



**Hochschule
Albstadt-Sigmaringen**
University of Applied Sciences

Fakultät Informatik

Cyber Security
Angreifer & Bedrohungen verstehen
Wintertagung 2019 - LBB

Tobias Scheible, M.Eng.

Tobias Scheible, M.Eng.

- Studium Kommunikations- und Softwaretechnik, Fachrichtung Kommunikationstechnik, Hochschule Albstadt-Sigmaringen
- 2009 bis 2012: Softwareingenieur im Bereich Web Development
- Seit 2012: Wissenschaftlicher Mitarbeiter an der Hochschule Albstadt-Sigmaringen im Bereich IT-Sicherheit & Digitale Forensik
 - Bachelorstudiengang IT Security
 - Institut für Wissenschaftliche Weiterbildung



Cyber Security
Angreifer & Bedrohungen verstehen

Praktikum Cybersecurity

IT Security (Bachelor) – 4. Semester
Prof. Holger Morgenstern

Seminar Cybersecurity

IT Security (Bachelor) – 4. Semester
Prof. Holger Morgenstern

Digitale Forensik

IT Security (Bachelor) – 5. Semester
Prof. Holger Morgenstern

Projektstudium

IT Security (Bachelor) – 5. Semester
Prof. Holger Morgenstern

Grundlagen Digitale Forensik

IT GRC Management – 4. Semester
Prof. Dr. Stefan Ruf

Workshops & Vorträge

LKA, VDI, IHK, Sparkasse, ...
Online veröffentlicht: <https://scheible.it>

Hochschule Albstadt-Sigmaringen

- 1971 Gründung der Fachhochschule Sigmaringen

Fakultät
Engineering



Fakultät
Business Science
and Management

- 1988/89 Campus Albstadt



- 2004 Fachhochschule wird in Hochschule umbenannt

Fakultät Life
Sciences



Fakultät
Informatik

- 24 Bachelor- und Masterstudiengänge

- Weiterbildung (berufsbegleitende Angebote)

- Zertifikate, Data Science (Master), Digitale Forensik (Master) und IT GRC Management (Master)

Cyber Security
Angreifer & Bedrohungen verstehen

Bachelorstudiengänge

- + IT Security
- + Technische Informatik
- + Wirtschaftsinformatik

Masterstudiengänge

- + Business Analytics
- + Systems Engineering

Weiterbildungsangebote

- + Studium Initiale
- + Hochschulzertifikate
- + Data Science
- + Digitale Forensik
- + IT GRC Management

Weitere Informationen:
<http://hs-albsig.de/inf>

Cyber Security
Angreifer & Bedrohungen verstehen

Zahlen & Fakten



Cyber Security
Angreifer & Bedrohungen verstehen

Agenda

- Cyber Security
 - Schadsoftware
 - Aktuelle Vorfälle
 - Bug or Feature?
 - Suchmaschinen
 - Internet of Things
 - Cybercrime as a Service
- Social Engineering
 - Faktor Mensch
 - Website manipulieren
 - CEO Fraud
- Passwortsicherheit
 - Öffentliche Passwörter
 - Angriffe auf Passwörter
 - Sperrmuster
 - Sichere Passwörter
- Hardware Hacks
 - Probe Requests Scanner
 - Hardware Tools
 - BadUSB
- Zukünftige Entwicklung

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering

Passwortsicherheit

Hardware Hacks

Zukünftige Entwicklung

The background of the image is a complex, glowing circuit board pattern. The left side is dominated by warm orange and red tones, while the right side transitions into cooler blue and cyan hues. A horizontal band of solid blue color runs across the middle of the image. Overlaid on this background are several padlock icons. A large, glowing orange padlock is centered in the upper half. To its right, in the blue section, is a smaller, glowing blue padlock. In the bottom left corner, there is a faint, semi-transparent blue padlock. The text 'Cyber Security' is centered within the blue horizontal band.

Cyber Security

00000000
?

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security
[PIN Beispiel](#)
Schadsoftware
Aktuelle Vorfälle
Bug or Feature?
Suchmaschinen
Internet of Things
Cybercrime as a Service

Social Engineering

Passwortsicherheit

Hardware Hacks

Zukünftige Entwicklung

00000000

Launch-Code für die in den USA stationierten Atomraketen

(1962 bis 1977)

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security
[PIN Beispiel](#)
Schadsoftware
Aktuelle Vorfälle
Bug or Feature?
Suchmaschinen
Internet of Things
Cybercrime as a Service

Social Engineering

Passwortsicherheit

Hardware Hacks

Zukünftige Entwicklung

Atomraketen: Steuerungstechnik aus den 70ern



Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security
[PIN Beispiel](#)
Schadsoftware
Aktuelle Vorfälle
Bug or Feature?
Suchmaschinen
Internet of Things
Cybercrime as a Service

Social Engineering

Passwortsicherheit

Hardware Hacks

Zukünftige Entwicklung

Geschichte der Schadsoftware

■ Proof of Concept

- 80er Jahre Der Begriff Computervirus wird zum ersten Mal verwendet und erste Konzepte werden öffentlich vorgestellt und diskutiert
- 1985 Zum ersten Mal berichtet eine deutschsprachige Zeitung über Computerviren
- 1988 Zum ersten Mal werden Würmer (sich selbst replizierende Schadsoftware) eingesetzt

■ Ausnutzung von Schwachstellen

- 1997 Schadsoftware nutzt nun gezielt Schwachstellen in Programmen, Betriebssystemen oder in Hardware aus
- 2000 „I love you“ Virus findet auch in Deutschland große Verbreitung
- 2000 Erster Trojaner für mobile Endgeräte (PDAs)

■ Krimineller Hintergrund

- 2004 Schadsoftware wird immer mehr von organisierten Kriminellen eingesetzt
- 2005 Erster Wurm verbreitet sich automatisch auf Symbian Smartphones per MMS

Ransomware - AIDS

- Bereits 1989 wurden die ersten Angriffe mit Ransomware durchgeführt
- Die Schadsoftware wurde per 5,25“ Diskette ca. 20.000 Mal mit der Post verschickt
- Nach 90 Starts wurden die Dateinamen auf dem Laufwerk C: 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://www.wikipedia.org) (4)

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security
PIN Beispiel
[Schadsoftware](#)
Aktuelle Vorfälle
Bug or Feature?
Suchmaschinen
Internet of Things
Cybercrime as a Service

Social Engineering

Passwortsicherheit


Hardware Hacks

Zukünftige Entwicklung

.....
25.01.2019 | Wintertagung 2019 - LBB

Tobias Scheible, M.Eng.



Aktuelle Vorfälle - Doxing

 München 1°

Süddeutsche Zeitung

SZ.de Zeitung Magazin


Shop Jobs Immobilien Anzeigen
[Login](#) [Abo](#)

 Politik Wirtschaft Panorama Sport München Bayern Kultur Gesellschaft Wissen Digital Karriere Reise Auto Stil mehr... 



Home > Digital > IT-Sicherheit > Doxing - die alte Hacker-Waffe

8. Januar 2019, 12:22 Uhr Private Daten im Netz

Doxing - eine alte Hacker-Waffe trifft den deutschen Mainstream



Im Unterschied zum investigativen Journalismus oder Whistleblowing, ist die Intension beim Doxing, eine Person bloßzustellen oder einzuschüchtern. (Foto: imago/photothek)



Feedback

Schon in den Neunzigern nutzen Hacker die Entblößung ihrer Kontrahenten im Netz als digitalen Flammenwerfer. Heute wird damit schmutzig Politik gemacht.

