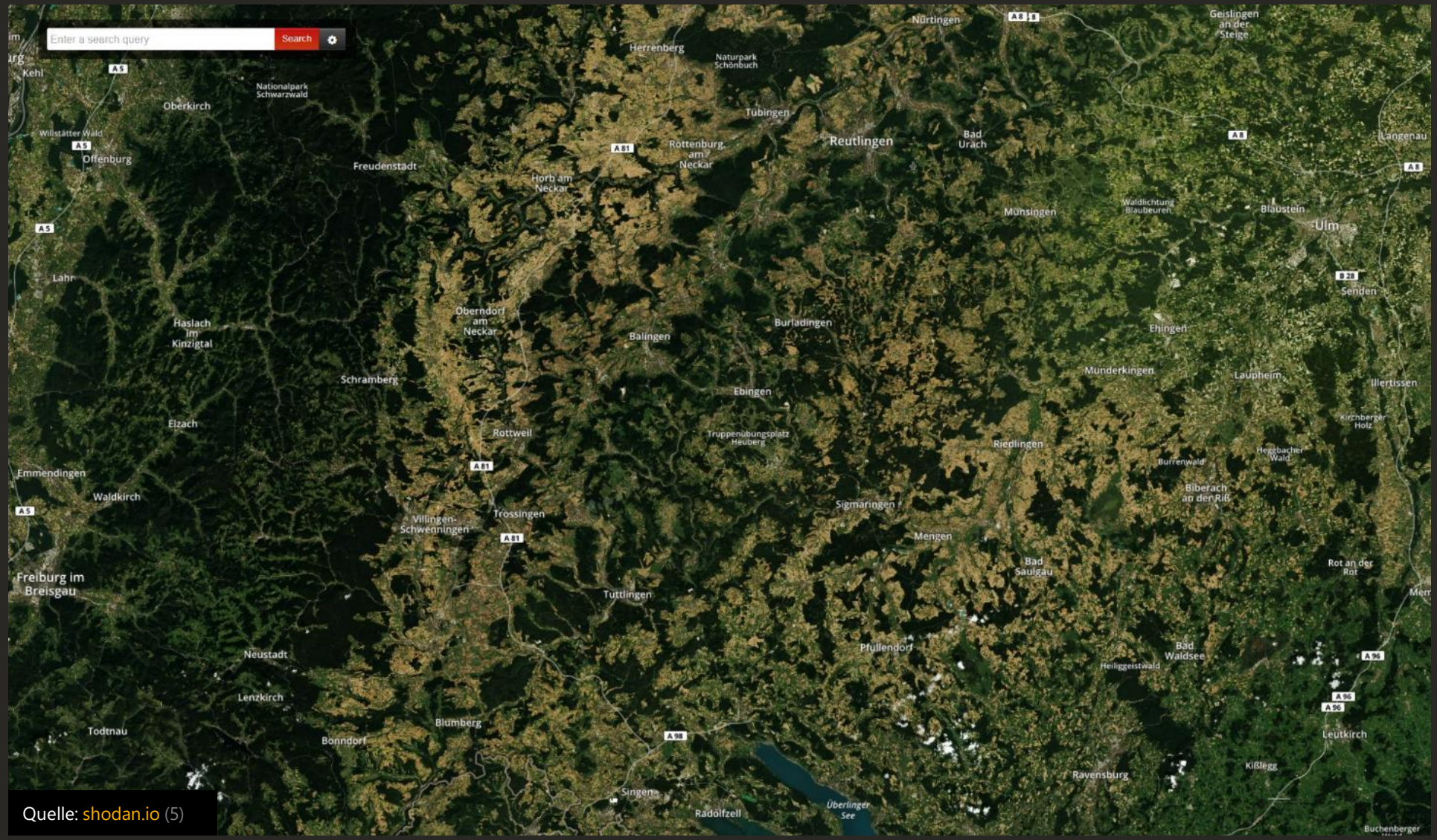
Quelle: heise.de (3)

Spezialisierte Suchmaschine



Quelle: shodan.io (4)

LIVE Spezialisierte Suchmaschine



Quelle: shodan.io (5)

Cybercrime as a Service

Cybercrime as a Service

Quelle: youtube.com (6)

Was ist die häufigste Angriffsmethode?

