

Tobias Scheible, M.Eng.

# Bedrohungen aus dem Internet IT-Sicherheit im Planungsbüro

- 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

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



Quelle: [zeit.de](https://www.zeit.de) (2)

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

03.03.2020 | bdlA

Tobias Scheible, M.Eng.

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

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

03.03.2020 | bdla

Tobias Scheible, M.Eng.



# Spezialisierte Suchmaschine

Bedrohungen aus dem Internet  
IT-Sicherheit im Planungsbüro

Shodan Developers Monitor View All...

SHODAN [Search Bar] 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

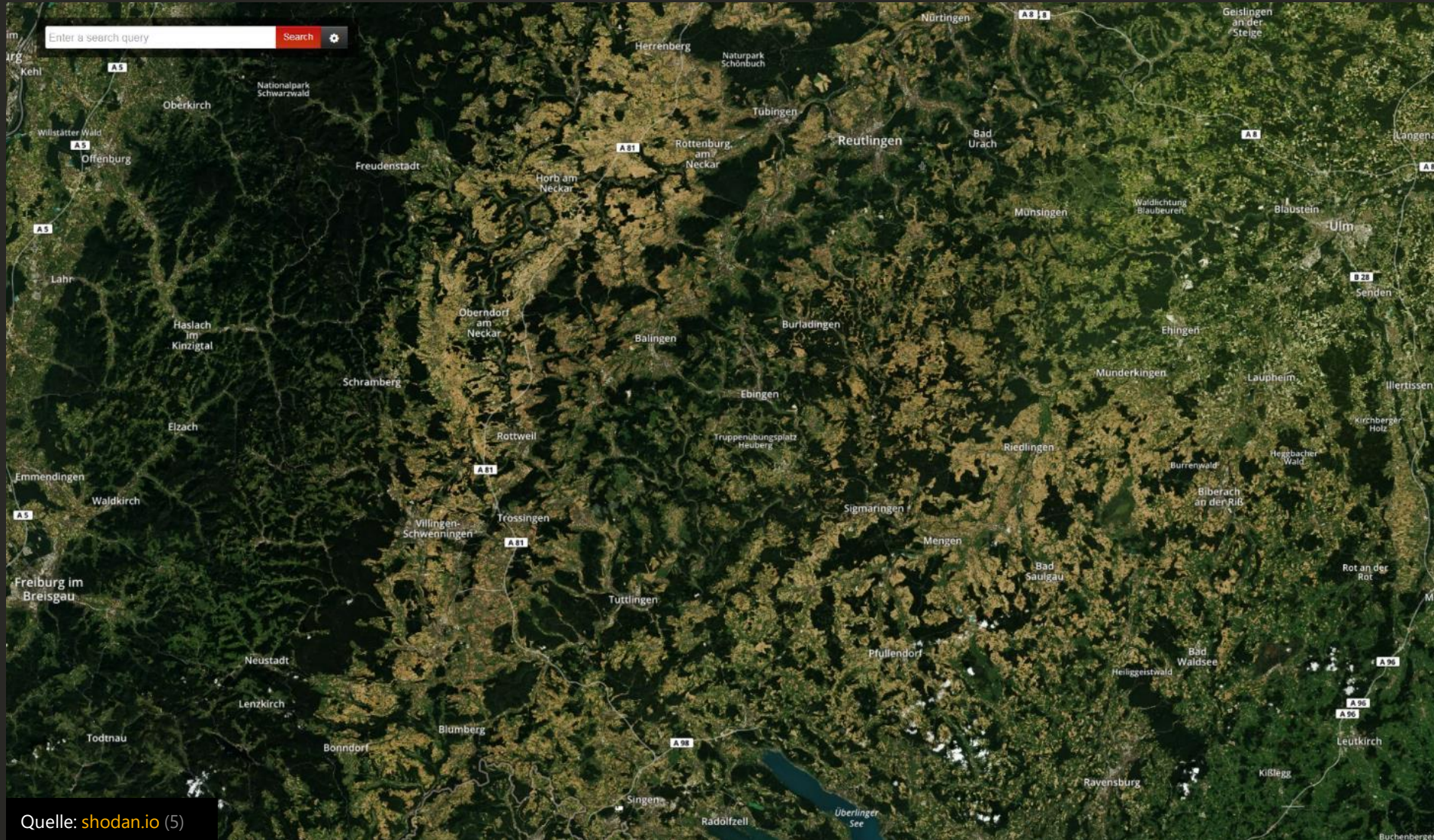
## Social Engineering

## Passwortsicherheit

## Hacking Hardware

# LIVE Spezialisierte Suchmaschine

Bedrohungen aus dem Internet  
IT-Sicherheit im Planungsbüro



Quelle: [shodan.io](https://shodan.io) (5)