Von [Jannis Brühl](#)

Für Schattenkrieger ist das Wichtigste, dass niemand ihr Gesicht und ihren Namen kennt. Deshalb fürchteten [Hacker](#) schon in den Neunzigern das, was die Szene später Doxing taufen sollte: Eine Person veröffentlicht strategisch eine

Quelle: [sueddeutsche.de](https://www.sueddeutsche.de) (5)

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security
PIN Beispiel
Schadsoftware
[Aktuelle Vorfälle](#)
Bug or Feature?
Suchmaschinen
Internet of Things
Cybercrime as a Service

Social Engineering

Passwortsicherheit

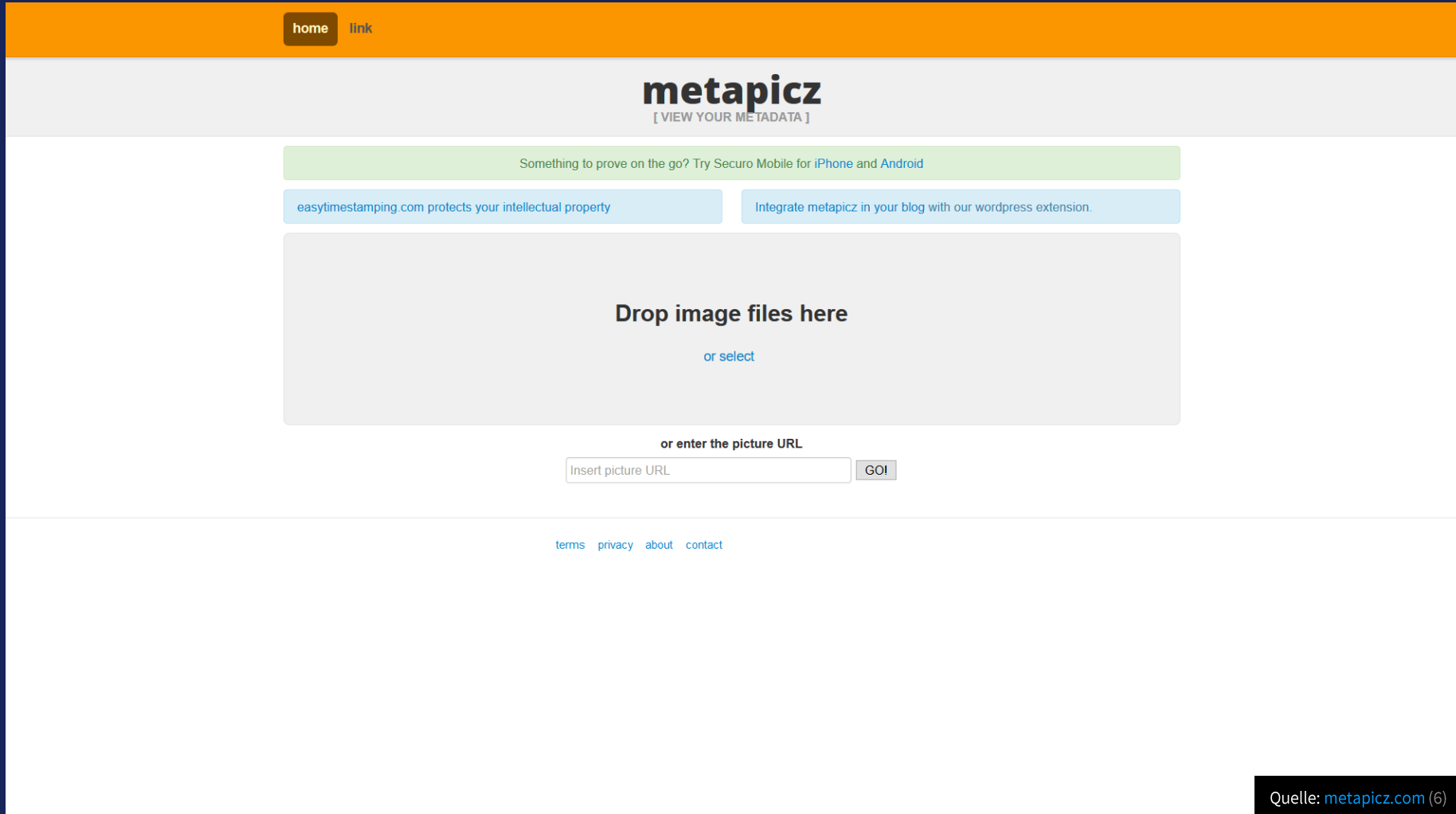
Hardware Hacks

Zukünftige Entwicklung

.....
25.01.2019 | Wintertagung 2019 - LBB

Tobias Scheible, M.Eng.

DEMO Versteckte Informationen auslesen



The screenshot shows the metapicz website. At the top is an orange navigation bar with 'home' and 'link' buttons. Below this is a grey header with the 'metapicz' logo and the tagline '[VIEW YOUR METADATA]'. The main content area has a green banner with the text 'Something to prove on the go? Try Securo Mobile for iPhone and Android'. Below the banner are two blue buttons: 'easytimestamping.com protects your intellectual property' and 'Integrate metapicz in your blog with our wordpress extension.'. The central part of the page is a large grey box with the text 'Drop image files here' and a link 'or select'. Below this is a section titled 'or enter the picture URL' with a text input field labeled 'Insert picture URL' and a 'GO!' button. At the bottom of the page is a footer with links for 'terms', 'privacy', 'about', and 'contact'.

Quelle: metapicz.com (6)

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security
PIN Beispiel
Schadsoftware
Aktuelle Vorfälle
Bug or Feature?
Suchmaschinen
Internet of Things
Cybercrime as a Service

Social Engineering

Passwortsicherheit

Hardware Hacks

Zukünftige Entwicklung

.....
25.01.2019 | Wintertagung 2019 - LBB

Tobias Scheible, M.Eng.

Aktuelle Vorfälle – Data Leaks


ABO SHOP AKADEMIE JOBS MEHR ▾

E-PAPER AUDIO APPS ARCHIV ANMELDEN

ZEIT  ONLINE

Suche



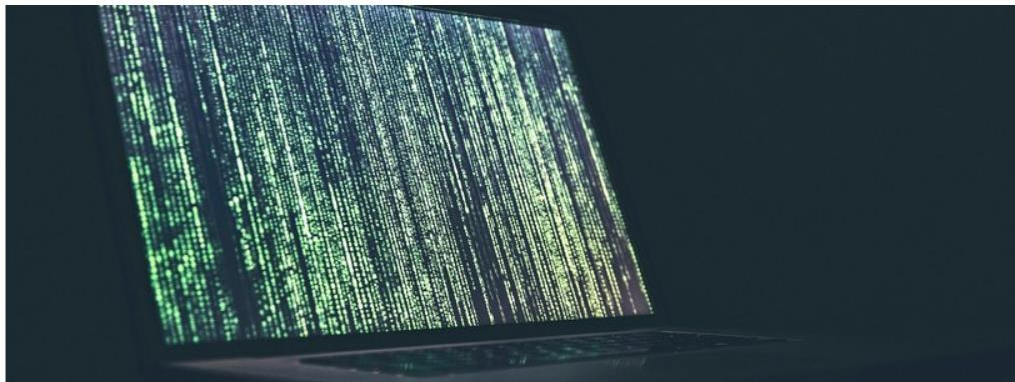
Politik Gesellschaft Wirtschaft Kultur ▾ Wissen **Digital** Campus ▾ Arbeit Entdecken Sport ZEITmagazin Podcasts mehr ▾ 

Datenleak

Millionen Passwörter im Netz veröffentlicht

Ein IT-Sicherheitsexperte hat im Internet ein riesiges Datenleak entdeckt. Zahlreiche E-Mail-Adressen und Passwörter von privaten Nutzern sind demnach frei zugänglich.

17. Januar 2019, 15:22 Uhr / Quelle: ZEIT ONLINE, dpa, jci / [82 Kommentare](#)



Quelle: [zeit.de](#) (7)

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security
PIN Beispiel
Schadsoftware
Aktuelle Vorfälle
Bug or Feature?
Suchmaschinen
Internet of Things
Cybercrime as a Service

Social Engineering

Passwortsicherheit

Hardware Hacks

Zukünftige Entwicklung

.....
25.01.2019 | Wintertagung 2019 - LBB

Tobias Scheible, M.Eng.

DEMO Bug or Feature?

