



Tobias Scheible, M.Eng.

IT Security für Handwerksbetriebe
Kreishandwerkerschaft Sigmaringen

- 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

00000000

?

Cyber Security

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

Social Engineering

Passwortsicherheit

Hacking Hardware

00000000

Launch-Code für die in den USA stationierten Atomraketen

(1962 bis 1977)

Cyber Security

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

Social Engineering

Passwortsicherheit

Hacking Hardware

PIN Code Beispiel - Steuerungstechnik

IT-Security für Handwerksbetriebe
Kreishandwerkerschaft Sigmaringen



Quelle: [zeit.de](#) (2)

Cyber Security

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

Social Engineering

Passwortsicherheit

Hacking Hardware

06.10.2021 | Sigmaringen

Tobias Scheible, M.Eng.

IoT Beispielprodukt

IT-Security für Handwerksbetriebe
Kreishandwerkerschaft Sigmaringen

heise online

Anmelden

Suchen

Q

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](https://www.heise.de) (3)

Cyber Security

Pin Code Beispiel

IoT Beispielprodukt

Spezialisierte Suchmaschine

Cybercrime as a Service

Social Engineering

Passwortsicherheit

Hacking Hardware

06.10.2021 | Sigmaringen

Tobias Scheible, M.Eng.

Spezialisierte Suchmaschine

IT-Security für Handwerksbetriebe
Kreishandwerkerschaft Sigmaringen

Shodan Developers Monitor View All...

SHODAN

Explore Pricing Enterprise Access New to Shodan? Login or Register

The search engine for Webcams

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account Getting Started

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

21% of Fortune 100

1,000+ Universities

Quelle: shodan.io (4)

Cyber Security

Pin Code Beispiel
IoT Beispielprodukt
Spezialisierte Suchmaschine
Cybercrime as a Service

