



Tobias Scheible, M.Eng.

Cyber Security Vortrag  
Digitales Partner Forum

- 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

- Schadsoftware
- Ransomware
- Aktueller Vorfall

## ■ Social Engineering

- Gefängnisausbruch
- Fallbeispiel Locky
- SMS fälschen

## ■ Passwortsicherheit

- Faktor Mensch
- Gehackte Accounts
- Passwortlisten

## ■ Zielgerichtete Angriffe

- Problematische Hardware
- Systeme suchen

# Cyber Security

# Entwicklung 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

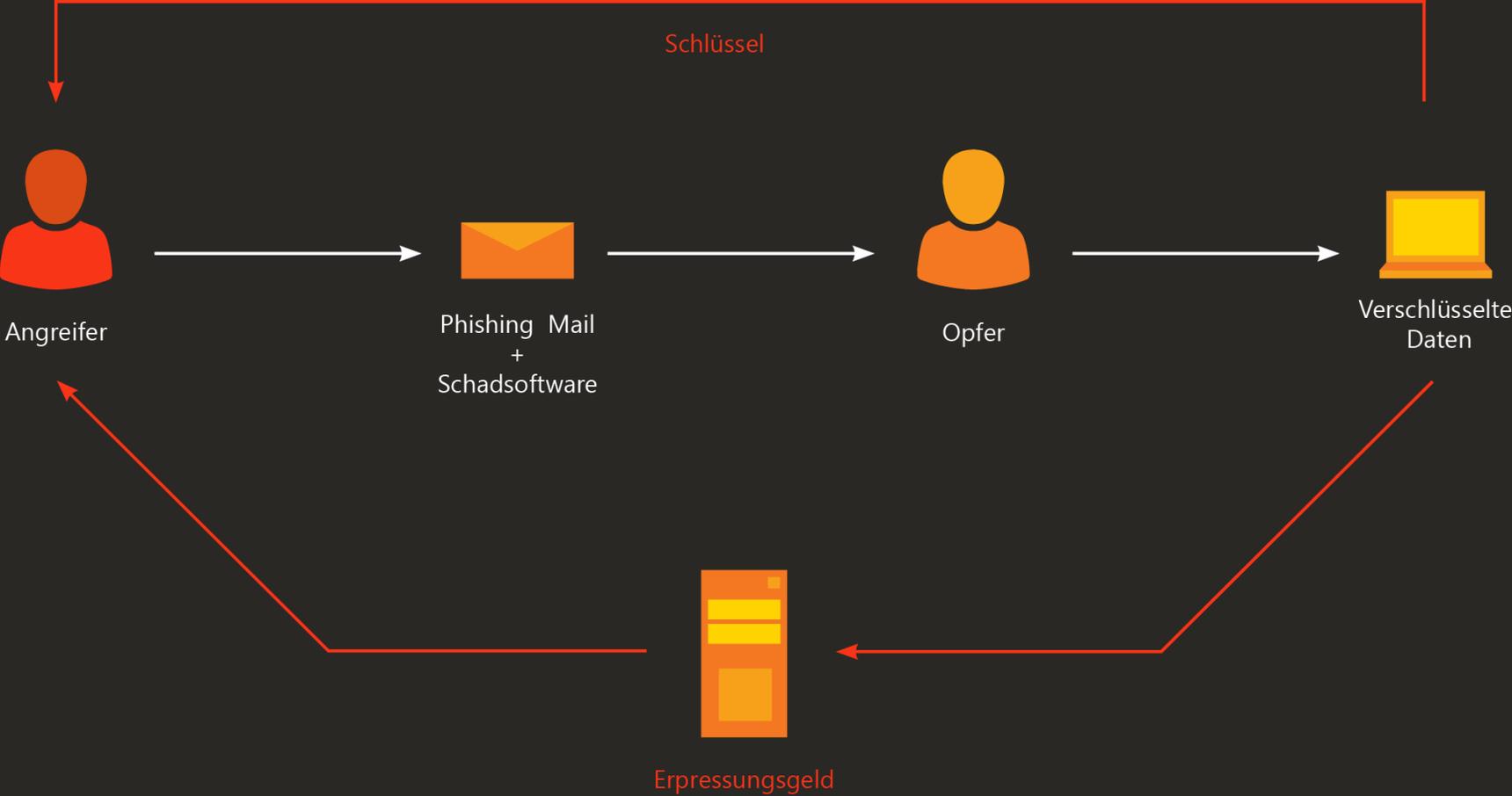
## ■ Ausnutzung von Schwachstellen

- 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

# Ransomware



**Cyber Security**  
Schadsoftware  
Ransomware  
Aktueller Vorfall

**Social Engineering**

**Passwortsicherheit**

**Zielgerichtete Angriffe**

# Ransomware - 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

```
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.

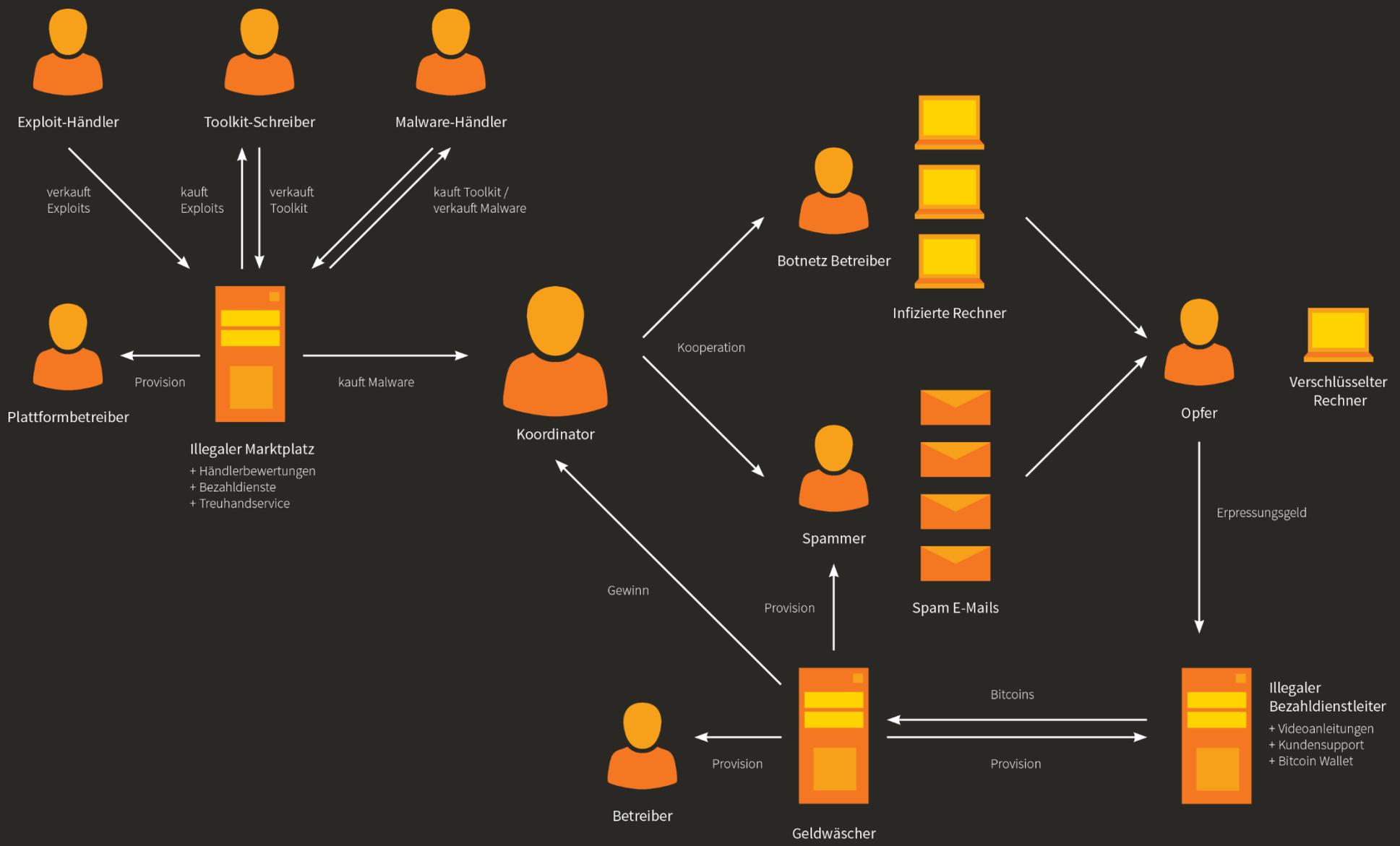
Important reference numbers: A5599796-2695577-

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](#) (2)