Cyber Security Angreifer & Bedrohungen verstehen

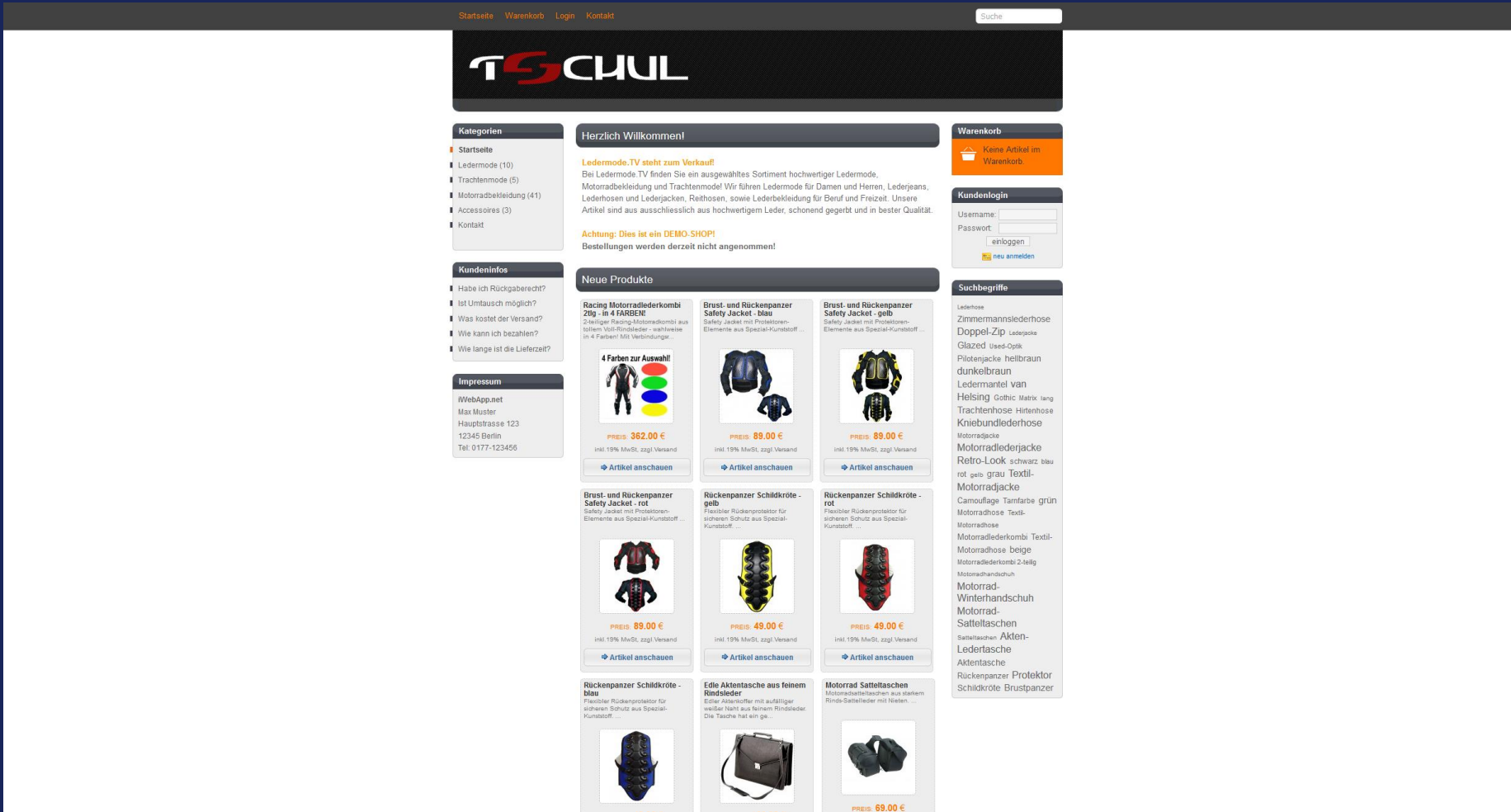
- Cyber Security
- PIN Beispiel
- Schadsoftware
- Aktuelle Vorfälle
- Bug or Feature?
- Suchmaschinen
- Internet of Things
- Cybercrime as a Service

Social Engineering

Passwortsicherheit

Hardware Hacks

Zukünftige Entwicklung



Suchmaschinen - Hacking mit Google



Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security
PIN Beispiel
Schadsoftware
Aktuelle Vorfälle
Bug or Feature?
Suchmaschinen
Internet of Things
Cybercrime as a Service

Social Engineering

Passwortsicherheit

Hardware Hacks

Zukünftige Entwicklung

Suchmaschinen - Hacking mit Google

Parameter	Beschreibung
site:	Eine Suche mit dem Suchparameter "site" in Verbindung mit einer Domain oder URL liefert alle Seiten dieser Domain, die verfügbar sind. Beispiel: <i>it security site:hs-albsig.de</i>
intitle:	Eine Suche mit dem Suchparameter "intitle" in Verbindung mit einem Suchbegriff liefert Ergebnisse von Webseiten, deren Titel diesen Suchbegriff enthält. Beispiel: <i>intitle:"it security"</i>
inurl:	Eine Suche mit dem Suchparameter "inurl:" in Verbindung mit einem Suchbegriff liefert Ergebnisse von Webseiten, deren URL den Suchbegriff enthalten. Beispiel: <i>inurl:"it-security"</i>
intext:	Mit dem Suchparameter "intext" in Verbindung mit einem Suchbegriff werden Webseiten angezeigt, in denen der Begriff im Text der Seite vorkommt. Beispiel: <i>intext:"it security bachelor"</i>

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security
PIN Beispiel
Schadsoftware
Aktuelle Vorfälle
Bug or Feature?
[Suchmaschinen](#)
Internet of Things
Cybercrime as a Service

Social Engineering

Passwortsicherheit

Hardware Hacks

Zukünftige Entwicklung

DEMO Suchmaschinen - Hacking mit Google

- Beispiel Suchanfragen nach Webcams:
 - intitle:webcam 7 inurl:8080 -intext:8080
 - intext:"powered by webcamXP 5"
 - inurl:"viewerframe?mode=motion"
 - intitle:"Live View / - AXIS"
 - inurl:indexFrame.shtml
 - intitle:"EvoCam" inurl:"webcam.html"

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security
PIN Beispiel
Schadsoftware
Aktuelle Vorfälle
Bug or Feature?
[Suchmaschinen](#)
Internet of Things
Cybercrime as a Service


Social Engineering

Passwortsicherheit












Hardware Hacks

Zukünftige Entwicklung

Suchmaschinen - GHDB



EXPLOIT
DATABASE



Google Hacking Database

Filters

Reset All

Show 15

Quick Search

Date Added	Dork	Category	Author
2019-01-17	inurl:/setup.cgi@next_file	Various Online Devices	ManhNho
2019-01-14	intitle:"Index of /" inurl:passport	Sensitive Directories	Bl4k43m0n
2019-01-14	intext:"- 2019 Cott Systems, Inc."	Web Server Detection	FlyingFrog
2019-01-14	"I have been invoked by servletToJSP"	Web Server Detection	g.go
2019-01-09	inurl:/sasp/bc/bap	Pages Containing Login Portals	FlyingFrog
2019-01-09	inurl:/rj/portal	Pages Containing Login Portals	FlyingFrog
2019-01-09	inurl:/scripts/wgate	Network or Vulnerability Data	FlyingFrog
2019-01-09	inurl:infoviewapp	Pages Containing Login Portals	FlyingFrog
2019-01-09	inurl:"/rj/go/km/docs/"	Sensitive Directories	FlyingFrog
2019-01-09	inurl:"/rj/go/km/" intext:navigation	Sensitive Directories	FlyingFrog
2019-01-09	inurl:"/webdynpro/resources/sap.com/"	Sensitive Directories	FlyingFrog
2019-01-09	filetype:cwr inurl:apstoken	Pages Containing Login Portals	FlyingFrog
2019-01-09	inurl:apassword	Files Containing Juicy Info	FlyingFrog
2019-01-02	filetype:pub "ssh-rsa"	Files Containing Juicy Info	Kevin Randall
2019-01-02	filetype:doc "Answer Key"	Files Containing Juicy Info	Kevin Randall

Showing 1 to 15 of 4,584 entries

FIRST

PREVIOUS

1

2

3

4

5

...

306

NEXT

LAST

Downloads

Certifications

Training

Professional Services

Kali Linux

Kali NetHunter

Kali Linux Revealed Book

OSCP

OSWP

OSCE

OSEE

OSWE

KLCP

Penetration Testing with Kali Linux (PWK)

Offensive Security Wireless Attacks (WiFi)

Cracking the Perimeter (CTP)

Metasploit Unleashed (MSFU)

Free Kali Linux Training

Penetration Testing

Advanced Attack Simulation

Application Security Assessment

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security
PIN Beispiel
Schadsoftware
Aktuelle Vorfälle
Bug or Feature?
Suchmaschinen
Internet of Things
Cybercrime as a Service

Social Engineering

Passwortsicherheit

Hardware Hacks

Zukünftige Entwicklung

Quelle: exploit-db.com (10)










25.01.2019 | Wintertagung 2019 - LBB

Tobias Scheible, M.Eng.

20

IoT - Bug or Feature?