Social Engineering

Passwortsicherheit

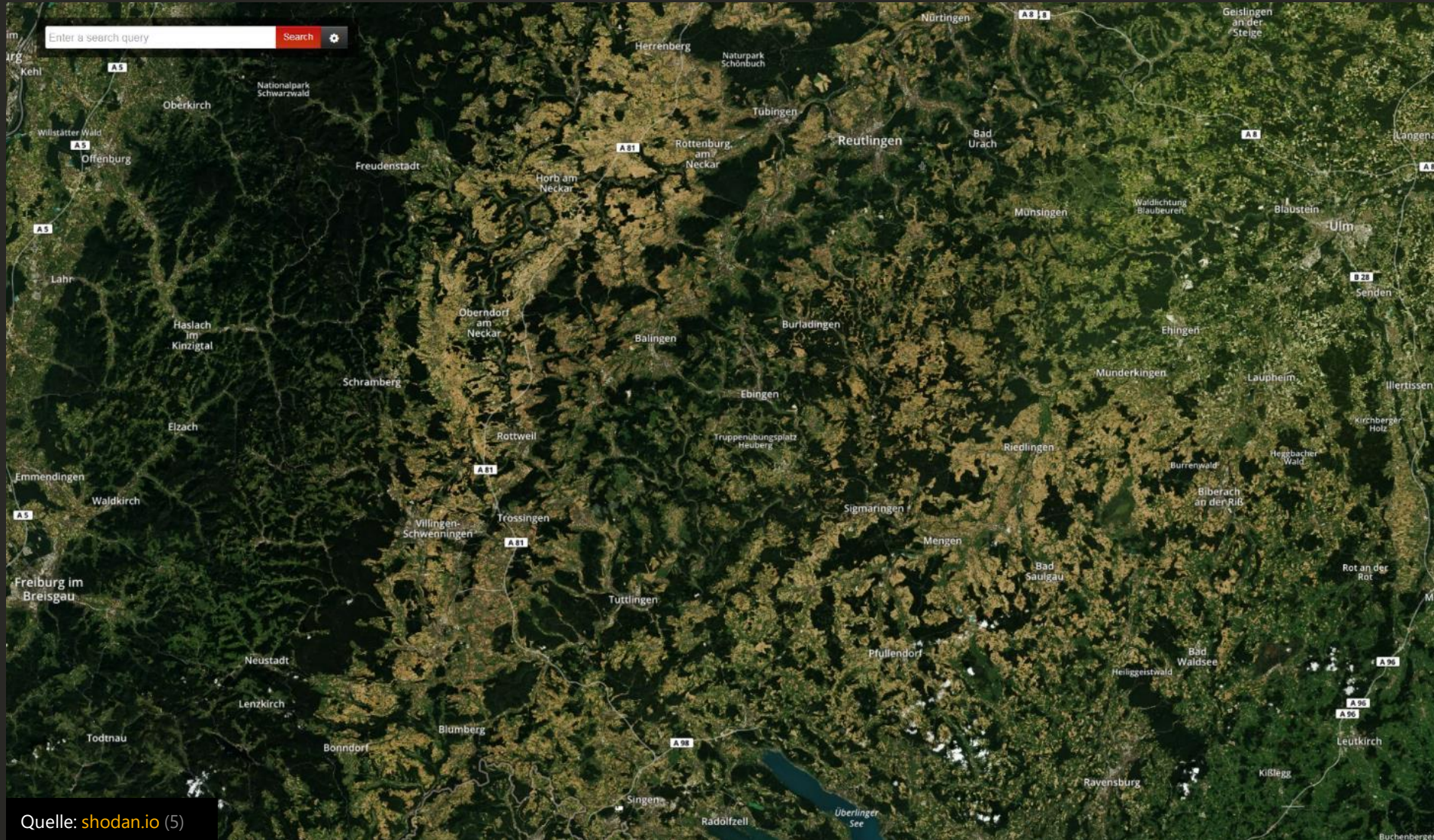
Hacking Hardware

06.10.2021 | Sigmaringen

Tobias Scheible, M.Eng.

LIVE Spezialisierte Suchmaschine

IT-Security für Handwerksbetriebe
Kreishandwerkerschaft Sigmaringen



Cyber Security

Pin Code Beispiel
IoT Beispielprodukt
Spezialisierte Suchmaschine
Cybercrime as a Service

Social Engineering

Passwortsicherheit

Hacking Hardware

06.10.2021 | Sigmaringen

Tobias Scheible, M.Eng.

Cybercrime as a Service



Koordinator

Cyber Security

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

Social Engineering

Passwortsicherheit

Hacking Hardware

Cybercrime as a Service



Quelle: [youtube.com](https://www.youtube.com/watch?v=6j8K8K8K8K) (6)

Cyber Security

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

Social Engineering

Passwortsicherheit

Hacking Hardware

Was ist die häufigste Angriffsmethode?

Ausnutzung von Schwachstellen

A

Physische Attacken

B

Manipulation von Personen

C

Ausnutzung von Fehlern

D

The background of the slide is a dark, textured surface with a network of glowing orange lines and nodes. The nodes are represented by various icons: some are square boxes with an 'X' inside, resembling email symbols, and others are circles containing an '@' symbol, representing email addresses. The lines connect these nodes in a complex, web-like pattern. Some nodes are larger and more prominent than others. The overall color scheme is dominated by dark tones with bright orange highlights from the network elements.

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

Cyber Security

Social Engineering

Moderner Gefängnisausbruch
CEO Fraud
E-Mails fälschen
Ransomware
AIDS – Erste Ransomware
Fallbeispiel Locky


Passwortsicherheit

Hacking Hardware

LIVE E-Mails fälschen

Fake Mail Sender - Lab | scheible x +

https://lab.scheible.it/demos/fakemailsender/



Demonstration Lab

IT Security & IT Forensics Examples

Fake Mail Sender

Example to show how a mail sender can be faked.