# Organisierte Kriminalität



**Cyber Security**  
Schadsoftware  
Ransomware  
Aktueller Vorfall

**Social Engineering**

**Passwortsicherheit**

**Zielgerichtete Angriffe**

München 17°

Süddeutsche Zeitung  
SZ.de Zeitung Magazin

Shop Jobs Immobilien Anzeigen  
Login Abo

Coronavirus Politik Wirtschaft Meinung Panorama Sport München Bayern Kultur Gesellschaft Wissen Reise Auto mehr...

Home > Digital > IT-Sicherheit > IT-Sicherheit: Wenn die Trinkwasserversorgung gehackt wird

Digital Klimaneutral

12. Februar 2021, 18:13 Uhr IT-Sicherheit

## Wenn die Trinkwasserversorgung gehackt wird



Der Sheriff von Oldsmar bei seiner Pressekonferenz am Montag. (Foto: AP)

**Hacker dringen ins System eines Wasserversorgers in Florida ein und erhöhen den Anteil von gefährlichem Ätznatron im Wasser. Dass dabei Menschen zu Schaden kommen konnten, stört die Angreifer offenbar nicht.**

Quelle: [sueddeutsche.de](https://www.sueddeutsche.de) (3)

Cyber Security  
Schadsoftware  
Ransomware  
Aktueller Vorfall

Social Engineering

Passwortsicherheit

Zielgerichtete Angriffe