 **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)

Drei Modelle sind betroffen

Die Kameras IPC-10 AC, IPC-100 AC und IPC-20 C hat Aldi mit einer Firmware

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security
PIN Beispiel
Schadsoftware
Aktuelle Vorfälle
Bug or Feature?
Suchmaschinen
Internet of Things
Cybercrime as a Service

Social Engineering

Passwortsicherheit

Hardware Hacks

Zukünftige Entwicklung

IoT - Suchmaschine für das Internet der Dinge



The screenshot shows the Shodan website homepage. At the top, there's a navigation bar with links for Shodan, Developers, Blog, and View All. A search bar is prominently displayed with the Shodan logo. Below the navigation bar, a large banner features the text "The search engine for Security" and "Shodan is the world's first search engine for Internet-connected devices." There are two buttons: "Create a Free Account" and "Getting Started". The main content area is divided into four sections: "Explore the Internet of Things", "See the Big Picture", "Monitor Network Security", and "Get a Competitive Advantage". Each section has a brief description and an icon. Below this, a blue banner highlights "56% of Fortune 100" and "1,000+ Universities" using Shodan. The bottom section, "Analyze the Internet in Seconds", describes Shodan's global server network and provides a "Sample Report on Heartbleed" link. The footer mentions "Beyond the Web" and lists integrations with various tools like Nmap, Metasploit, and Firefox.

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security
PIN Beispiel
Schadsoftware
Aktuelle Vorfälle
Bug or Feature?
Suchmaschinen
Internet of Things
Cybercrime as a Service

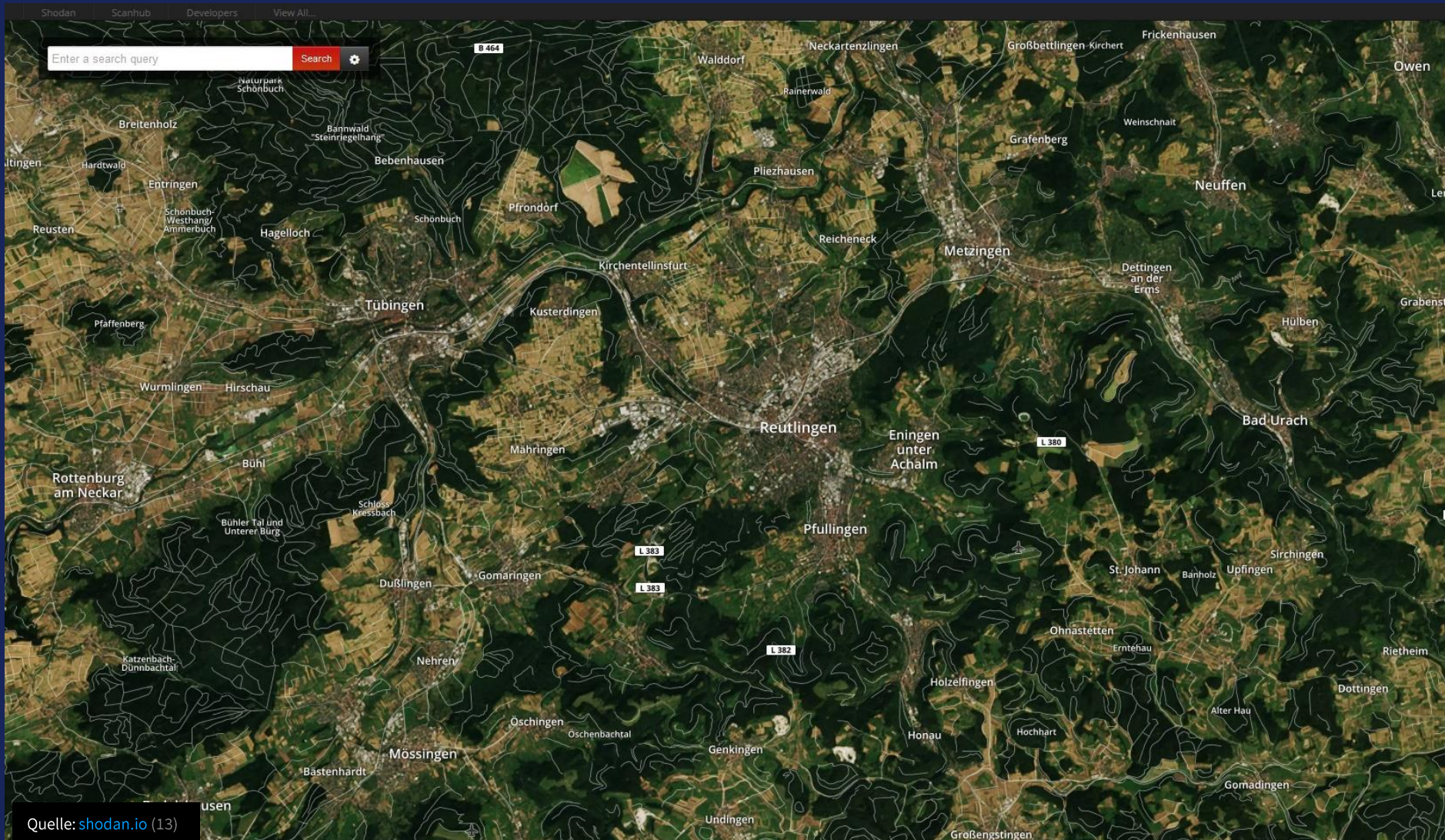
Social Engineering

Passwortsicherheit

Hardware Hacks

Zukünftige Entwicklung

DEMO IoT - Webcams mit Shodan finden



Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security
PIN Beispiel
Schadsoftware
Aktuelle Vorfälle
Bug or Feature?
Suchmaschinen
[Internet of Things](#)
Cybercrime as a Service

Social Engineering

Passwortsicherheit

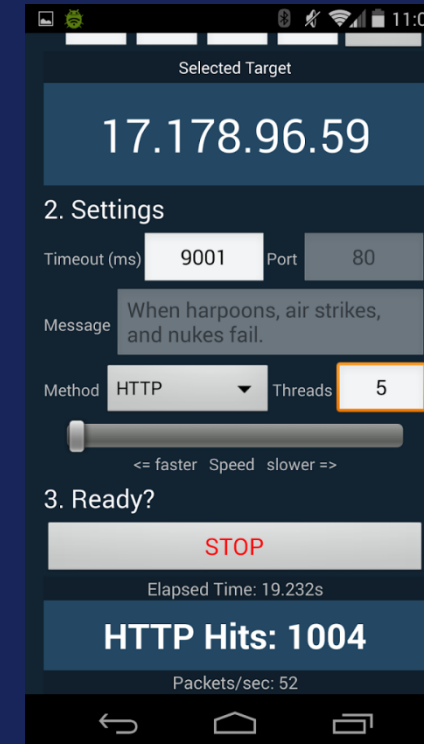
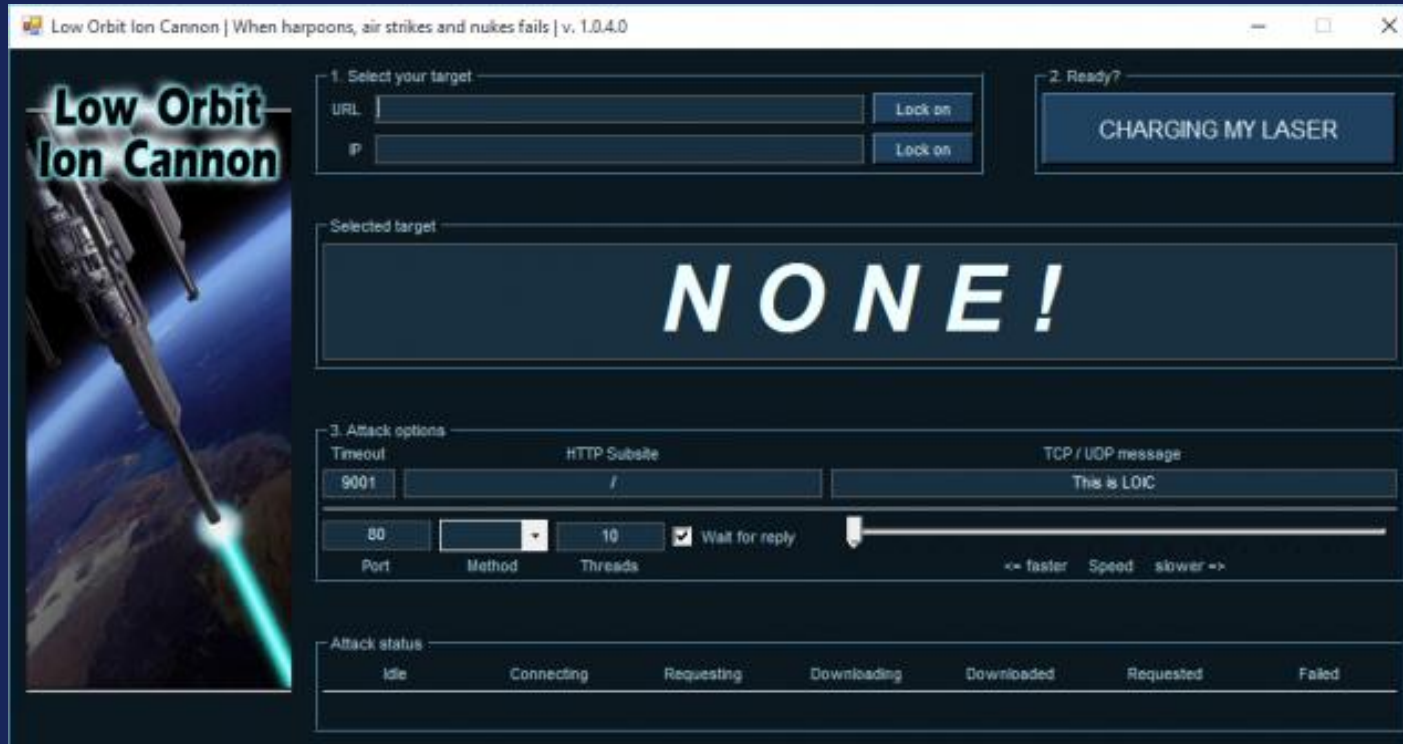
Hardware Hacks