Sender Mail	
Sender Name	
Receiver Mail	
Subject	

send mail

Cyber Security Lab © 2021 Tobias Scheible

IT-Security für Handwerksbetriebe
Kreishandwerkerschaft Sigmaringen

Cyber Security

Social Engineering

Moderner Gefängnisausbruch
CEO Fraud
E-Mails fälschen
Ransomware
AIDS – Erste Ransomware
Fallbeispiel Locky

Passwortsicherheit

Hacking Hardware

06.10.2021 | Sigmaringen

Tobias Scheible, M.Eng.

Ransomware



Cyber Security

Social Engineering

- Moderner Gefängnisausbruch
- CEO Fraud
- E-Mails fälschen
- Ransomware
- AIDS – Erste Ransomware
- Fallbeispiel Locky

Passwortsicherheit

Hacking Hardware

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

```
Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed INVOICE, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378. You must enclose a bankers draft,
cashier's check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

Press ENTER to continue
```

Quelle: [wikipedia.org](https://de.wikipedia.org/wiki/AIDS_(Ransomware)) (9)

Cyber Security

Social Engineering

Moderner Gefängnisausbruch
CEO Fraud
E-Mails fälschen
Ransomware
AIDS – Erste Ransomware
Fallbeispiel Locky

Passwortsicherheit

Hacking Hardware

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)

Cyber Security

Social Engineering

Moderner Gefängnisausbruch
CEO Fraud
E-Mails fälschen
Ransomware
AIDS – Erste Ransomware
Fallbeispiel Locky

Passwortsicherheit

Hacking Hardware



Passwortsicherheit

Faktor Mensch

I wonder what the code could be...



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



Quelle: de.pinterest.com (12)

Cyber Security

Social Engineering

Passwortsicherheit

- Faktor Mensch
- Bekannte Passwörter
- Gehackte Accounts
- Passwörter verraten
- Zwei-Faktor-Authentisierung
- Passwortmanager

Hacking Hardware

Faktor Mensch



Quelle: [heise.de](https://www.heise.de) (13)

IT-Security für Handwerksbetriebe
Kreishandwerkerschaft Sigmaringen

Cyber Security

Social Engineering

Passwortsicherheit

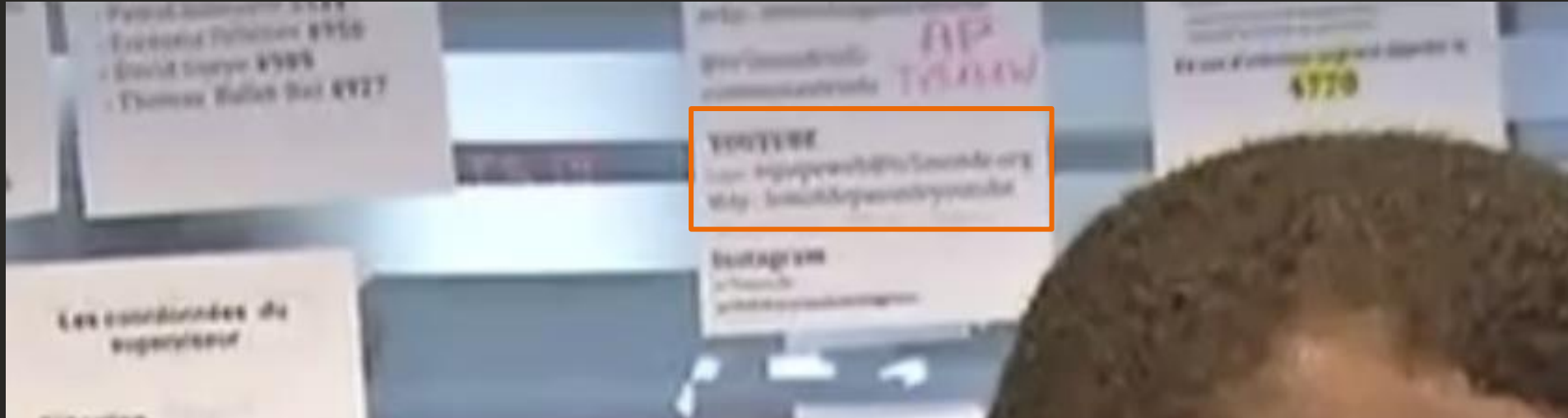
- Faktor Mensch
- Bekannte Passwörter
- Gehackte Accounts
- Passwörter verraten
- Zwei-Faktor-Authentisierung
- Passwortmanager

Hacking Hardware

06.10.2021 | Sigmaringen

Tobias Scheible, M.Eng.