## Cyber Security

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

## Social Engineering

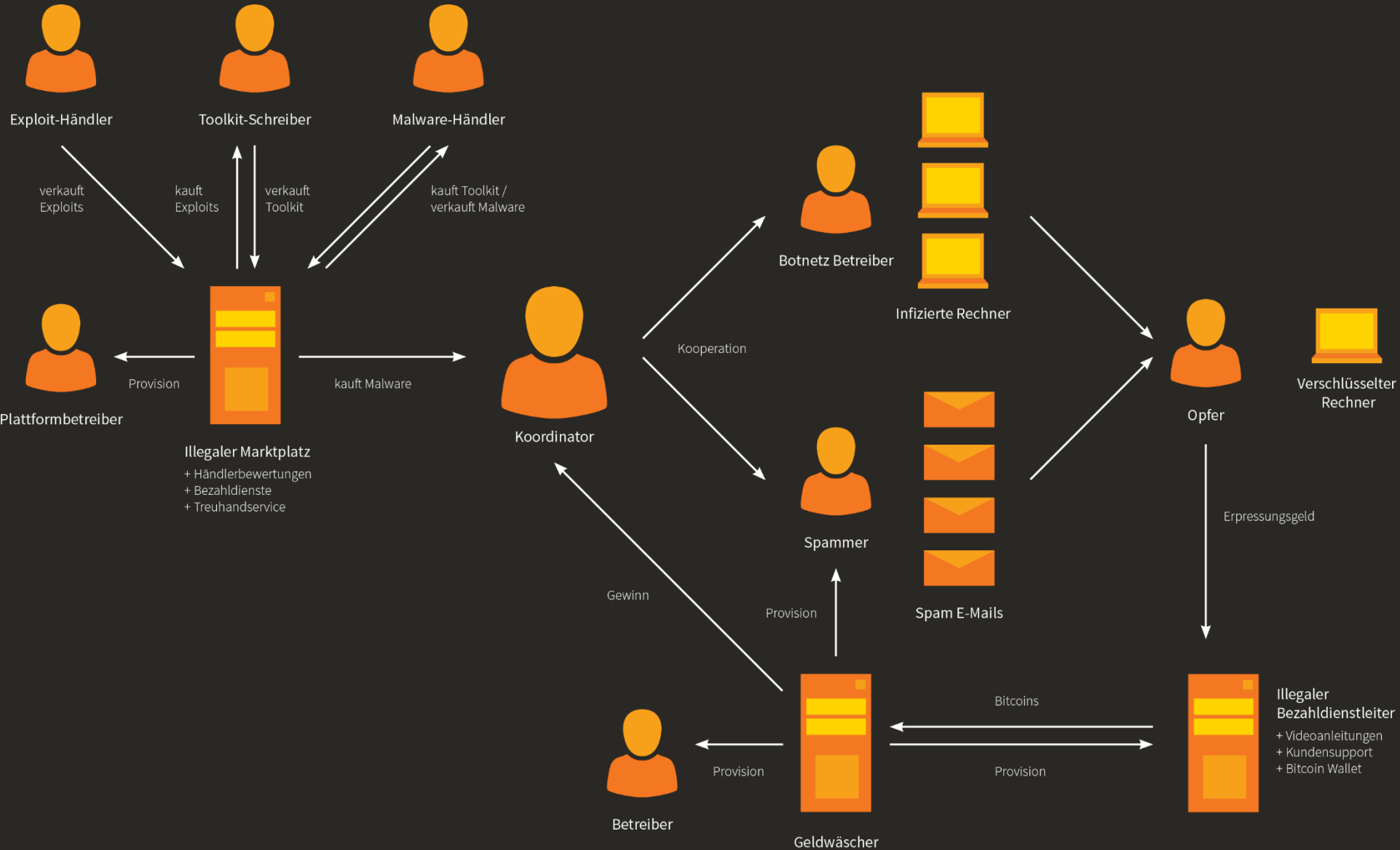
## Passwortsicherheit

## Hacking Hardware

03.03.2020 | bdla

Tobias Scheible, M.Eng.

# Cybercrime as a Service



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



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

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

---

03.03.2020 | bdla

Tobias Scheible, M.Eng.