Zukünftige Entwicklung

.....
25.01.2019 | Wintertagung 2019 - LBB

Tobias Scheible, M.Eng.

Cybercrime as a Service - Hackaktivisten



Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security
PIN Beispiel
Schadsoftware
Aktuelle Vorfälle
Bug or Feature?
Suchmaschinen
Internet of Things
[Cybercrime as a Service](#)

Social Engineering

Passwortsicherheit

Hardware Hacks

Zukünftige Entwicklung

Cybercrime as a Service



Quelle: [youtube.com](https://www.youtube.com/watch?v=16) (16)

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security
PIN Beispiel
Schadsoftware
Aktuelle Vorfälle
Bug or Feature?
Suchmaschinen
Internet of Things
Cybercrime as a Service

Social Engineering

Passwortsicherheit

Hardware Hacks

Zukünftige Entwicklung

.....
25.01.2019 | Wintertagung 2019 - LBB

Tobias Scheible, M.Eng.

Cybercrime as a Service



Koordinator

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security
PIN Beispiel
Schadsoftware
Aktuelle Vorfälle
Bug or Feature?
Suchmaschinen
Internet of Things
Cybercrime as a Service

Social Engineering

Passwortsicherheit

Hardware Hacks

Zukünftige Entwicklung

Cybercrime as a Service - Ransomware Locky

- Effektive Methode, um Geld zu ergaunern
- Auf deutsche Benutzer ausgerichtete Varianten
- Verschlüsselt alle Benutzerdateien, auch auf Netzwerklaufwerke
- 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
Angreifer & Bedrohungen verstehen

Cyber Security
PIN Beispiel
Schadsoftware
Aktuelle Vorfälle
Bug or Feature?
Suchmaschinen
Internet of Things
[Cybercrime as a Service](#)

Social Engineering

Passwortsicherheit

Hardware Hacks

Zukünftige Entwicklung

FAZIT Cyber Security

- 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.

Social Engineering



Was ist die häufigste Angriffsmethode?

Ausnutzung von Schwachstellen

A

Physische Attacken

B

Manipulation von Personen

C

Ausnutzung von Fehlern

D

Cyber Security
Angreifer & Bedrohungen verstehen

Faktor Mensch - Gefälschte E-Mail

Home | Video | Themen | Forum | English | DER SPIEGEL | SPIEGEL TV | Abo | Shop | Schlagzeilen | Wetter | TV-Programm | mehr ▼

SPIEGEL ONLINE SCHULSPIEGEL Login | Registrierung

Abi - und dann? | Querweltein | Leben U21 | Wissen

Nachrichten > SchulSPIEGEL > Wetter > Schulfrei in Niedersachsen wegen gefälschter E-Mail

Gefälschte E-Mail: Schulfrei ermöglicht



Winterwetter in Niedersachsen: Freier Tag im Schnee wegen gefälschter E-Mail

Eine gefälschte E-Mail hat Schülern in Niedersachsen einen freien Tag beschert. Der Unterricht falle wegen des Winterwetters aus, hieß es darin. Hunderte Schüler glaubten der Meldung - und blieben zu Hause.

Quelle: [spiegel.de](https://www.spiegel.de) (18)

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering
[Faktor Mensch](#)
Website manipulieren
CEO Fraud

Passwortsicherheit

Hardware Hacks

Zukünftige Entwicklung

Faktor Mensch - Beispiel



Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering
Faktor Mensch
Website manipulieren
CEO Fraud

Passwortsicherheit

Hardware Hacks

Zukünftige Entwicklung

Social Engineering - Gefängnisausbruch

- Moderner Ausbruch aus einem britischen Gefängnis (März 2015)
- Social Engineering 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
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering

Faktor Mensch

Website manipulieren

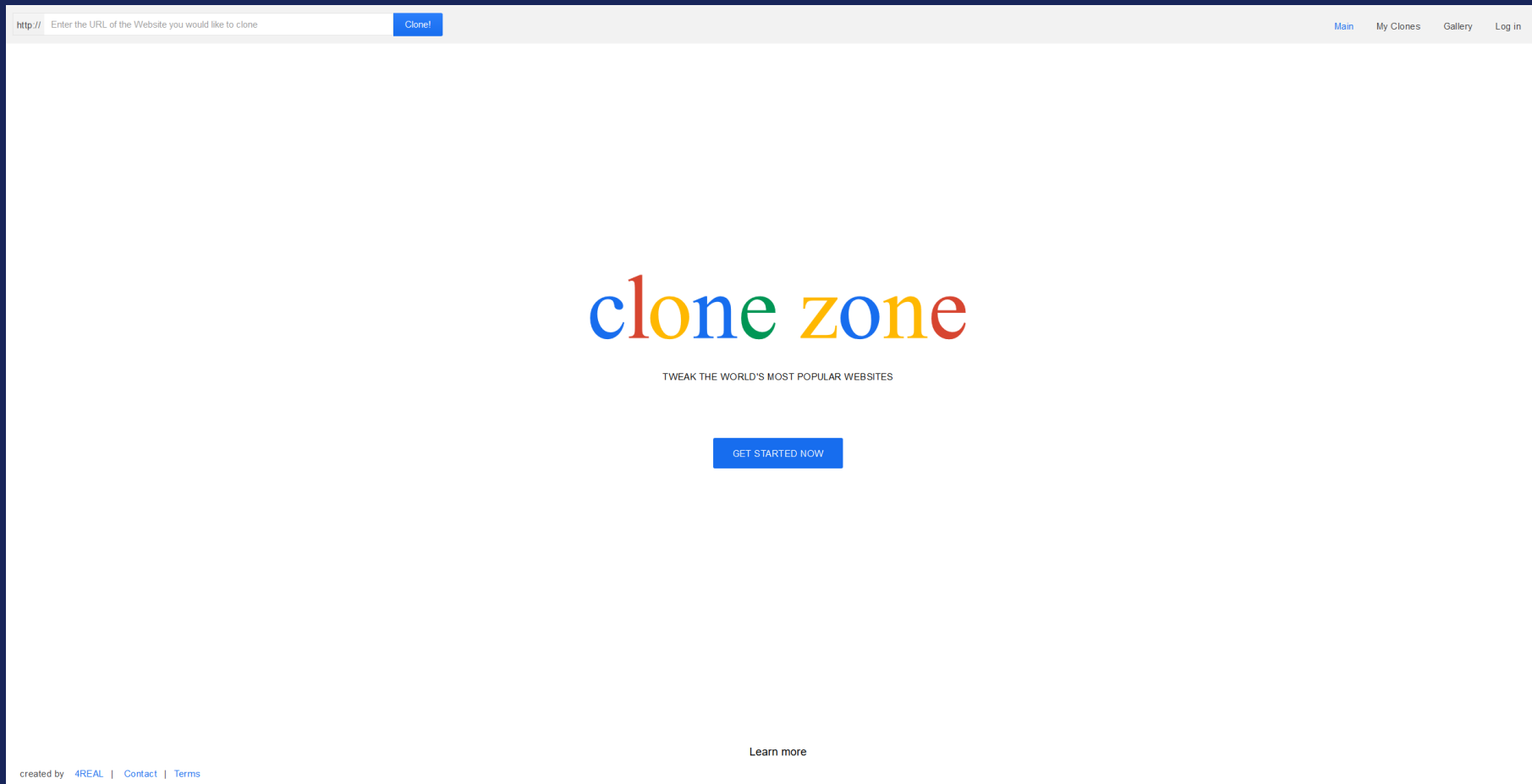
CEO Fraud

Passwortsicherheit

Hardware Hacks

Zukünftige Entwicklung

DEMO Website manipulieren



Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering
Faktor Mensch
[Website manipulieren](#)
CEO Fraud