Faktor Mensch



YouTube Passwort:

"lemotdepasseyoutube,, (etwa "dasyoutubepasswort")



Cyber Security

Social Engineering

Passwortsicherheit

- Faktor Mensch
- Bekannte Passwörter
- Gehackte Accounts
- Passwörter verraten
- Zwei-Faktor-Authentisierung
- Passwortmanager

Hacking Hardware

Faktor Mensch

IT-Security für Handwerksbetriebe
Kreishandwerkerschaft Sigmaringen



Quelle: [vice.com](https://www.vice.com) (14)

Cyber Security

Social Engineering

Passwortsicherheit

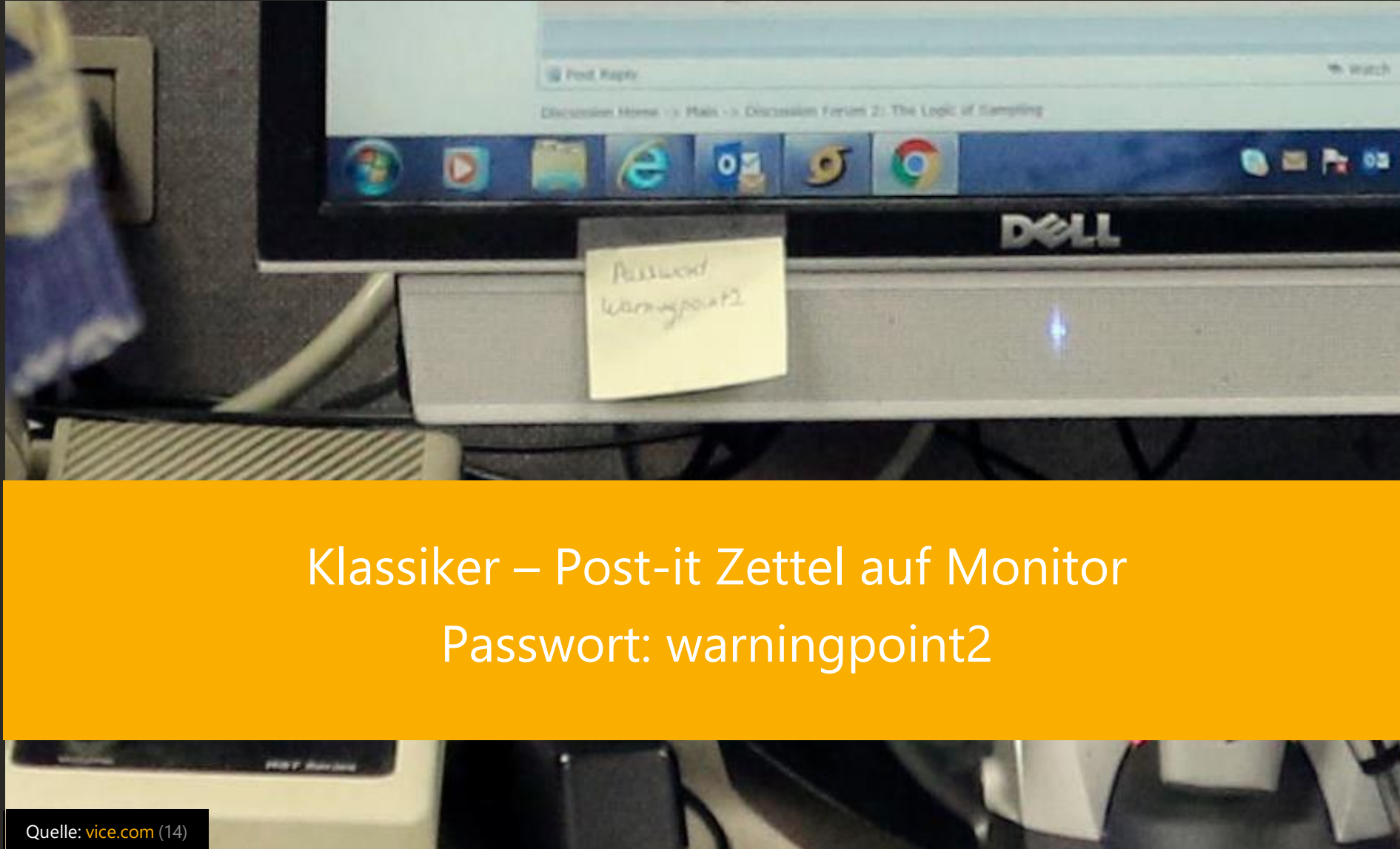
- Faktor Mensch
- Bekannte Passwörter
- Gehackte Accounts
- Passwörter verraten
- Zwei-Faktor-Authentisierung
- Passwortmanager