# 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

## Cyber Security

### Social Engineering

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

### Passwortsicherheit

### Hacking Hardware



# CEO Fraud

Bedrohungen aus dem Internet  
IT-Sicherheit im Planungsbüro

Freitag, 12. Februar 2016

Service | Abo | Shop | Newsletter | Login | Registrieren | Suchbegriff, WKN, ISIN

WirtschaftsWoche

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%
-------------------------	--------------------------------	---------------------------	-------------------------------	-------------------------------	--------------------------

Die WirtschaftsWoche > Erfolg > Management > Falsche Chefs zocken Firmen ab: Den Enkeltrick gibt's auch bei Unternehmen

## Falsche Chefs zocken Firmen ab

### Den Enkeltrick gibt's auch bei Unternehmen

18. August 2015

★★★★☆

0


Kommentare

Versenden

Drucken

Merken

Startseite



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 als Vertreter der Geschäftsführung aus. Dann fordern sie bestimmte Beträge auf

Quelle: [wiwo.de](http://wiwo.de) (8)

## Cyber Security

### Social Engineering

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

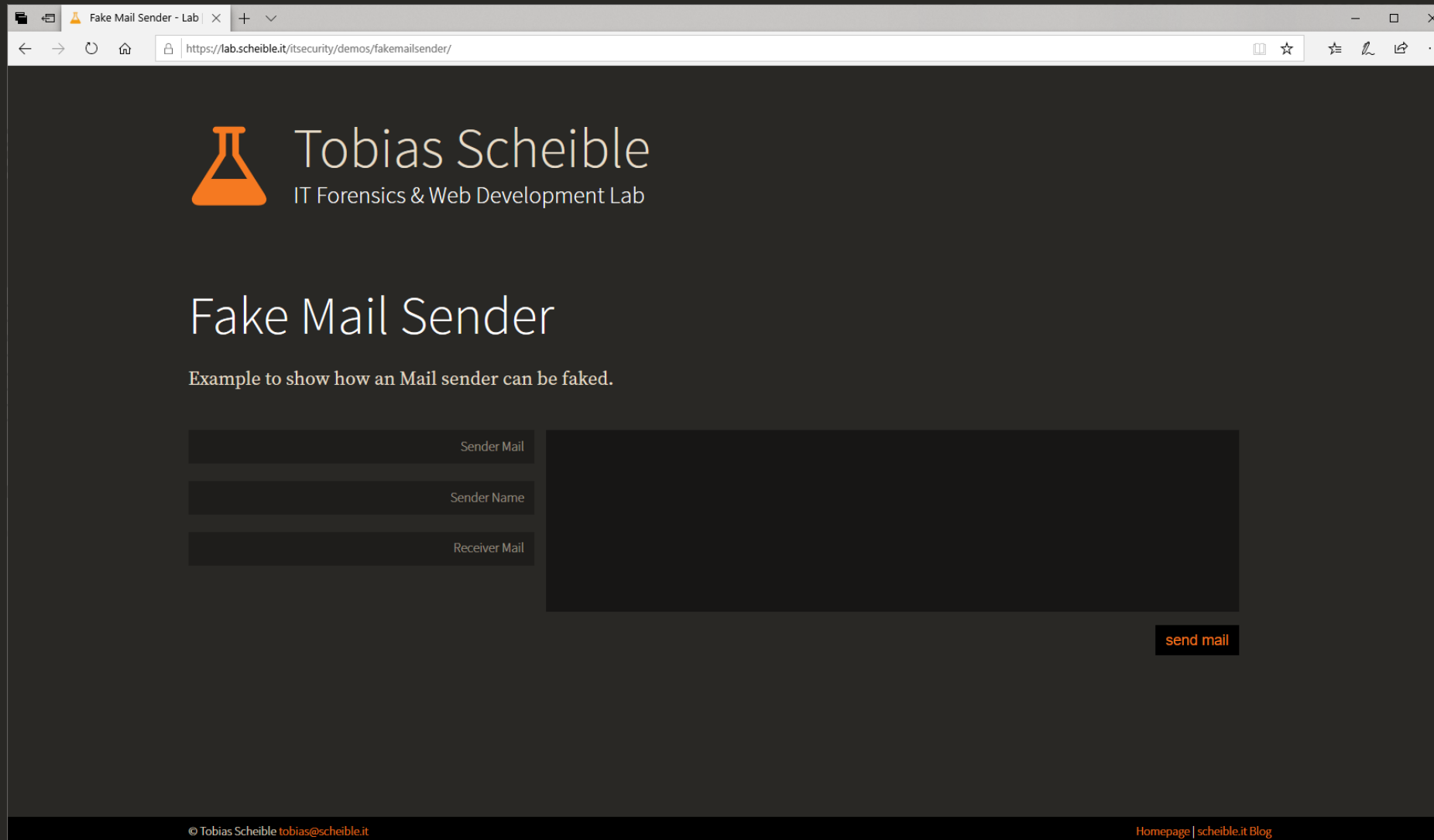
### Passwortsicherheit

### Hacking Hardware

03.03.2020 | bdla

Tobias Scheible, M.Eng.