# FAZIT Cyber Security

- Cyberkriminelle führen Angriffe aus, um Geld zu erbeuten.
- Die Akteure sind der organisierten Kriminalität zuzuordnen.
- Oft ist es ein loser Verbund aus verschiedenen Gruppierungen, die spezialisierte Aufgaben isoliert ausführen.
- Allerdings gibt es auch immer wieder Innentäter, die aus persönlichen Motiven wie Rache handeln.
- Diese setzen häufig alte Passwörter, die immer noch aktiv sind oder überall gleich sind, oder sehr simple Tools ein.



# 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

Gefängnisausbruch  
Fallbeispiel Locky  
SMS fälschen

### Passwortsicherheit

### Zielgerichtete Angriffe

# 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

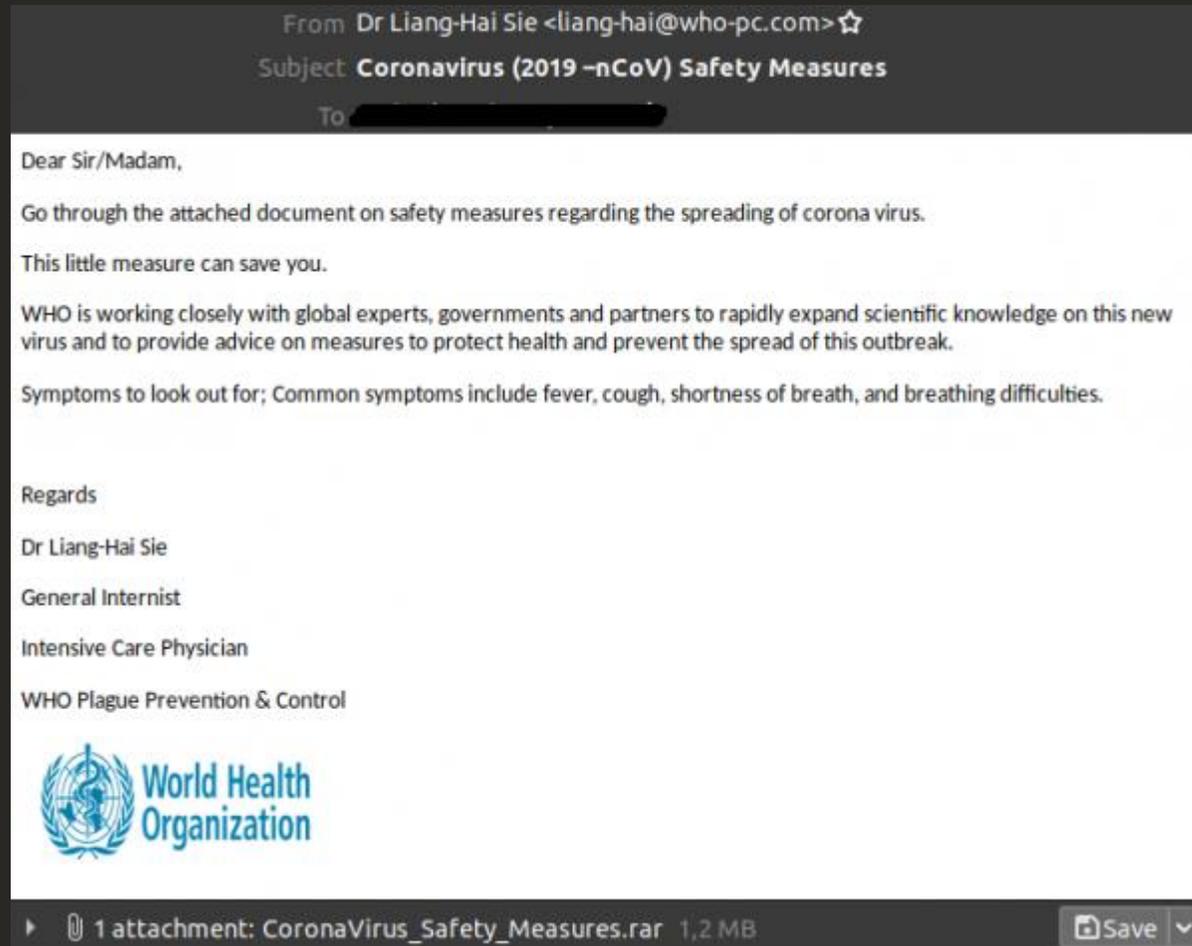
### Social Engineering

Gefängnisausbruch  
Fallbeispiel Locky  
SMS fälschen

### Passwortsicherheit

### Zielgerichtete Angriffe

# Mails fälschen



## Cyber Security

### Social Engineering

- Gefängnisausbruch
- Fallbeispiel Locky
- SMS fälschen

### Passwortsicherheit

### Zielgerichtete Angriffe

# LIVE SMS fälschen

Fake SMS Sender - Lab | scheible x +