Hacking Hardware

06.10.2021 | Sigmaringen

Tobias Scheible, M.Eng.

Faktor Mensch



Klassiker – Post-it Zettel auf Monitor
Passwort: warningpoint2

Quelle: [vice.com](https://www.vice.com) (14)

Cyber Security

Social Engineering

Passwortsicherheit

- Faktor Mensch
- Bekannte Passwörter
- Gehackte Accounts
- Passwörter verraten
- Zwei-Faktor-Authentisierung
- Passwortmanager

Hacking Hardware

Bekannte Passwörter

https://stricture-group.co

https://stricture-group.com/files/adobe-top100.txt

Top 100 Adobe Passwords with Count

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

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

#	Count	Ciphertext	Plaintext
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			

Quelle: [github.com](#) (15)

- Cyber Security
- Social Engineering
- Passwortsicherheit
 - Faktor Mensch
 - Bekannte Passwörter
 - Gehackte Accounts
 - Passwörter verraten
 - Zwei-Faktor-Authentisierung
 - Passwortmanager
- Hacking Hardware

LIVE Gehackte Accounts

[Home](#) [Notify me](#) [Domain search](#) [Who's been pwned](#) [Passwords](#) [API](#) [About](#) [Donate](#)

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

pwned?

Generate secure, unique passwords for every account [Learn more at 1Password.com](#)

Why 1Password?

340

pwned websites

6,474,028,664

pwned accounts

87,569

pastes

96,065,928

paste accounts

Largest breaches

772,904,991 [Collection #1 accounts](#)

711,477,622 [Onliner Spambot accounts](#)

593,427,119 [Exploit.In accounts](#)

457,962,538 [Anti Public Combo List accounts](#)

393,430,309 [River City Media Spam List accounts](#)

359,420,698 [MySpace accounts](#)

234,842,089 [NetEase accounts](#)

Recently added breaches

772,904,991 [Collection #1 accounts](#)

87,633 [FaceUP accounts](#)

4,848,734 [Dangdang accounts](#)

213,415 [BannerBit accounts](#)

7,633,234 [BlankMediaGames accounts](#)

242,715 [GoldSilver accounts](#)

205,242 [Mappery accounts](#)

Quelle: [haveibeenpwned.com](#) (16)

IT-Security für Handwerksbetriebe
Kreishandwerkerschaft Sigmaringen

Cyber Security

Social Engineering

Passwortsicherheit

- Faktor Mensch
- Bekannte Passwörter
- Gehackte Accounts
- Passwörter verraten
- Zwei-Faktor-Authentisierung
- Passwortmanager

Hacking Hardware

06.10.2021 | Sigmaringen

Tobias Scheible, M.Eng.