Ausnutzung von Schwachstellen

A

Physische Attacken

B

Manipulation von Personen

C

Ausnutzung von Fehlern

D

Social Engineering

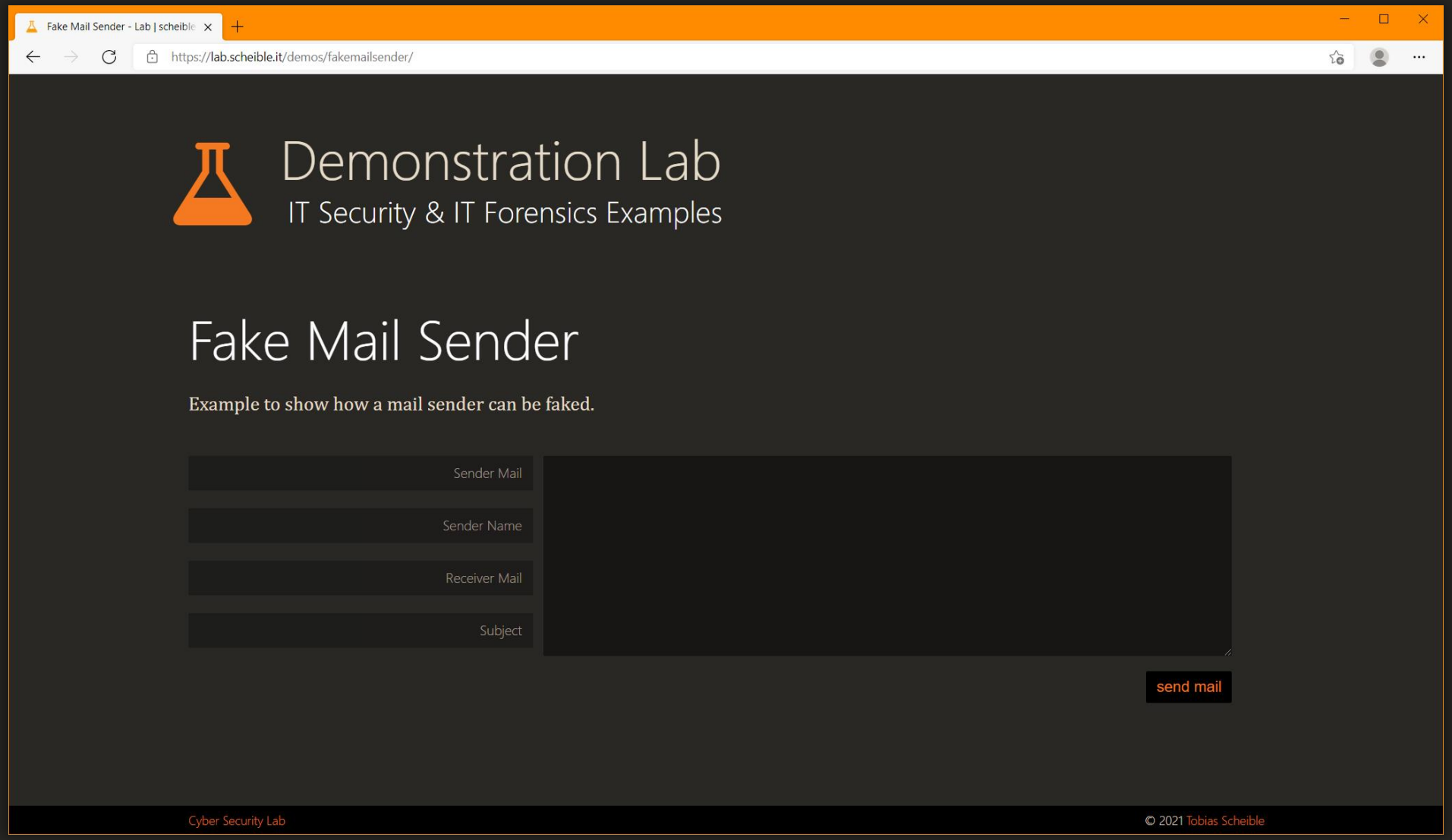
Moderner Gefängnisausbruch

- 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)