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

Fake SMS Sender -...

 **Demonstration Lab**  
IT Security & IT Forensics Examples

## Fake SMS Sender

Example to show how an SMS sender can be faked.

Receiver Number

Sender Number

send sms

Cyber Security Lab

© 2021 Tobias Scheible

## Cyber Security

### Social Engineering

Gefängnisausbruch  
Fallbeispiel Locky  
SMS fälschen

### Passwortsicherheit

### Zielgerichtete Angriffe

# 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

00000000



Cyber Security

Social Engineering

Passwortsicherheit

Faktor Mensch

Passwortlisten

Gehackte Accounts

Zielgerichtete Angriffe

Cyber Security

Social Engineering

Passwortsicherheit

Faktor Mensch

Passwortlisten

Gehackte Accounts

Zielgerichtete Angriffe

00000000

Launch-Code für die in den USA  
stationierten Atomraketen

(1962 bis 1977)

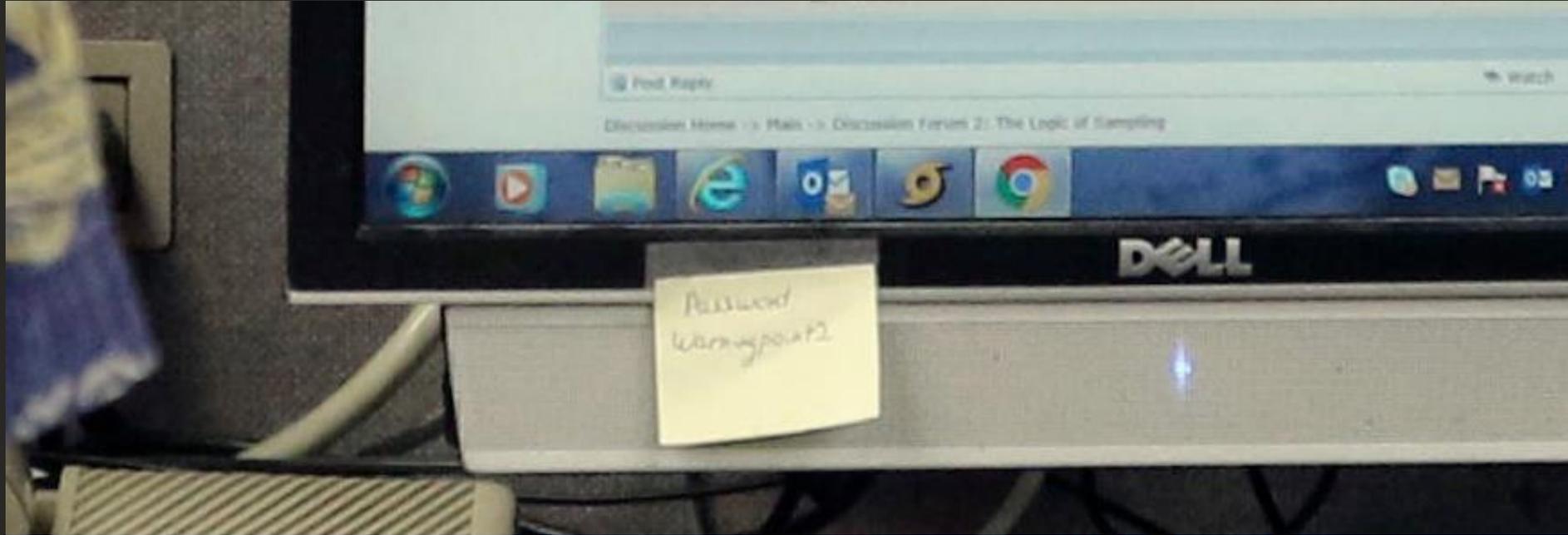
# Faktor Mensch



Quelle: [vice.com](https://www.vice.com) (8)

- Cyber Security
- Social Engineering
- Passwortsicherheit
  - Faktor Mensch
  - Passwortlisten
  - Gehackte Accounts