Passwortsicherheit

Hardware Hacks

Zukünftige Entwicklung

CEO Fraud

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) 1.242,63 -0,30%	EUR/USD 1,1315 -0,00%	■ Börsenkurse ■ cM Indikationen
-------------------------	--------------------------------	---------------------------	-------------------------------	-------------------------------	--------------------------	------------------------------------

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 (22)

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering
Faktor Mensch
Website manipulieren
[CEO Fraud](#)

Passwortsicherheit

Hardware Hacks

Zukünftige Entwicklung

.....
25.01.2019 | Wintertagung 2019 - LBB

Tobias Scheible, M.Eng.

CEO Fraud - Beispiel

Von: Gustav.Geschäftsführer@firma.de <Gustav.Geschäftsführer@firma-gmbh.de>

An: Otto Opfer

Sehr geehrter Herr Opfer!

Sind Sie im Moment verfügbar?

Hochachtungsvoll

Gustav Geschäftsführer

Quelle: LKA Präsentation, Bedrohungslage Cybercrime, Albstadt 21.1.2016, S. 21

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering
Faktor Mensch
Website manipulieren
CEO Fraud

Passwortsicherheit

Hardware Hacks

Zukünftige Entwicklung

CEO Fraud - Beispiel

..wir führen momentan eine finanzielle Transaktion durch, bei der es um eine Unternehmensübernahme in Asien geht.

Diese Übernahme **muss streng vertraulich behandelt werden**. Sie sind als einziger Ansprechpartner damit betraut worden, diesen Vorgang auszuführen und Zahlungen vorzunehmen (Alle Informationslecks oder die Nichteinhaltung des unten genannten Verfahrens können zu **Vertragsstrafen und Sanktionen** gegen unsere Firmen führen).

Die öffentliche Bekanntgabe der Übernahme wird am 15.09.2015 in unseren Räumlichkeiten in Anwesenheit des gesamten Managements stattfinden.

Sie finden diesbezüglich einen von der BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht) erteilten Zahlungsauftrag.

Bitte nehmen Sie zur Einreichung der Bankdaten zur sofortigen Ausführung der Zahlung umgehend Kontakt mit unserem französischen **Berater B. Berater** auf (Dieser interveniert zwischen BaFin und AMF, um unsere Interessen zu verteidigen).

Quelle: LKA Präsentation, Bedrohungslage Cybercrime, Albstadt 21.1.2016, S. 20

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering
Faktor Mensch
Website manipulieren
[CEO Fraud](#)

Passwortsicherheit

Hardware Hacks

Zukünftige Entwicklung

CEO Fraud - Beispiel

Bitte vermeiden Sie in persönlichen wie in telefonischen Gesprächen jegliche Anspielung auf diesen Vorgang. Nutzen Sie ausschließlich den E-Mail-Verkehr mit Herrn B. (Berater), der Ihr einziger Ansprechpartner für diesen Vorgang sein wird.

Kontaktdaten von Herrn B. Berater.: B.Berater@berater-firma.com

Sobald Sie die Bankdaten erhalten, führen Sie bitte die Zahlung gemäß der beigefügten Zahlungsanweisung auf eine Weise aus, die Sie alleine vornehmen können.

Ich bitte Sie auch, Herrn B. einen Zahlungsbeleg zuzusenden, sobald er zur Verfügung steht.

Ich möchte, dass Sie bei diesem Vorgang der einzige Gesprächspartner und Ausführende innerhalb unseres Unternehmens sind.

Vielen Dank für Ihr zügiges Vorgehen. Die Finanztransaktion läuft.

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering
Faktor Mensch
Website manipulieren
CEO Fraud

Passwortsicherheit

Hardware Hacks

Zukünftige Entwicklung

CEO Fraud - Beispiel

Von: Gustav.Geschäftsführer@firma.de <Gustav.Geschäftsführer@firma-gmbh.de>

An: Otto Opfer

Konnten Sie das Nötige erledigen?

Hochachtungsvoll

Gustav Geschäftsführer

Quelle: LKA Präsentation, Bedrohungslage Cybercrime, Albstadt 21.1.2016, S. 21

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering
Faktor Mensch
Website manipulieren
CEO Fraud

Passwortsicherheit

Hardware Hacks

Zukünftige Entwicklung

CEO Fraud - Beispiel

Dear Mr Opfer,

Mr G. (Geschäftsführer) just sent me the document signed by him and Mr Z. (2. Genehmiger).

Unfortunately I need to provide to BaFin a Specimen of signature (for security reason) from them, can you please send to me an example of signature of Mr G. and Mr Z. on a document older than today ?

Thank you.

Best regards

B. Berater

BaFin /AMF Consultant

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering
Faktor Mensch
Website manipulieren
[CEO Fraud](#)

Passwortsicherheit

Hardware Hacks

Zukünftige Entwicklung

FAZIT Social Engineering

- Informationen im Internet, aber auch in der realen Welt, können sehr einfach gefälscht werden. Machen Sie sich Gedanken, wie Sie Informationen überprüfen können.
- E-Mails können sehr einfach gefälscht werden und können sogar die Absenderadresse eines persönlichen Kontaktes beinhalten.
- Allerdings können auch SMS und andere Nachrichten einfach gefälscht werden.
- Sensibilisieren der Mitarbeiter und Schulung der Mitarbeiter über Social Engineering-Strategien und –Methoden, regelmäßiger Hinweis auf die Bedeutung der Datenweitergabe.
- Schriftliche Festlegungen, welche Informationen vertraulich behandelt werden müssen, Festlegungen zur Form von Anfragen und Datenweitergabe und Vier-Augen-Prinzip.
- Tipp: Auf einem anderen Kanal nachfragen, ob es wirklich stimmt.



Passwortsicherheit

Öffentliche Passwörter

I wonder what the code could be...



Quelle: pics-for-fun.com (23)



Quelle: de.pinterest.com (24)

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering

Passwortsicherheit

Öffentliche Passwörter

Passwörter erraten

Brute-Force Methode

Bekannte Passwörter

Sperrmuster

Sichere Passwörter

Hardware Hacks

Zukünftige Entwicklung

.....
25.01.2019 | Wintertagung 2019 - LBB

Tobias Scheible, M.Eng.

Öffentliche Passwörter - Interview



Quelle: youtube.com (25)

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering

Passwortsicherheit
Öffentliche Passwörter
Passwörter erraten
Brute-Force Methode
Bekannte Passwörter
Sperrmuster
Sichere Passwörter

Hardware Hacks

Zukünftige Entwicklung

.....
25.01.2019 | Wintertagung 2019 - LBB

Tobias Scheible, M.Eng.