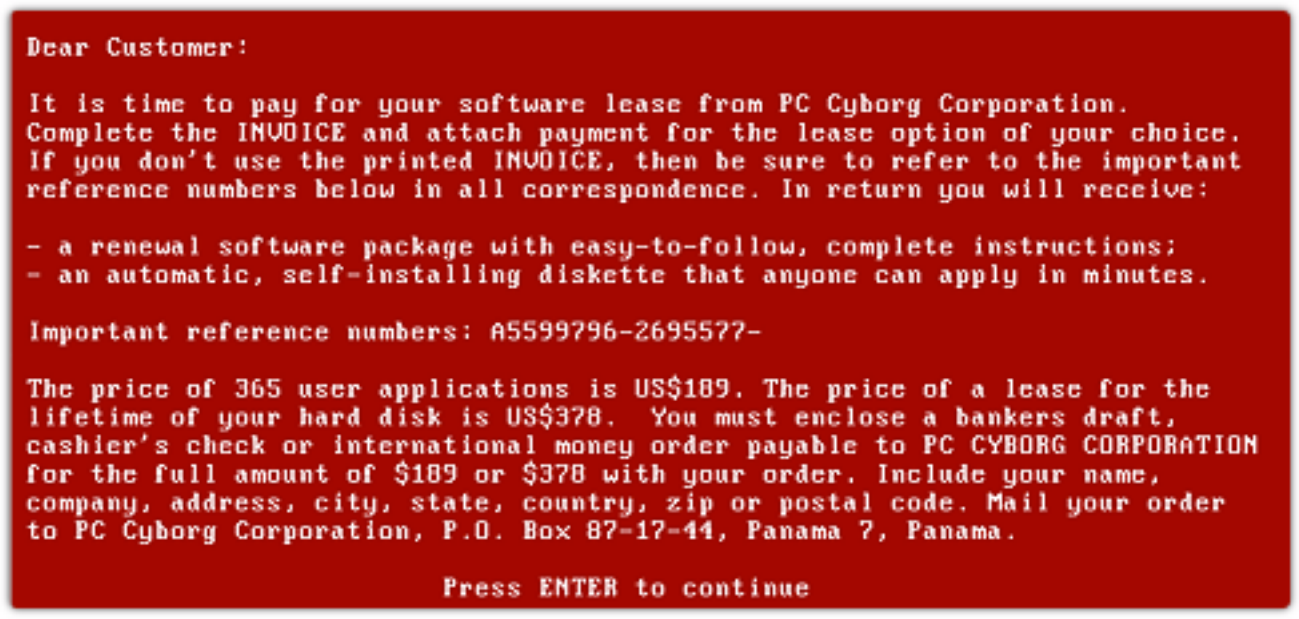
LIVE E-Mails fälschen



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)

Passwortsicherheit

Faktor Mensch

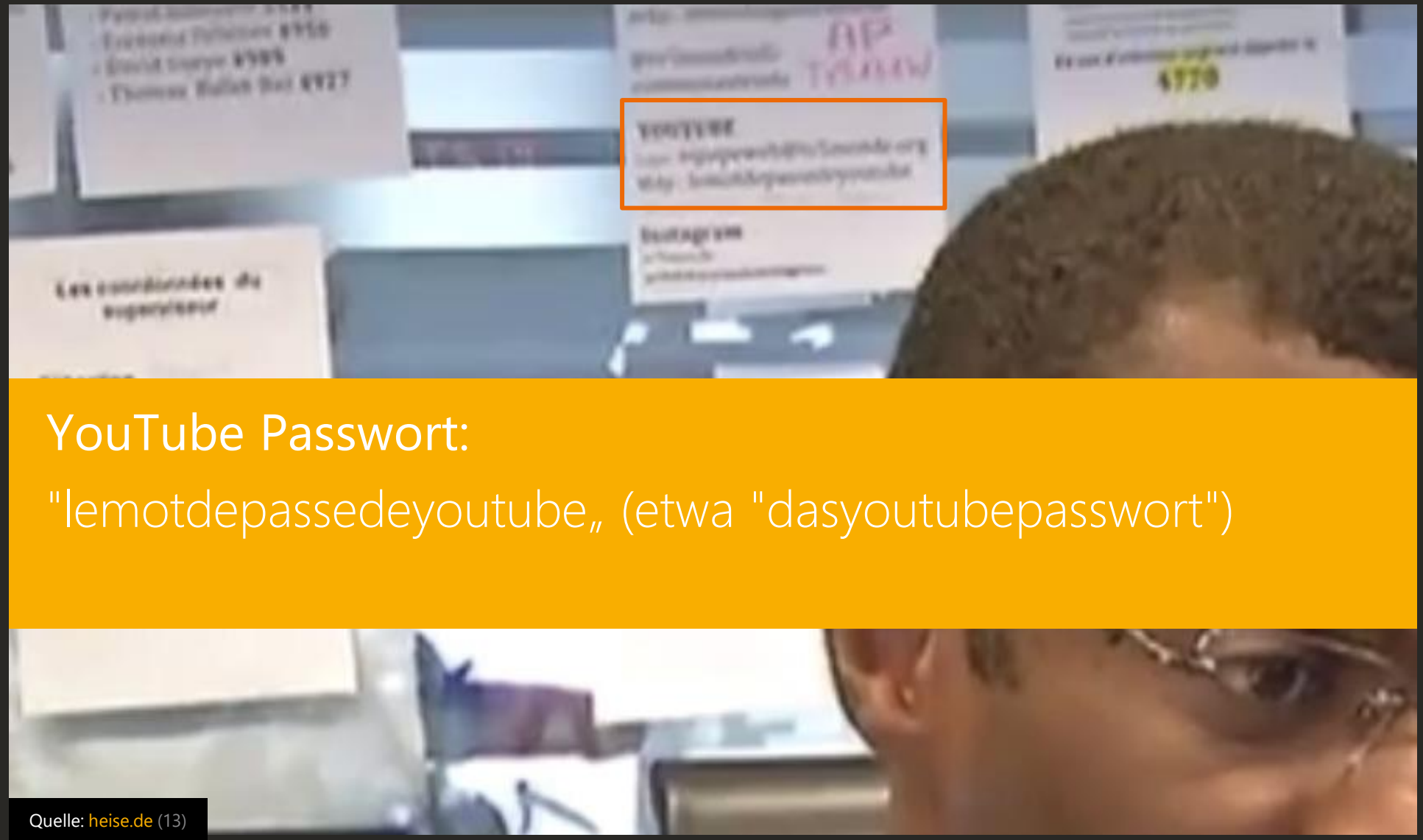
Quelle: pics-for-fun.com (11)

Quelle: de.pinterest.com (12)

Faktor Mensch

Quelle: heise.de (13)