- Zielgerichtete Angriffe

# Faktor Mensch



Klassiker – Post-it Zettel auf Monitor  
Passwort: warningpoint2

Cyber Security

Social Engineering

Passwortsicherheit

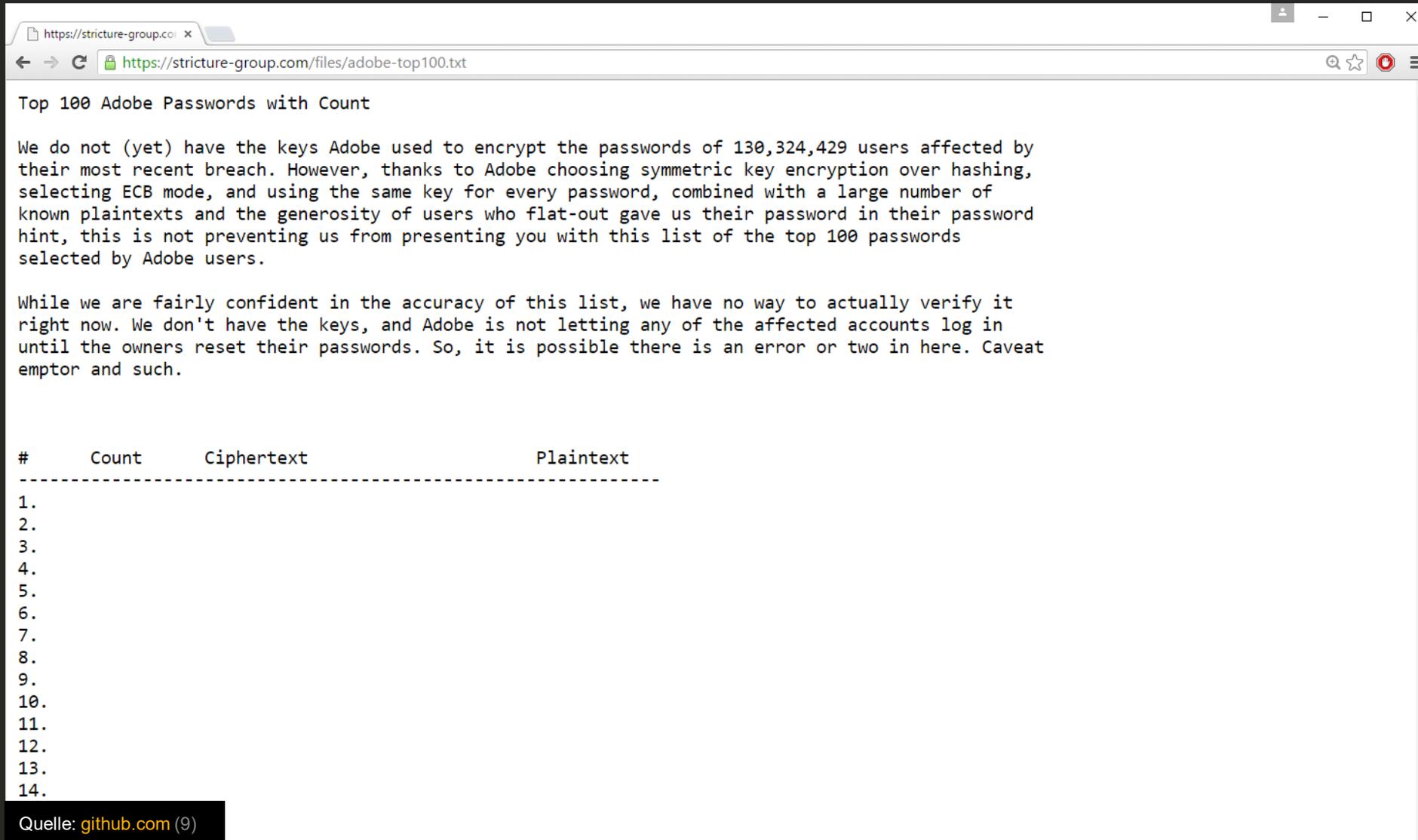
Faktor Mensch

Passwortlisten

Gehackte Accounts

Zielgerichtete Angriffe

# Passwortlisten



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](#) (9)

## Cyber Security

## Social Engineering

## Passwortsicherheit

Faktor Mensch

Passwortlisten

Gehackte Accounts

## Zielgerichtete Angriffe

# LIVE Gehackte Accounts

The screenshot shows the homepage of haveibeenpwned.com. At the top, there is a navigation bar with links: Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main heading is a large white box containing the text "';--have i been pwned?". Below this is a sub-heading: "Check if you have an account that has been compromised in a data breach". A search form is present with a text input field labeled "email address" and a button labeled "pwned?". Below the search form, there is a promotional banner for 1Password: "Generate secure, unique passwords for every account" with a link to "Learn more at 1Password.com".