# LIVE E-Mails fälschen



The screenshot shows a web browser window with the address bar displaying `https://lab.scheible.it/itsecurity/demos/fakemailsender/`. The page header features the logo of Tobias Scheible, IT Forensics & Web Development Lab, which consists of an orange flask icon. The main heading is "Fake Mail Sender" with the subtitle "Example to show how an Mail sender can be faked." Below this, there is a form with three input fields: "Sender Mail", "Sender Name", and "Receiver Mail". A "send mail" button is located at the bottom right of the form area. The footer of the page contains the copyright information "© Tobias Scheible tobias@scheible.it" and a link to the "Homepage | scheible.it Blog".

Bedrohungen aus dem Internet  
IT-Sicherheit im Planungsbüro

## Cyber Security

### Social Engineering

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

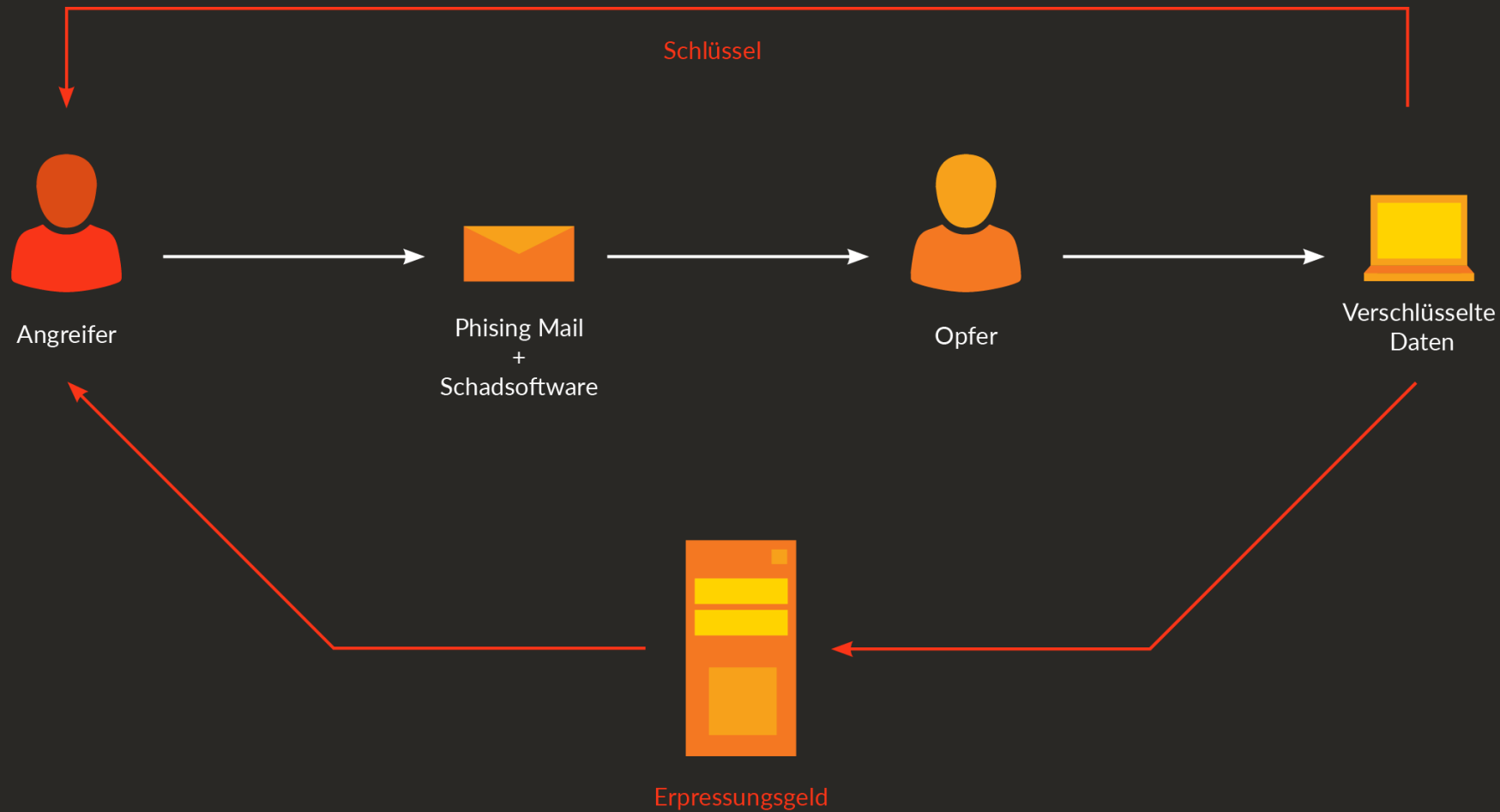
### Passwortsicherheit

### Hacking Hardware

03.03.2020 | bdlA

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

# 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.

A photograph of a server room with a strong blue color cast. In the foreground, several network cables are plugged into a patch panel, with their indicator lights glowing green. The background shows rows of server racks with more green lights. A semi-transparent orange banner is overlaid at the bottom of the image.