Faktor Mensch

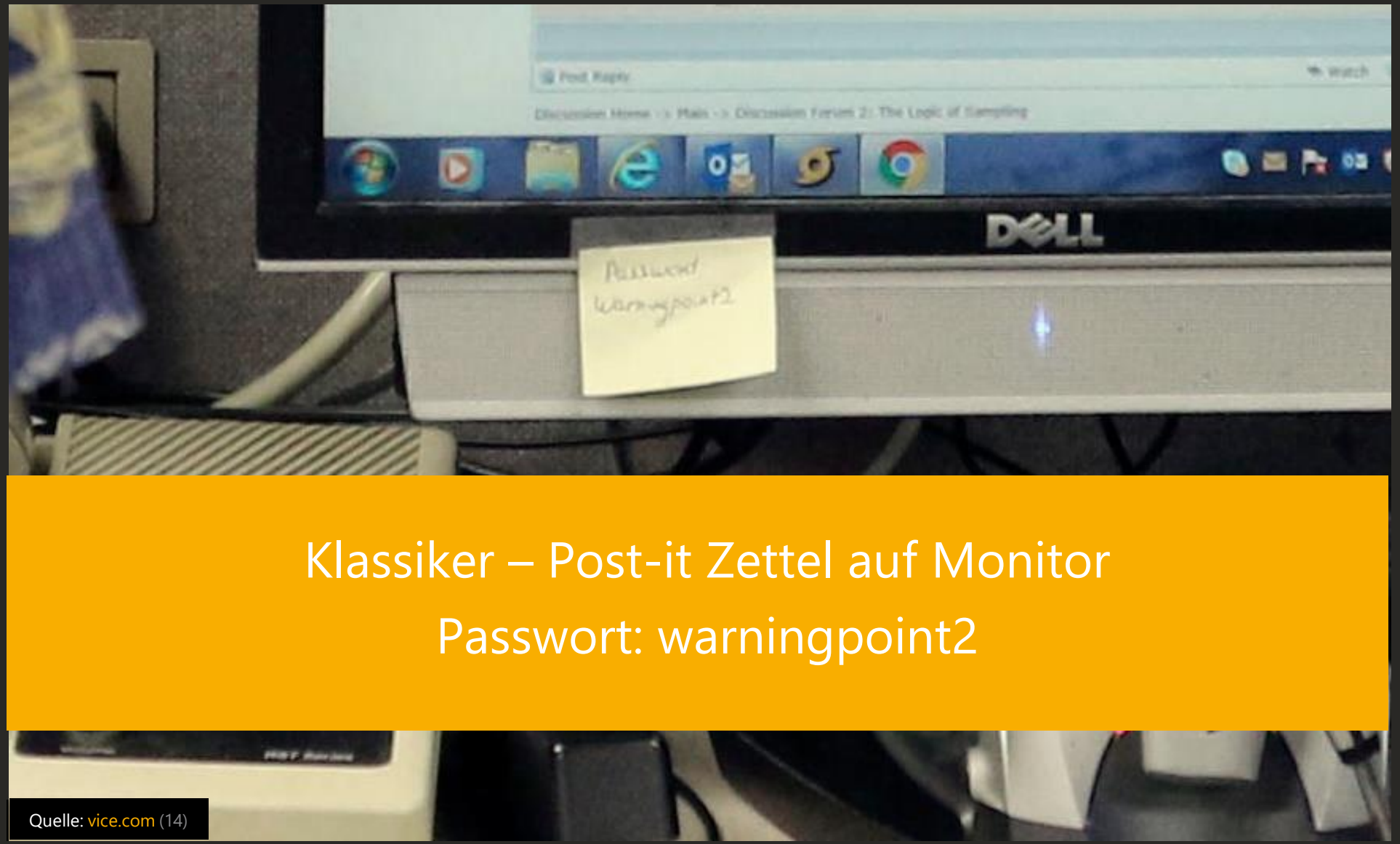


Quelle: heise.de (13)

Faktor Mensch

Quelle: vice.com (14)