Statistics section:

- 340 pwned websites
- 6,474,028,664 pwned accounts
- 87,569 pastes
- 96,065,928 paste accounts

Two columns of breach lists are shown:

- 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) (10)

## Cyber Security

### Social Engineering

### Passwortsicherheit

Faktor Mensch

Passwortlisten

Gehackte Accounts

### Zielgerichtete Angriffe

# 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.

# Zielgerichtete Angriffe

# Problematische Hardware

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

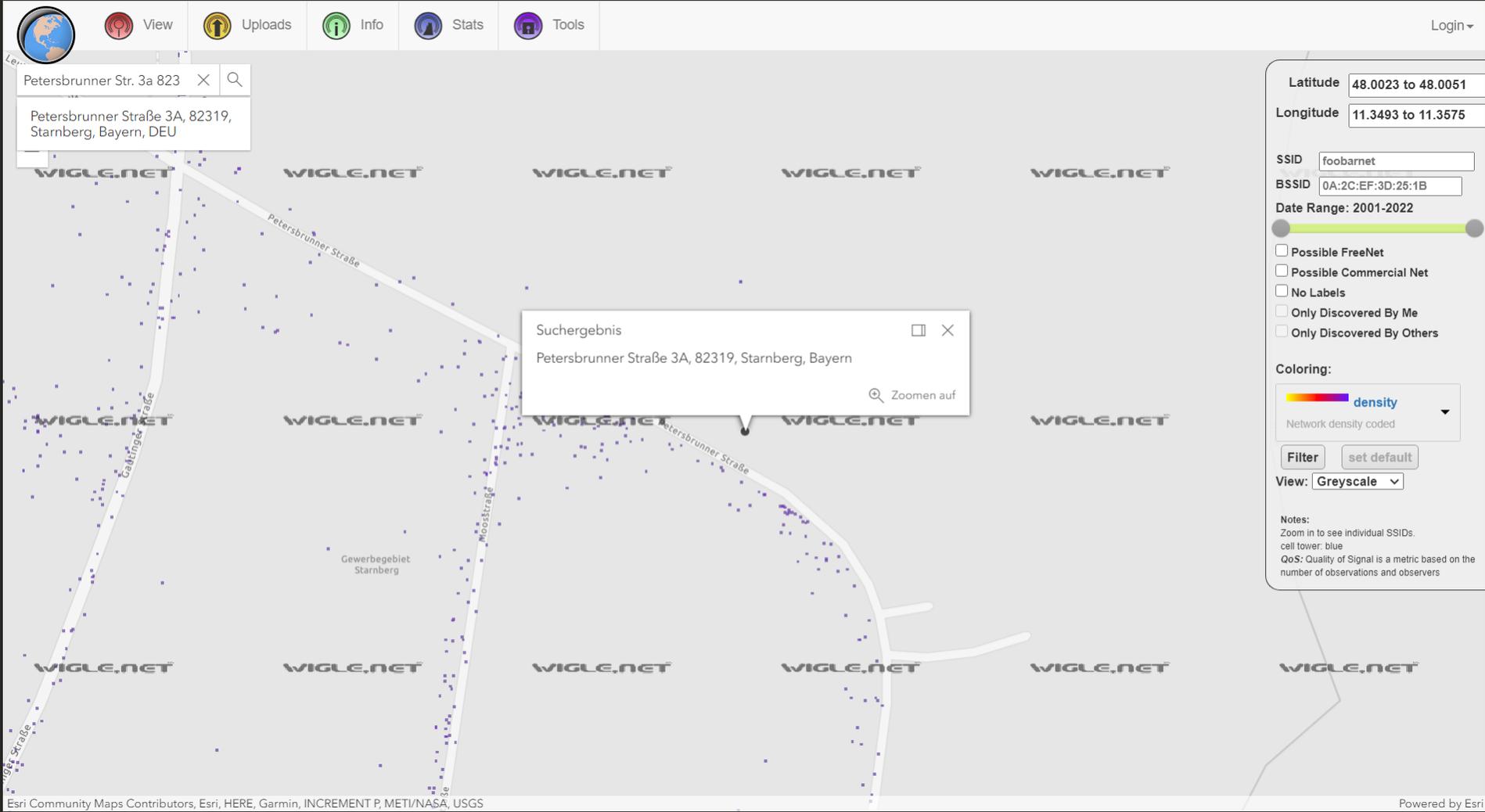


Die bei Aldi verkauften IP-Überwachungskameras der Marke Maginon haben massive Sicherheitsprobleme: Unbefugte könnten über das Internet auf das Kamerabild zugreifen und sogar den Ton anzapfen. Zudem verraten die Geräte unter anderem die Passwörter für WLAN, E-Mail und FTP-Zugang ihres Besitzers. Hunderte 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)

# Problematische Hardware



- Cyber Security
- Social Engineering
- Passwortsicherheit
- Zielgerichtete Angriffe