Passwortsicherheit

# Faktor Mensch

Bedrohungen aus dem Internet  
IT-Sicherheit im Planungsbüro



Cyber Security

Social Engineering

Passwortsicherheit

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

Hacking Hardware

03.03.2020 | bdla

Tobias Scheible, M.Eng.



# Faktor Mensch



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

Bedrohungen aus dem Internet  
IT-Sicherheit im Planungsbüro

Cyber Security

Social Engineering

Passwortsicherheit

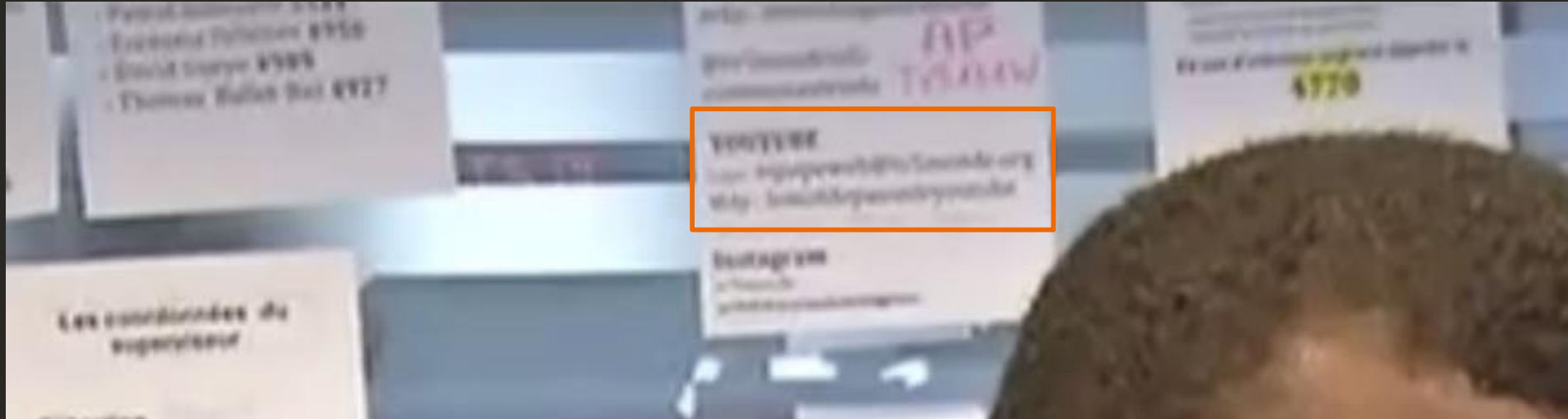
- Faktor Mensch
- Bekannte Passwörter
- Gehackte Accounts
- Passwörter verraten
- Zwei-Faktor-Authentisierung
- Passwortmanager

Hacking Hardware

03.03.2020 | bdla

Tobias Scheible, M.Eng.