31

Passwörter verraten



Quelle: [youtube.com](https://www.youtube.com/watch?v=17) (17)

IT-Security für Handwerksbetriebe
Kreishandwerkerschaft Sigmaringen

Cyber Security

Social Engineering

Passwortsicherheit

- Faktor Mensch
- Bekannte Passwörter
- Gehackte Accounts
- Passwörter verraten
- Zwei-Faktor-Authentisierung
- Passwortmanager

Hacking Hardware

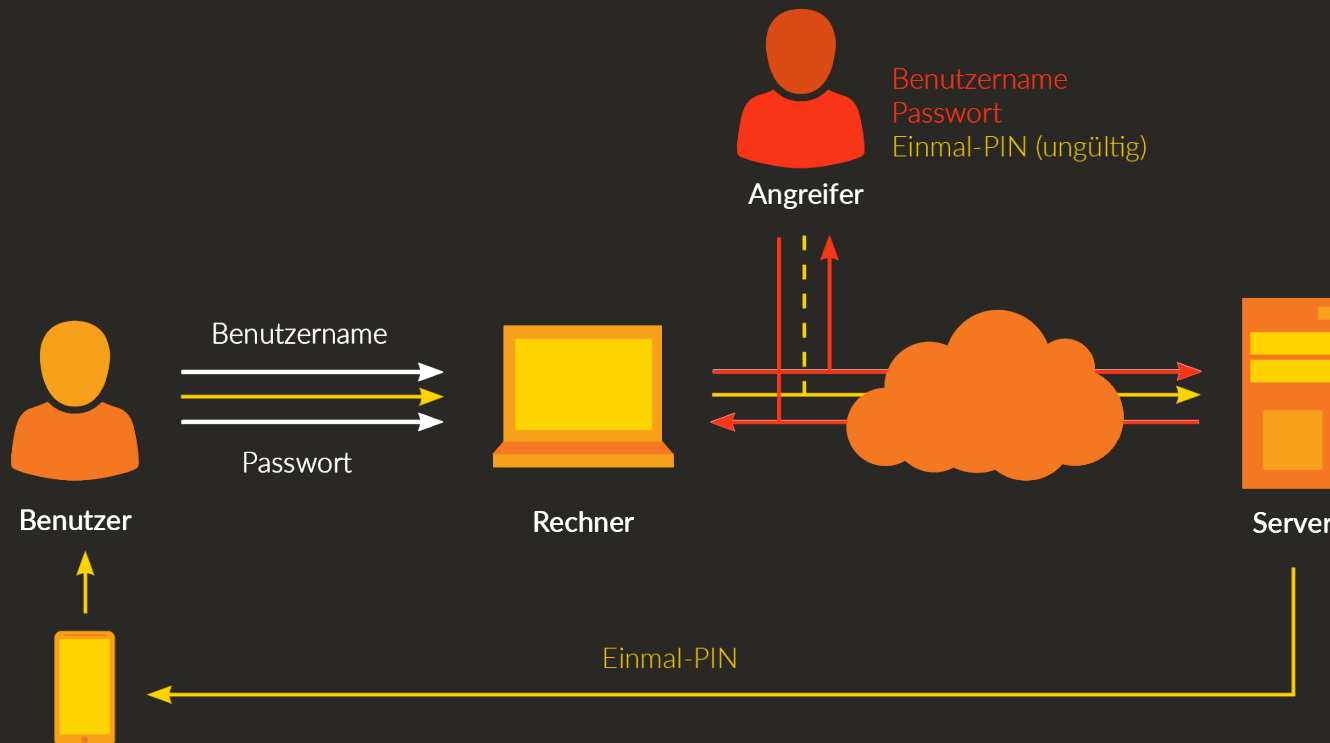
06.10.2021 | Sigmaringen

Tobias Scheible, M.Eng.