  - Problematische Hardware Systeme suchen

Quelle: [wigle.net](http://wigle.net) (12)

# Systeme suchen

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.



### 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!



### 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.



### 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](#) (13)

Cyber Security

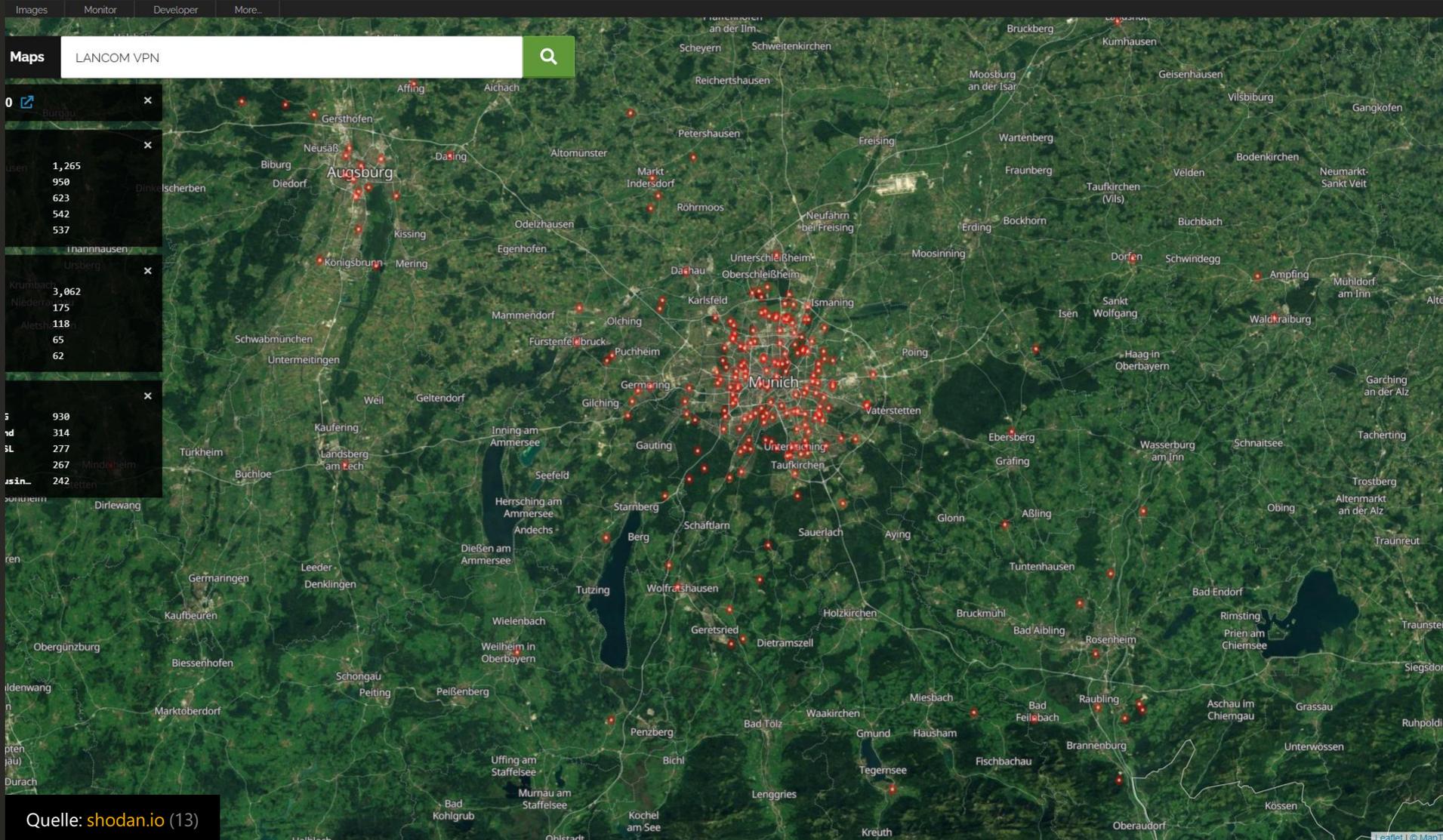
Social Engineering

Passwortsicherheit

Zielgerichtete Angriffe

Problematische Hardware  
Systeme suchen

# LIVE Systeme suchen



Quelle: [shodan.io](https://shodan.io) (13)

## Cyber Security

## Social Engineering

## Passwortsicherheit

## Zielgerichtete Angriffe

Problematische Hardware  
Systeme suchen

# FAZIT Zielgerichtete Angriffe

- Geräte oder Anwendungen, die im Internet sind, können nicht durch komplizierte Links oder weil die Adresse nirgendwo steht, geschützt werden.
- Die Standard-Passwörter von Geräten, die mit dem Internet verbunden sind, müssen immer geändert werden.
- Komponenten können sich auch selbstständig mit dem Internet verbinden, daher muss die Konfiguration immer geprüft werden.