Angriff auf den Fernsehsender TV5Monde

- Umfangreicher Angriff auf den französischen Sender TV5Monde
 - Alle Kanäle des Fernsehunternehmens TV5Monde gingen offline
 - Die Website verbreitete kurzfristig islamistische Drohungen
 - Auf der Facebook-Seite wurden ebenfalls Drohungen verbreitet
 - Spekulationen über öffentlich einsehbare Passwörter

Faktor Mensch - Angriff auf TV5 Monde



Quelle: heise.de (26)

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering

Passwortsicherheit
Öffentliche Passwörter
Passwörter erraten
Brute-Force Methode
Bekannte Passwörter
Sperrmuster
Sichere Passwörter

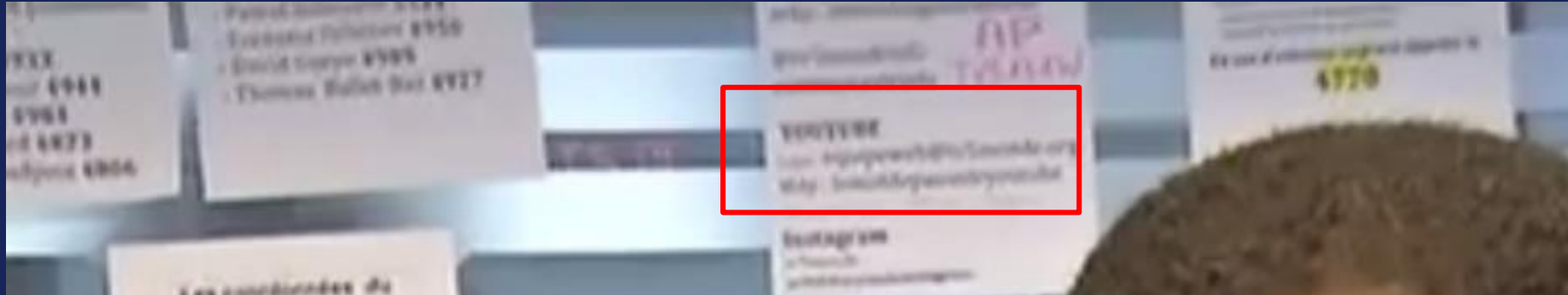
Hardware Hacks

Zukünftige Entwicklung

.....
25.01.2019 | Wintertagung 2019 - LBB

Tobias Scheible, M.Eng.

Faktor Mensch - Angriff auf TV5 Monde



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



Quelle: heise.de (26)

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering

Passwortsicherheit
Öffentliche Passwörter
Passwörter erraten
Brute-Force Methode
Bekannte Passwörter
Sperrmuster
Sichere Passwörter

Hardware Hacks

Zukünftige Entwicklung

.....
25.01.2019 | Wintertagung 2019 - LBB

Tobias Scheible, M.Eng.

Faktor Mensch



Quelle: [vice.com](https://www.vice.com) (27)

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering

Passwortsicherheit
Öffentliche Passwörter
Passwörter erraten
Brute-Force Methode
Bekannte Passwörter
Spernmuster
Sichere Passwörter

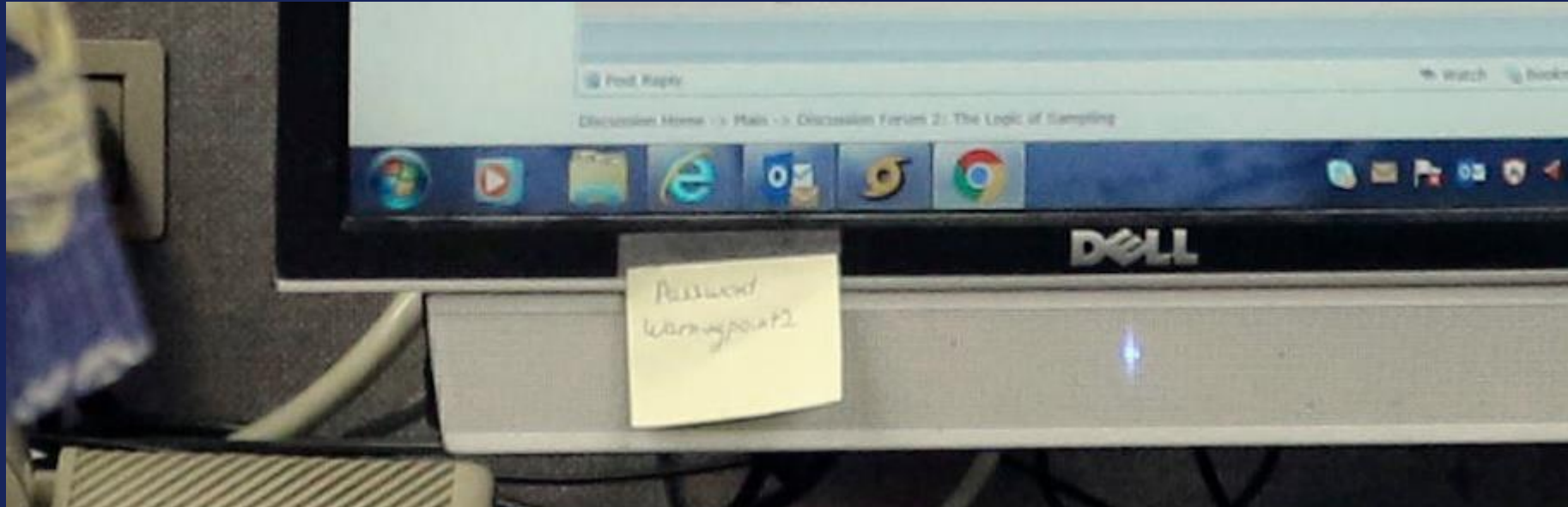
Hardware Hacks

Zukünftige Entwicklung

.....
25.01.2019 | Wintertagung 2019 - LBB

Tobias Scheible, M.Eng.

Faktor Mensch



Klassiker – Post-it Zettel auf Monitor
Passwort: warningpoint2

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering

Passwortsicherheit
Öffentliche Passwörter
Passwörter erraten
Brute-Force Methode
Bekannte Passwörter
Sperrmuster
Sichere Passwörter

Hardware Hacks

Zukünftige Entwicklung

Quelle: [vice.com](https://www.vice.com) (27)

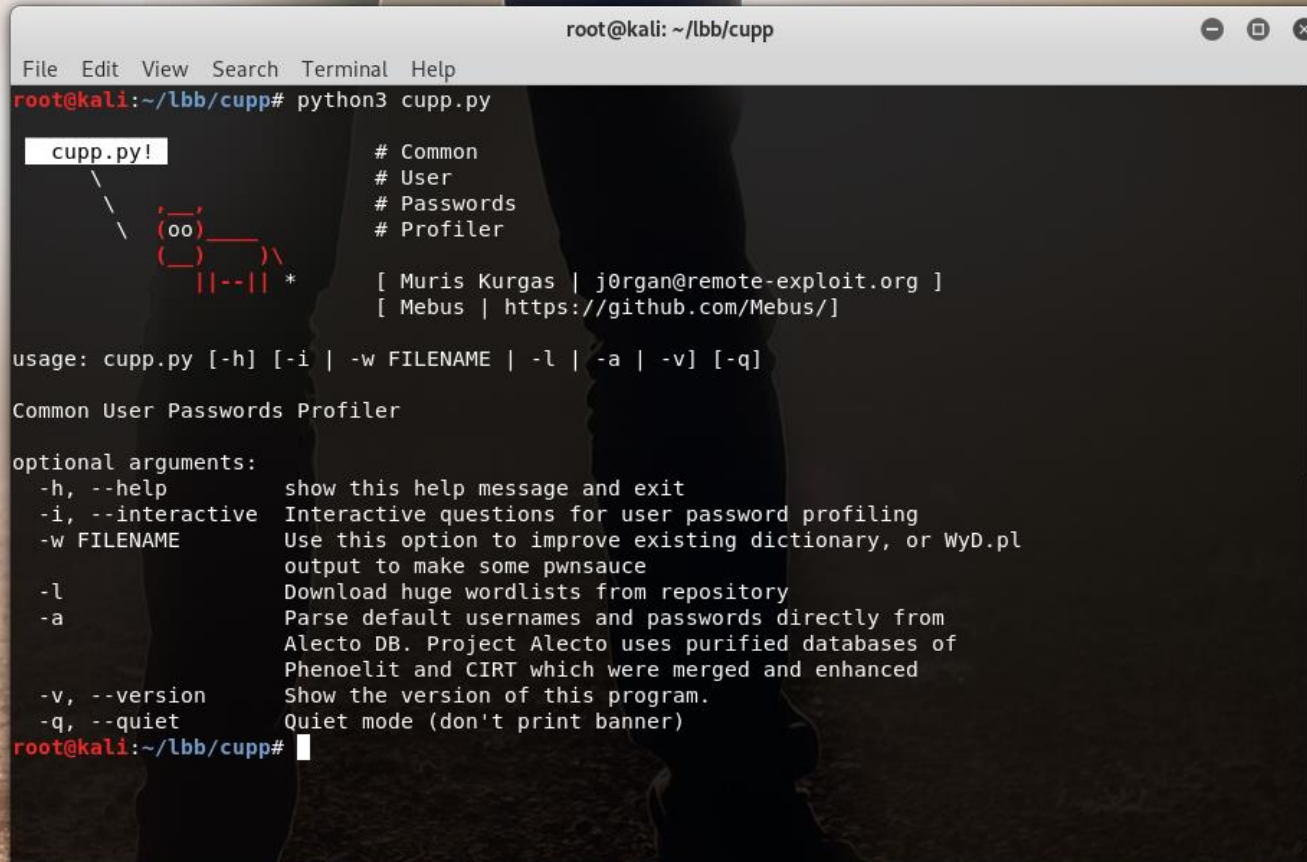
25.01.2019 | Wintertagung 2019 - LBB

Tobias Scheible, M.Eng.