Faktor Mensch

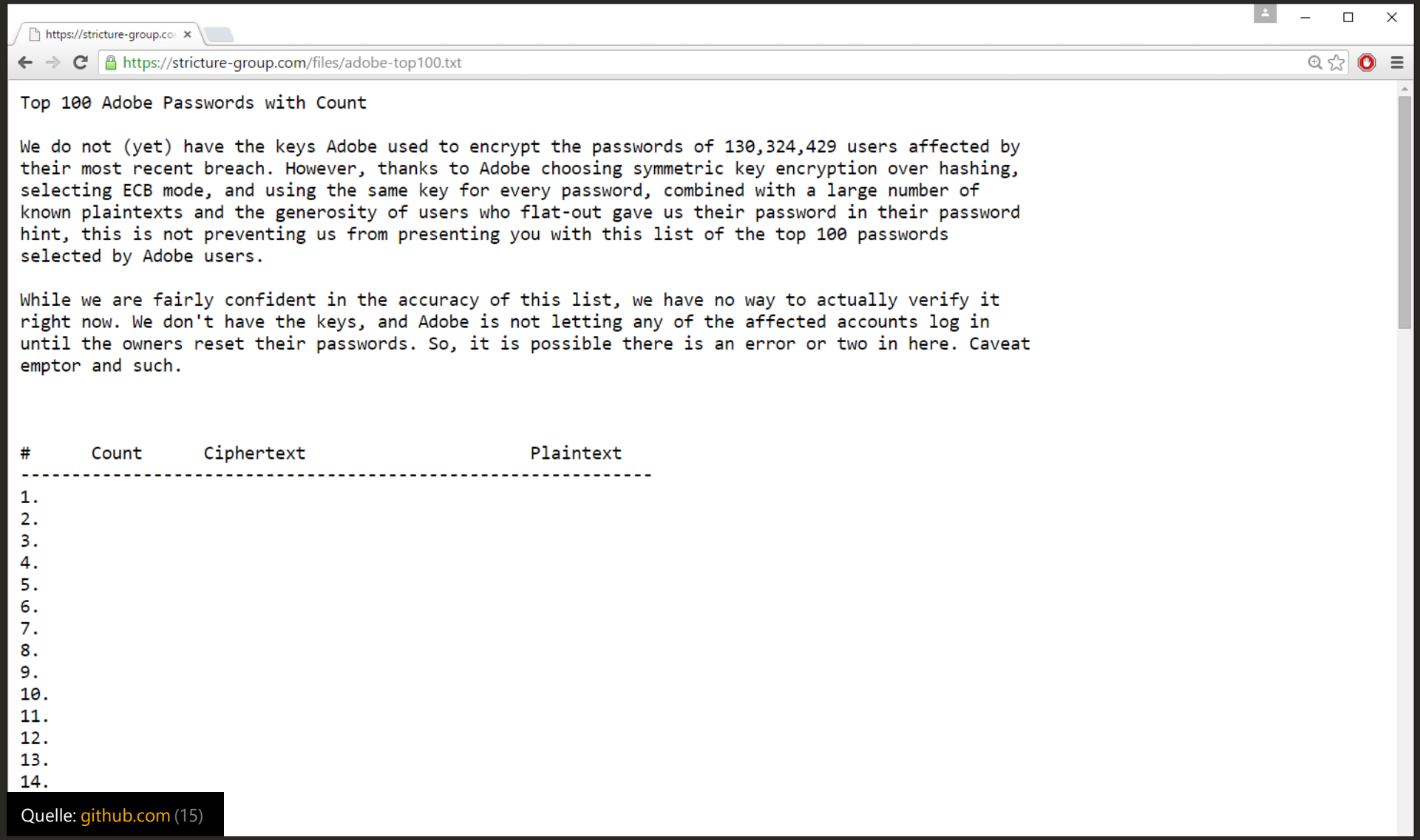


Klassiker – Post-it Zettel auf Monitor

Passwort: warningpoint2

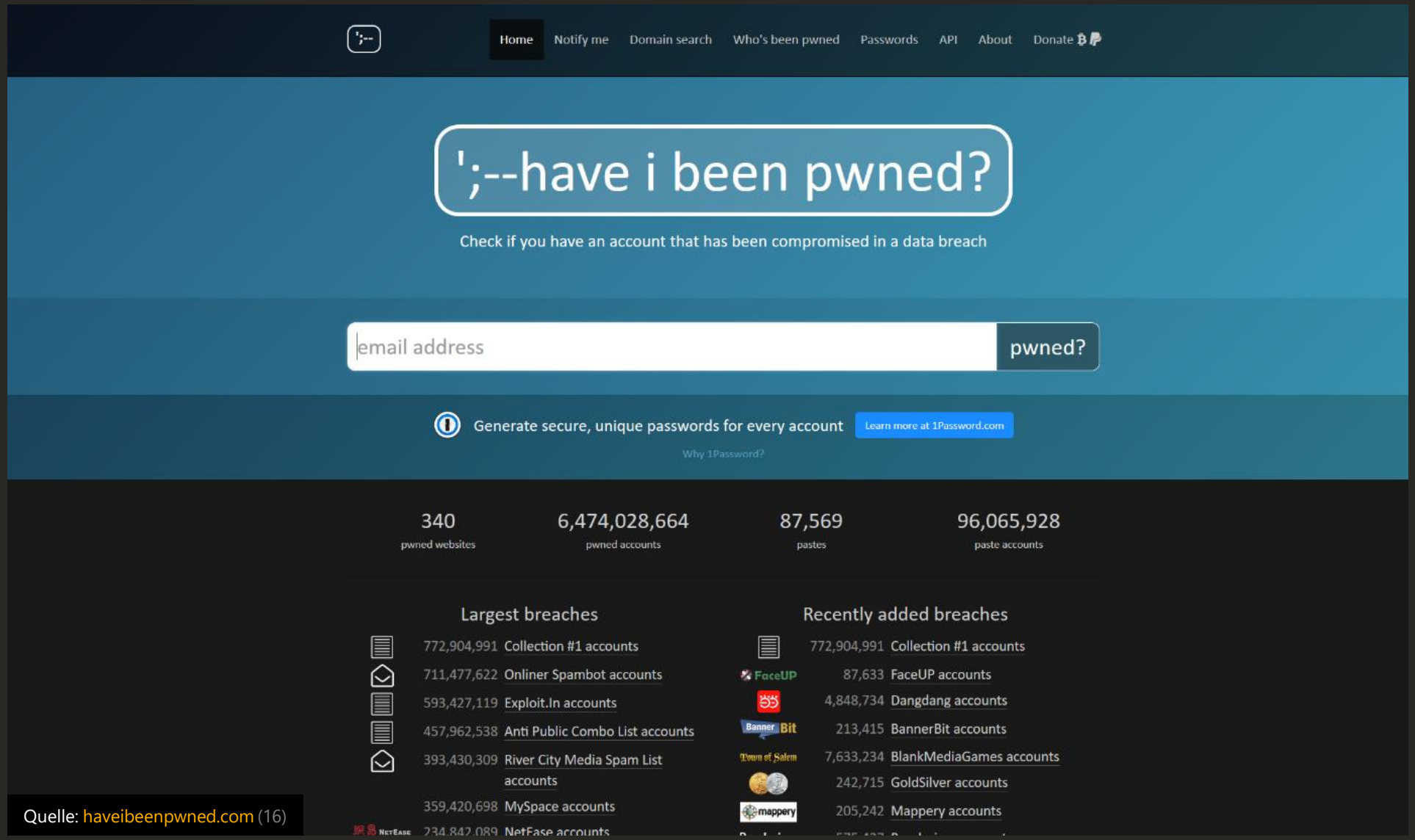
Quelle: vice.com (14)