- Alle Systeme, die online sind, werden von speziellen Suchmaschinen gefunden.



Vielen Dank  
Fragen?

# Quellen

- 1) <https://www.gdata.de/ratgeber/was-ist-eigentlich-die-geschichte-der-malware>
- 2) [https://de.wikipedia.org/wiki/AIDS\\_\(Schadprogramm\)](https://de.wikipedia.org/wiki/AIDS_(Schadprogramm))
- 3) <https://www.sueddeutsche.de/digital/it-sicherheit-hacker-wasserwerk-florida-1.5205113>
- 4) <http://www.heise.de/newsticker/meldung/Gefaengnisausbruch-mittels-E-Mail-Betrug-2587303.html>
- 5) <https://de.wikipedia.org/wiki/Locky>
- 6) <https://www.datensicherheit.de/corona-virus-gefaehrliche-e-mails-virulent>
- 7) <http://www.heise.de/security/meldung/00000000-Passwort-fuer-US-Atomraketen-2060077.html>
- 8) [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)
- 9) <https://github.com/morontt/symfobroute/blob/master/adobe-top100.txt>
- 10) <https://haveibeenpwned.com>
- 11) <http://www.heise.de/security/meldung/IP-Kameras-von-Aldi-als-Sicherheits-GAU-3069735.html>
- 12) <https://wagle.net>
- 13) <https://shodan.io>