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)



Cyber Security

Social Engineering

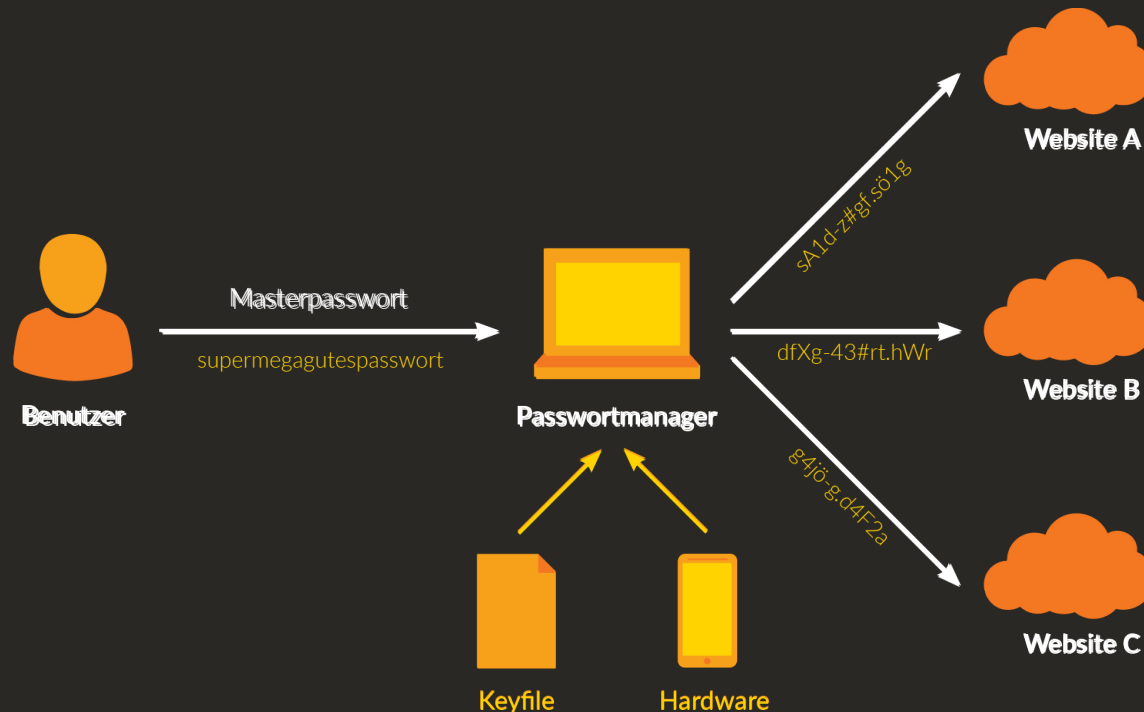
Passwortsicherheit

Faktor Mensch
Bekannte Passwörter
Gehackte Accounts
Passwörter verraten
Zwei-Faktor-Authentisierung
Passwortmanager

Hacking Hardware

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, ...)



Cyber Security

Social Engineering

Passwortsicherheit

Faktor Mensch
Bekannte Passwörter
Gehackte Accounts
Passwörter verraten
Zwei-Faktor-Authentisierung
Passwortmanager