Bekannte Passwörter



Quelle: github.com (15)

LIVE Gehackte Accounts



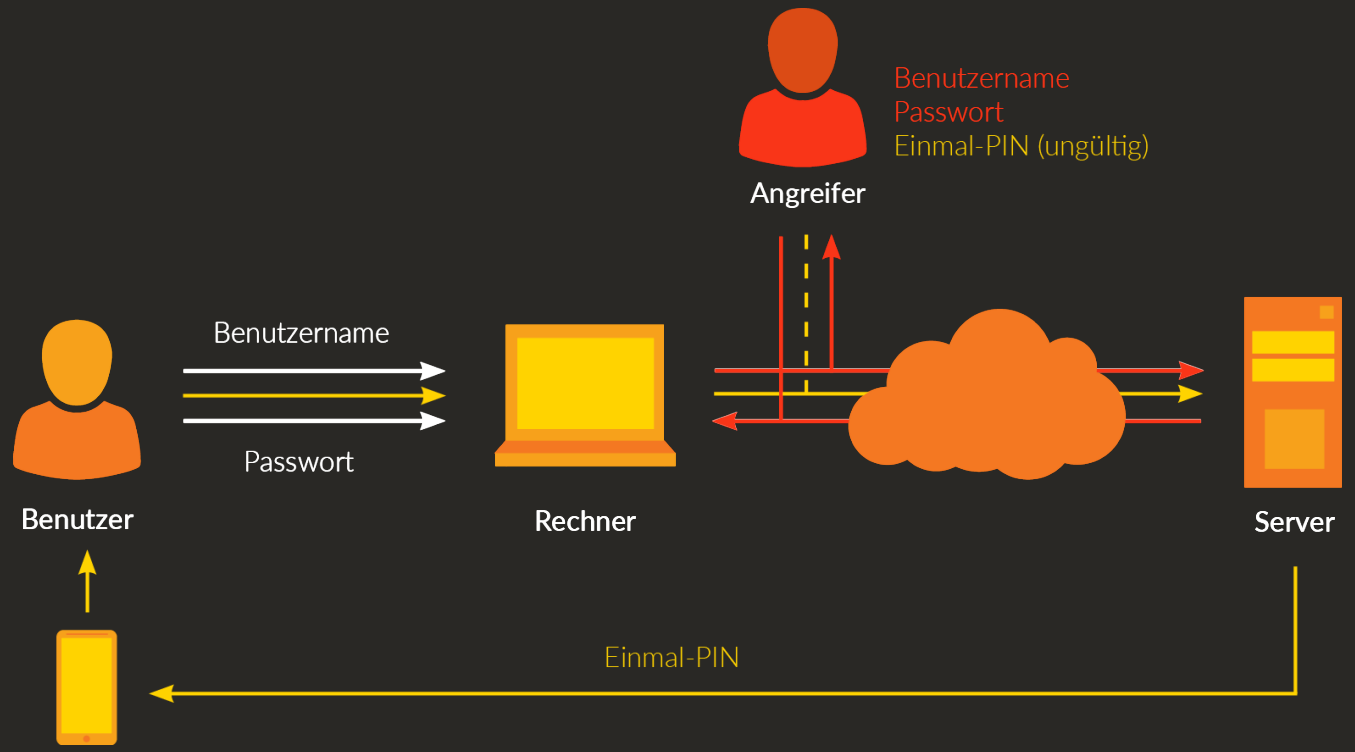
Quelle: haveibeenpwned.com (16)

Passwörter verraten

Quelle: youtube.com (17)