# Faktor Mensch



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

## Cyber Security

### Social Engineering

#### Passwortsicherheit

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

#### Hacking Hardware

# Faktor Mensch



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

Bedrohungen aus dem Internet  
IT-Sicherheit im Planungsbüro

Cyber Security

Social Engineering

Passwortsicherheit

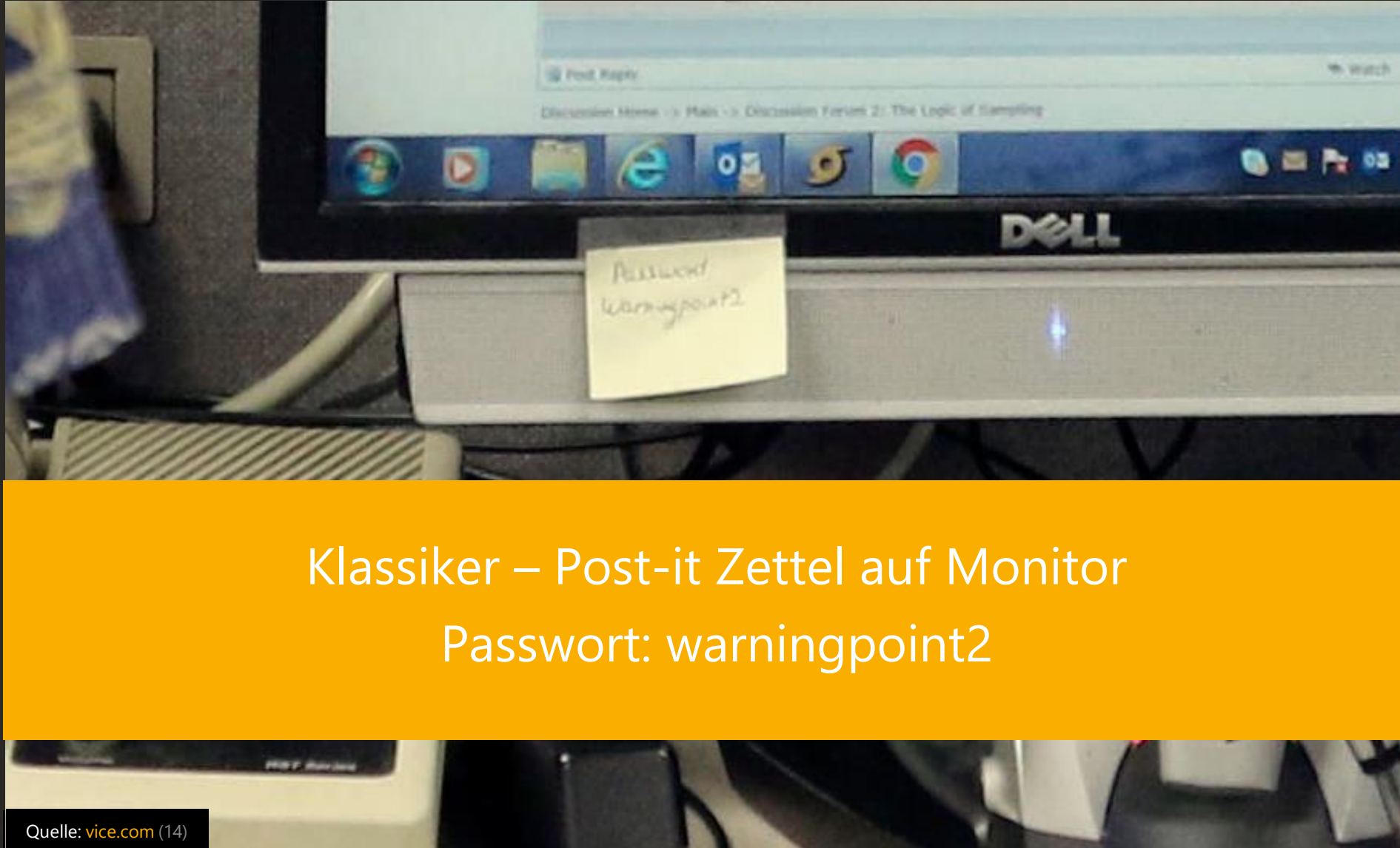
- Faktor Mensch
- Bekannte Passwörter
- Gehackte Accounts
- Passwörter verraten
- Zwei-Faktor-Authentisierung
- Passwortmanager

Hacking Hardware

03.03.2020 | bdla

Tobias Scheible, M.Eng.

# Faktor Mensch



Klassiker – Post-it Zettel auf Monitor  
Passwort: warningpoint2

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

Bedrohungen aus dem Internet  
IT-Sicherheit im Planungsbüro

Cyber Security

Social Engineering

Passwortsicherheit

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

Hacking Hardware

03.03.2020 | bdla

Tobias Scheible, M.Eng.

# Bekannte Passwörter

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](https://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

email address

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

Why 1Password?

340	6,474,028,664	87,569	96,065,928
pwned websites	pwned accounts	pastes	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](https://haveibeenpwned.com) (16)

Bedrohungen aus dem Internet  
IT-Sicherheit im Planungsbüro

## Cyber Security

## Social Engineering

## Passwortsicherheit

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

## Hacking Hardware

03.03.2020 | bdla

Tobias Scheible, M.Eng.