Hacking Hardware

Hacking Hardware

Hardware Tools

IT-Security für Handwerksbetriebe
Kreishandwerkerschaft Sigmaringen



Cyber Security

Social Engineering

Passwortsicherheit

Hacking Hardware

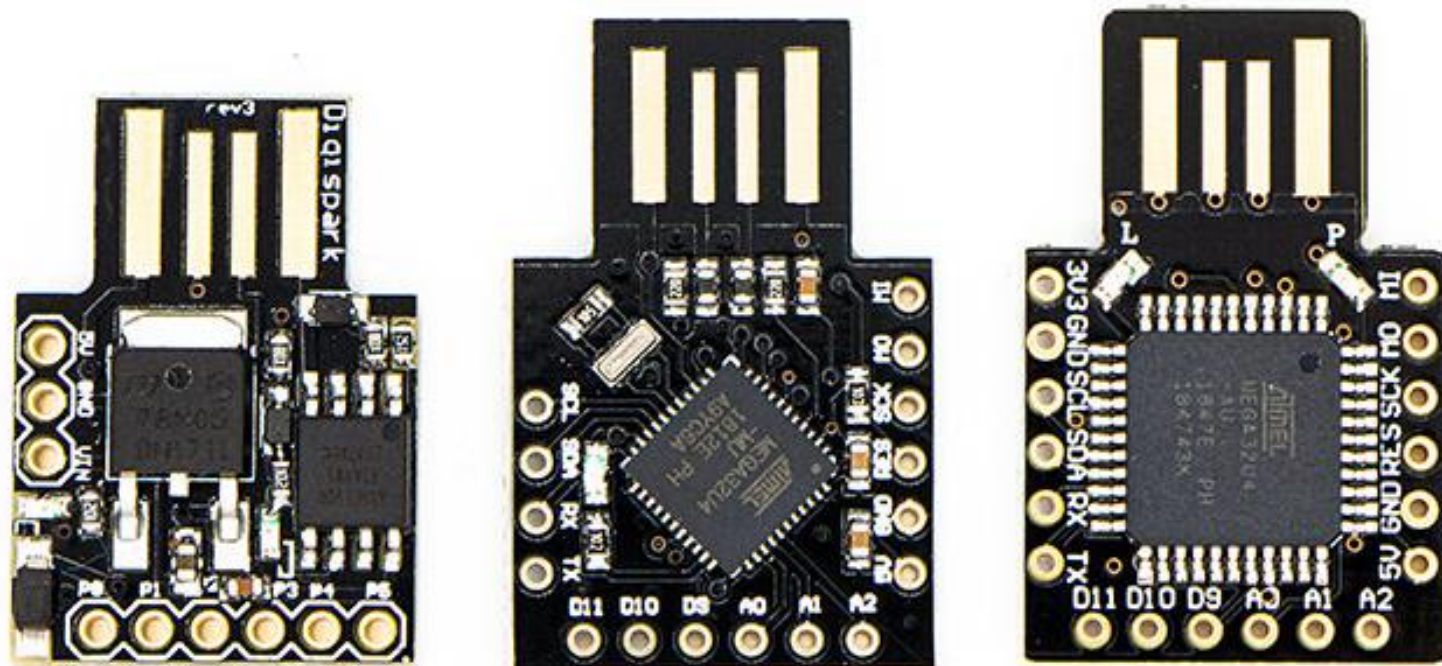
Hardware Tools

BadUSB

06.10.2021 | Sigmaringen

Tobias Scheible, M.Eng.

LIVE BadUSB



IT-Security für Handwerksbetriebe
Kreishandwerkerschaft Sigmaringen

Cyber Security

Social Engineering

Passwortsicherheit

Hacking Hardware

Hardware Tools

BadUSB

06.10.2021 | Sigmaringen

Tobias Scheible, M.Eng.

39



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.

Cyber Security

Social Engineering

Passwortsicherheit

Hacking Hardware

Zusammenfassung

Angriffsszenarien

Maßnahmen

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

Cyber Security

Social Engineering

Passwortsicherheit

Hacking Hardware

Zusammenfassung

Angriffsszenarien

Maßnahmen

Maßnahmen – weitere Ressourcen

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.

Checkliste Passwortsicherheit

- Werden sichere Passwörter eingesetzt?
- Wird überall wo möglich eine Zwei-Faktor-Authentisierung eingesetzt?
- Wird ein Passwortmanager verwendet?
- Werden alle Passwörter für den Notfall an einem sicheren Ort gespeichert?

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

Cyber Security

Social Engineering

Passwortsicherheit

Hacking Hardware

Zusammenfassung

Angriffsszenarien

Maßnahmen

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=5M9k7wfiWil>, 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_\(Schadprogramm\)](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/symfobroute/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=opRMrEfAlil>, abgerufen am 02.10.2021