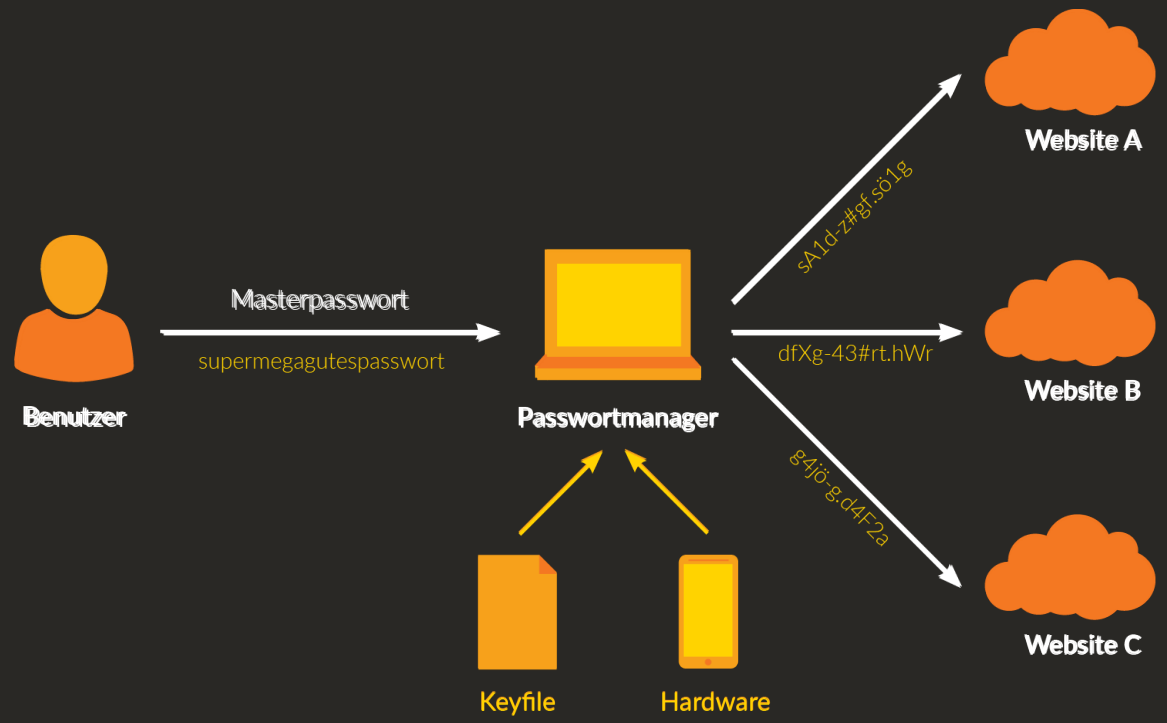
Zwei-Faktor-Authentisierung

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



Passwortmanager

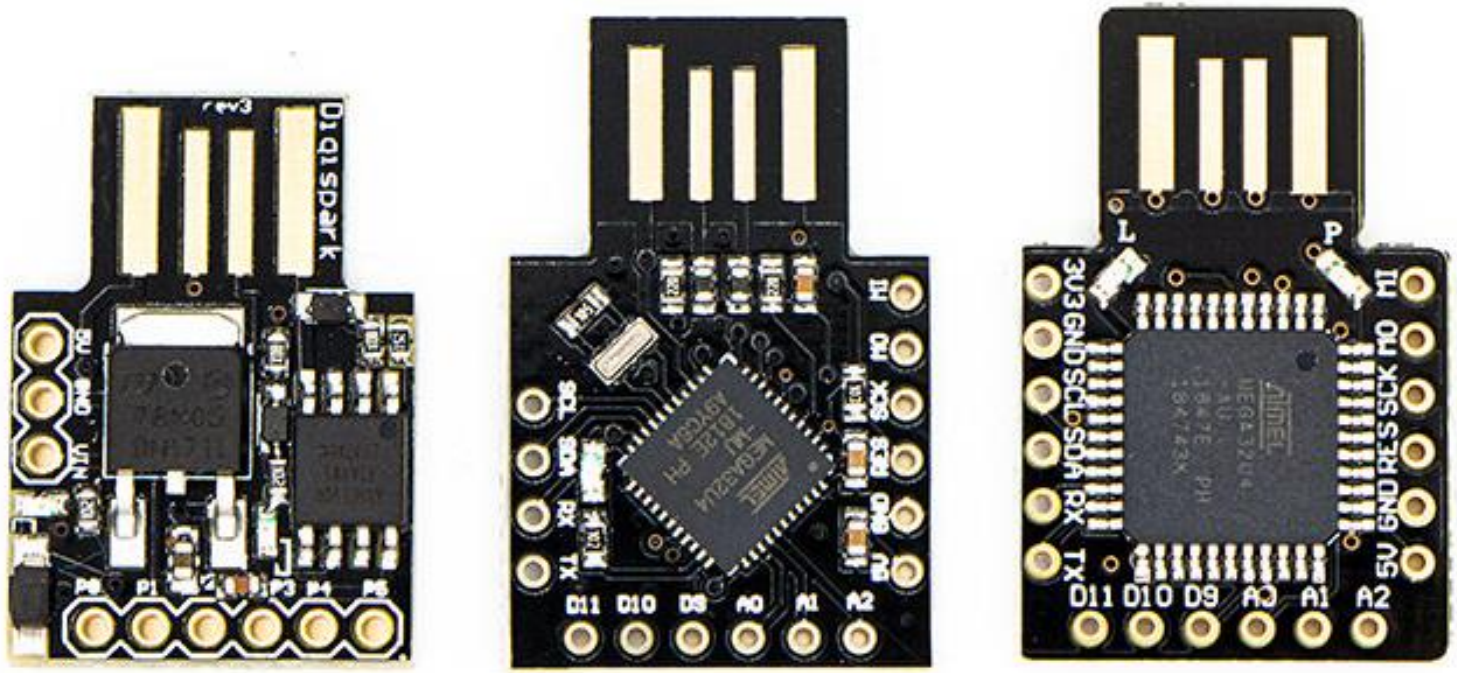
- Passwortmanager
  - Speichert Passwörter in einem verschlüsselten Container mit einem Masterpasswort und unterstützt bei der Generierung von Passwörtern
  - Verschiedene Lösungen sind vorhanden – z.B. KeePassXC
    - Viele Möglichkeiten zur Erweiterung (Firefox / Chrome Plugin, …)