# Passwörter verraten



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

Bedrohungen aus dem Internet  
IT-Sicherheit im Planungsbüro

Cyber Security

Social Engineering

Passwortsicherheit

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

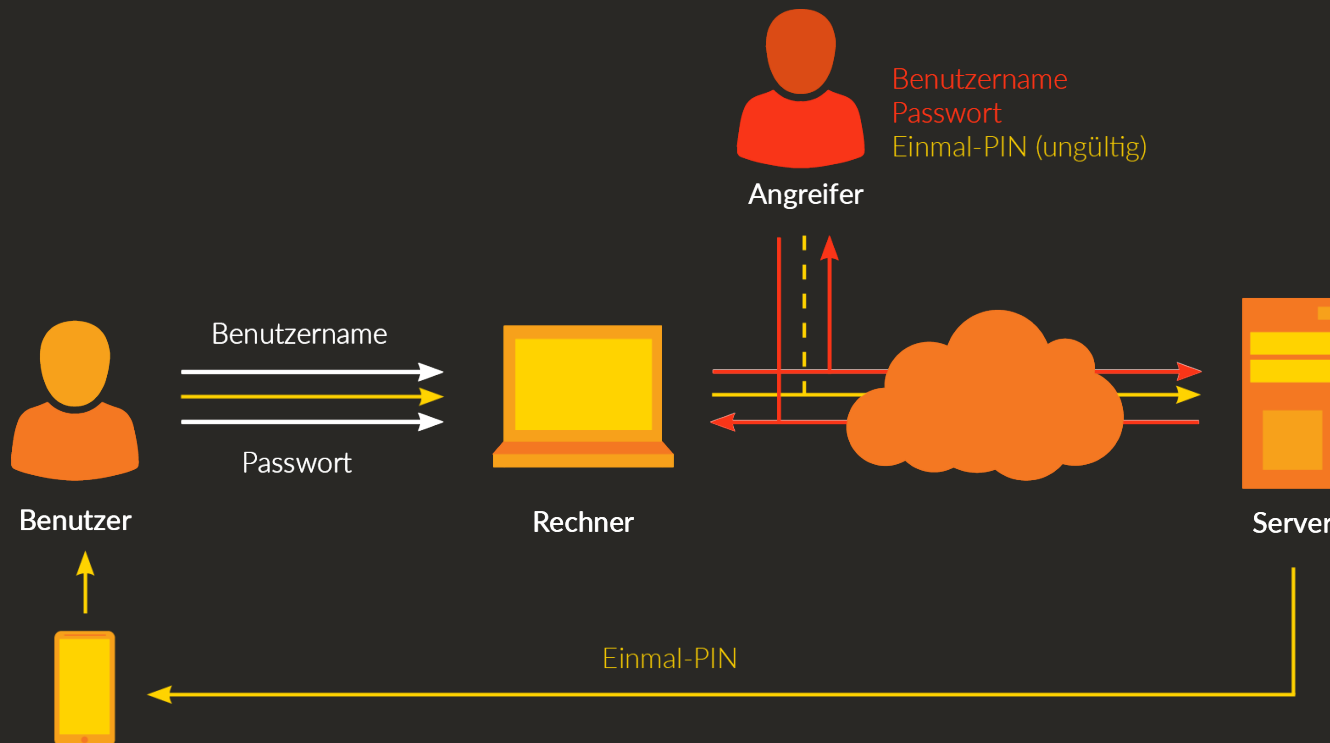
Hacking Hardware

03.03.2020 | bdla

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 von der Bezahlung per EC-Karte (Pin + Karte)



Bedrohungen aus dem Internet  
IT-Sicherheit im Planungsbüro

Cyber Security

Social Engineering

Passwortsicherheit

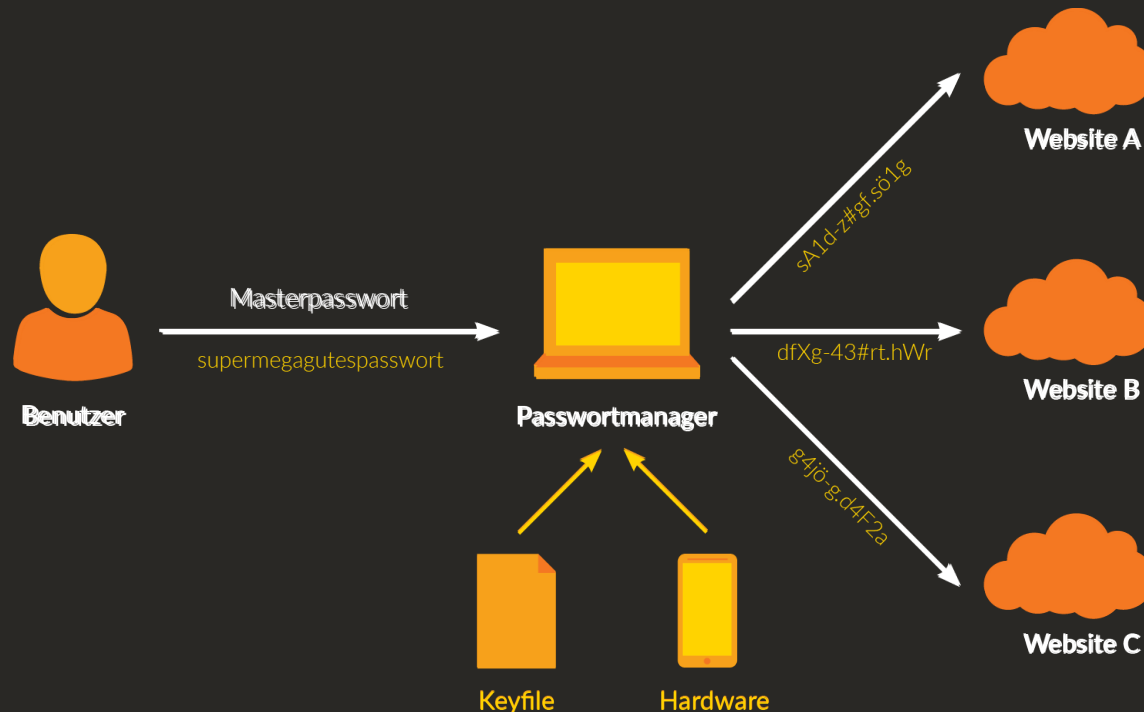
Faktor Mensch  
Bekannte Passwörter  
Gehackte Accounts  
Passwörter verraten  
Zwei-Faktor-Authentisierung  
Passwortmanager