Hacking Hardware

Hardware Tools

LIVE BadUSB



Zusammenfassung

Angriffsszenarien

Welche Angriffsszenarien sind für Handwerksbetriebe relevant?

- **Automatisierte Angriffe**
  Angreifer scannen systematisch alle über das Internet erreichbare Systeme. Werden Schwachstellen entdeckt, werden diese angegriffen.
- **Spam / Phishing Mails**
  Mails können von Angreifern einfach gefälscht werden. Teilweise basieren sie auf echten Mails von anderen Opfern.
- **Diebstahl von Geräten**
  Geräte (Notebooks / Tablets / Smartphones) werden auf Veranstaltungen, auf Baustellen oder aus Autos geklaut.
- **Verwundbare öffentliche WLANs**
  Angreifer können in öffentlichen WLANs zum Teil die Übertragungen mitlesen oder Anfragen auf andere Server automatisch umleiten.

Maßnahmen

10 Tipps für mehr IT-Sicherheit in Handwerksbetrieben:

1. So viel Software / Geräte wie nötig, so wenig wie möglich
2. Erneuern, organisieren und pflegen Sie Ihre Passwörter
3. Aktualisieren Sie immer Ihre Anwendungen und Systeme
4. Nutzen Sie Antivirenprogramme und Firewalls
5. Nutzen Sie die Systemverschlüsselung von mobilen Geräten
6. Reduzieren Sie die Zugriffsrechte auf ein Minimum
7. Setzen Sie eine sichere Backupstrategie für alle Ihre Systeme ein
8. Trennen Sie verschiedene Bereiche voneinander
9. Verwenden Sie ausschließlich verschlüsselte Verbindungen
10. Schärfen Sie das Sicherheitsbewusstsein Ihrer Mitarbeiter*innen

Maßnahmen – weitere Ressourcen

- Weitere Checklisten
  hwk.de | selbstaendig-im-handwerk.de
- Konkrete Handlungsempfehlungen für Handwerker
  it-sicherheit-handwerk.de
- IT-Grundschutz - Informationssicherheit mit System (BSI)
  bsi.bund.de

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 02.10.2021
2) Mit Floppy Disks Atombomben überwachen, http://www.zeit.de/politik/ausland/2016-05/us-militaer-pcs-technologie-veraltet-rechnungshof, abgerufen am 02.10.2021
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 02.10.2021
4) Shodan, https://shodan.io/, abgerufen am 02.10.2021
5) Shodan Maps, https://maps.shodan.io, abgerufen am 02.10.2021
6) Anuncio - gwapo's, https://www.youtube.com/watch?v=5M9k7wfiWiI, abgerufen am 02.10.2021
7) Gefängnisausbruch mittels E-Mail-Betrug, http://www.heise.de/newsticker/meldung/Gefaengnisausbruch-mittels-E-Mail-Betrug-2587303.html, abgerufen am 02.10.2021
8) AIDS (Schadprogramm), https://de.wikipedia.org/wiki/AIDS_(Schadprogramm), abgerufen am 02.10.2021
9) Locky, https://de.wikipedia.org/wiki/Locky, abgerufen am 02.10.2021
10) Code, http://pics-for-fun.com/wonder-what-the-code-could-be/, abgerufen am 02.10.2021
11) And the valuables are in the closet on the top shelf in a box marked, https://de.pinterest.com/pin/3025924727584002/, abgerufen am 02.10.2021
12) 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 02.10.2021
13) 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 02.10.2021
14) Top 100 Adobe Passwords with Count, https://github.com/morontt/symfobrute/blob/master/adobe-top100.txt, abgerufen am 02.10.2021
15) Have I Been Pwned, https://haveibeenpwned.com, abgerufen am 02.10.2021
16) What is Your Password?, https://www.youtube.com/watch?v=opRMrEfAIiI, abgerufen am 02.10.2021