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

# 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

Bedrohungen aus dem Internet  
IT-Sicherheit im Planungsbüro



Cyber Security

Social Engineering

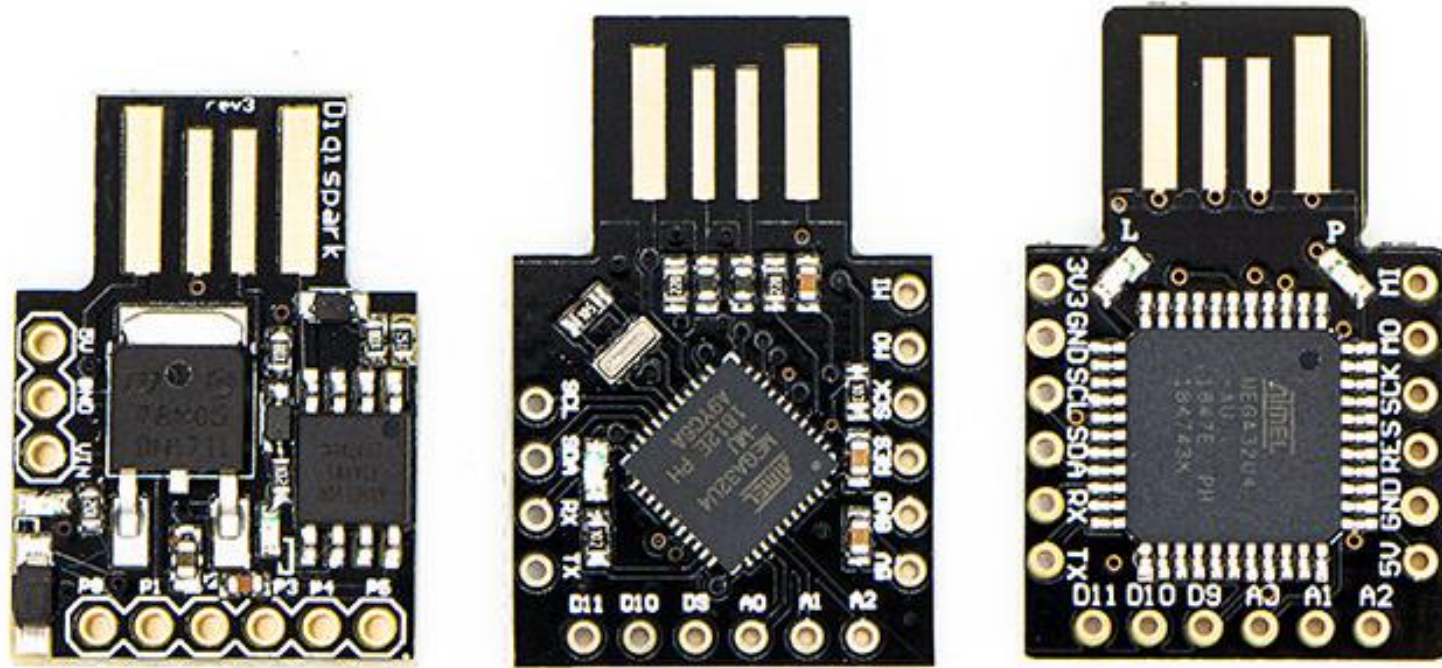
Passwortsicherheit

Hacking Hardware

[Hardware Tools](#)

[BadUSB](#)

# LIVE BadUSB



Bedrohungen aus dem Internet  
IT-Sicherheit im Planungsbüro

Cyber Security

Social Engineering

Passwortsicherheit

Hacking Hardware

Hardware Tools

BadUSB

# 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=5M9k7wfiWil>, 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\\_\(Schadprogramm\)](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/3025924727584002/>, 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](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/symfobroute/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=opRMrEfAlil>, abgerufen am 19.11.2019