Passwörter erraten

- Angreifer analysieren das Umfeld eines Opfers, um auf potentielle Passwörter schließen zu können und so diese zu erraten.
 - Alle Seiten bzw. Profile von einem Opfer werden gesucht und analysiert.
 - Dabei werden bevorzugt Inhalte von Social Media Seiten automatisch gescannt.
 - Auch Fotos werden ausgewertet und Texte automatisch erkannt – z.B. Autokennzeichen.
 - Typische Informationen wie Namen von Verwandten, Adressen, Geburtsdaten oder Haustiere werden gezielt gesucht.
 - Aus diesen Informationen werden individuelle Listen mit potentiellen Passwörtern generiert.
- Bei Unternehmen wird die Website gescannt und alle Dokumente analysiert.
 - Aus den gefundenen Begriffen werden vielfältige Kombinationen generiert.

DEMO Passwörter erraten – Generator



```
root@kali: ~/lbb/cupp
File Edit View Search Terminal Help
root@kali:~/lbb/cupp# python3 cupp.py

cupp.py!
  (oo)
  ( )
  ||--|| *

# Common
# User
# Passwords
# Profiler

[ Muris Kurgas | j0rgan@remote-exploit.org ]
[ Mebus | https://github.com/Mebus/ ]

usage: cupp.py [-h] [-i | -w FILENAME | -l | -a | -v] [-q]

Common User Passwords Profiler

optional arguments:
  -h, --help            show this help message and exit
  -i, --interactive      Interactive questions for user password profiling
  -w FILENAME            Use this option to improve existing dictionary, or WyD.pl
                        output to make some pwnsauce
  -l                    Download huge wordlists from repository
  -a                    Parse default usernames and passwords directly from
                        Alecto DB. Project Alecto uses purified databases of
                        Phenoelit and CIRT which were merged and enhanced
  -v, --version          Show the version of this program.
  -q, --quiet            Quiet mode (don't print banner)
root@kali:~/lbb/cupp#
```

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering

Passwortsicherheit
Öffentliche Passwörter
[Passwörter erraten](#)
Brute-Force Methode
Bekannte Passwörter
Sperrmuster
Sichere Passwörter

Hardware Hacks

Zukünftige Entwicklung

Brute-Force Methode

- Mit Brute-Force-Angriffen wird versucht, ein Passwort zu knacken, indem in schneller Abfolge verschiedene Zeichenkombinationen ausprobiert werden.
- Der Algorithmus ist sehr einfach und beschränkt sich auf das Ausprobieren möglichst vieler Zeichenkombinationen, weshalb auch von "erschöpfender Suche" gesprochen wird.
- Dabei hängt es von der verfügbaren Rechenleistung ab, wie viele Berechnungen pro Sekunde durchgeführt und entsprechend eine hohe Anzahl an Kombinationen ausprobiert werden können.
- Die Methode wird in der Praxis häufig erfolgreich eingesetzt, da viele Benutzer kurze Passwörter verwenden, die darüber hinaus oft nur aus Zeichen des Alphabets bestehen, womit die Anzahl der möglichen Kombinationen drastisch reduziert und das Erraten erleichtert wird.

Brute-Force Methode

- Komplexität von Passwörtern: Zeichenanzahl^{Passwortlänge} = Kombinationen

- Zeichenanzahl

- Alphabet = 26 Zeichen

- Mit Groß- und Kleinschreibung = 52 Zeichen

- Mit den Umlauten = 59 Zeichen

- Zahlen = 10 Zeichen

- Sonderzeichen = 32 Zeichen

- 101 verschiedene Zeichen

- Beispiele

- Kleinbuchstaben $26^4 = 456.976$

- Kleinbuchstaben + Zahlen $36^4 = 1.679.616$

- Alle Buchstaben + Zahlen $69^4 = 22.667.121$

- Alle Zeichen $101^4 = 104.060.401$

Cyber Security

Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering

Passwortsicherheit

Öffentliche Passwörter

Passwörter erraten

Brute-Force Methode

Bekannte Passwörter

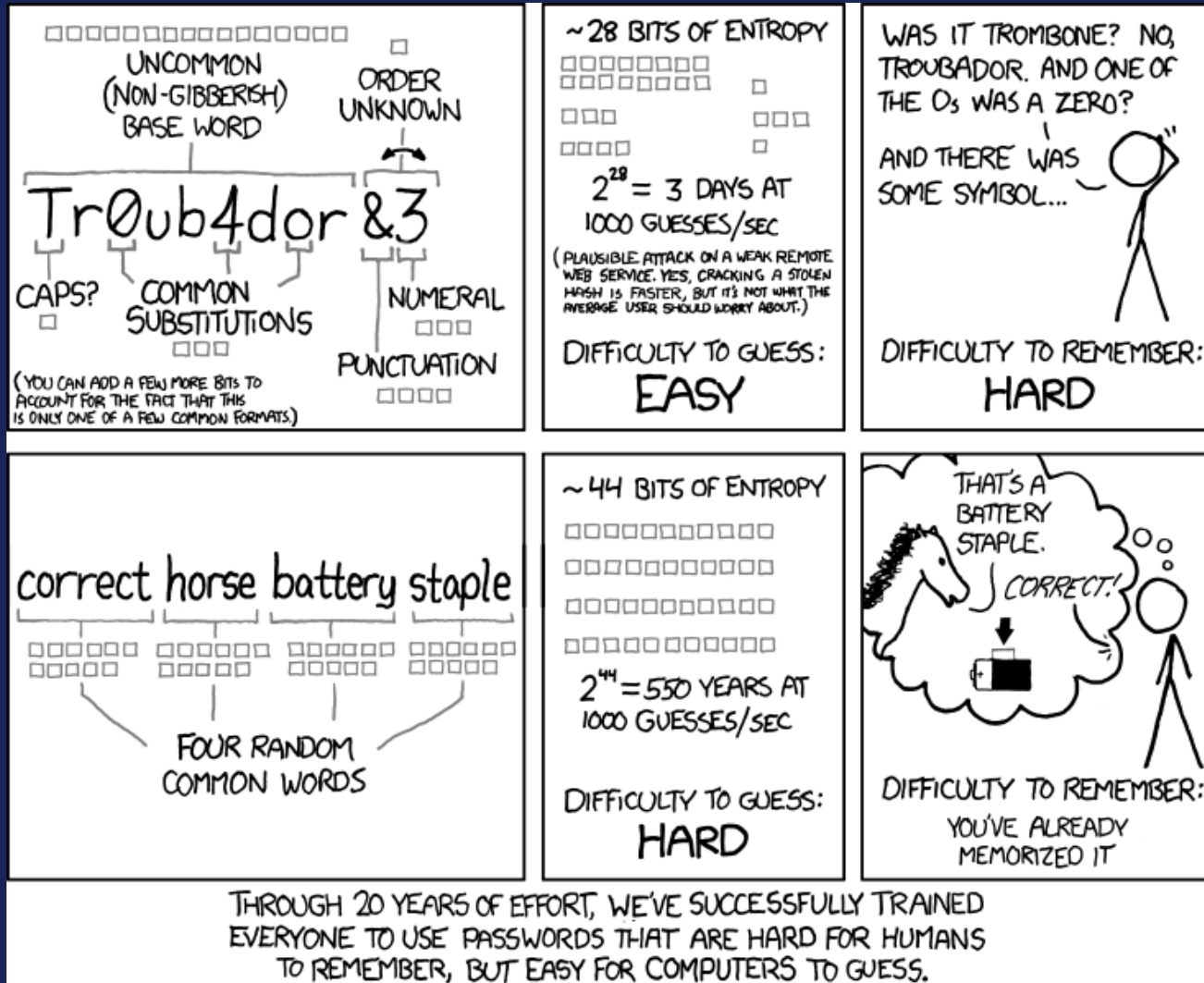
Sperrmuster

Sichere Passwörter

Hardware Hacks

Zukünftige Entwicklung

Brute-Force Methode



Quelle: [xkcd.com](https://xkcd.com/28/) (28)

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

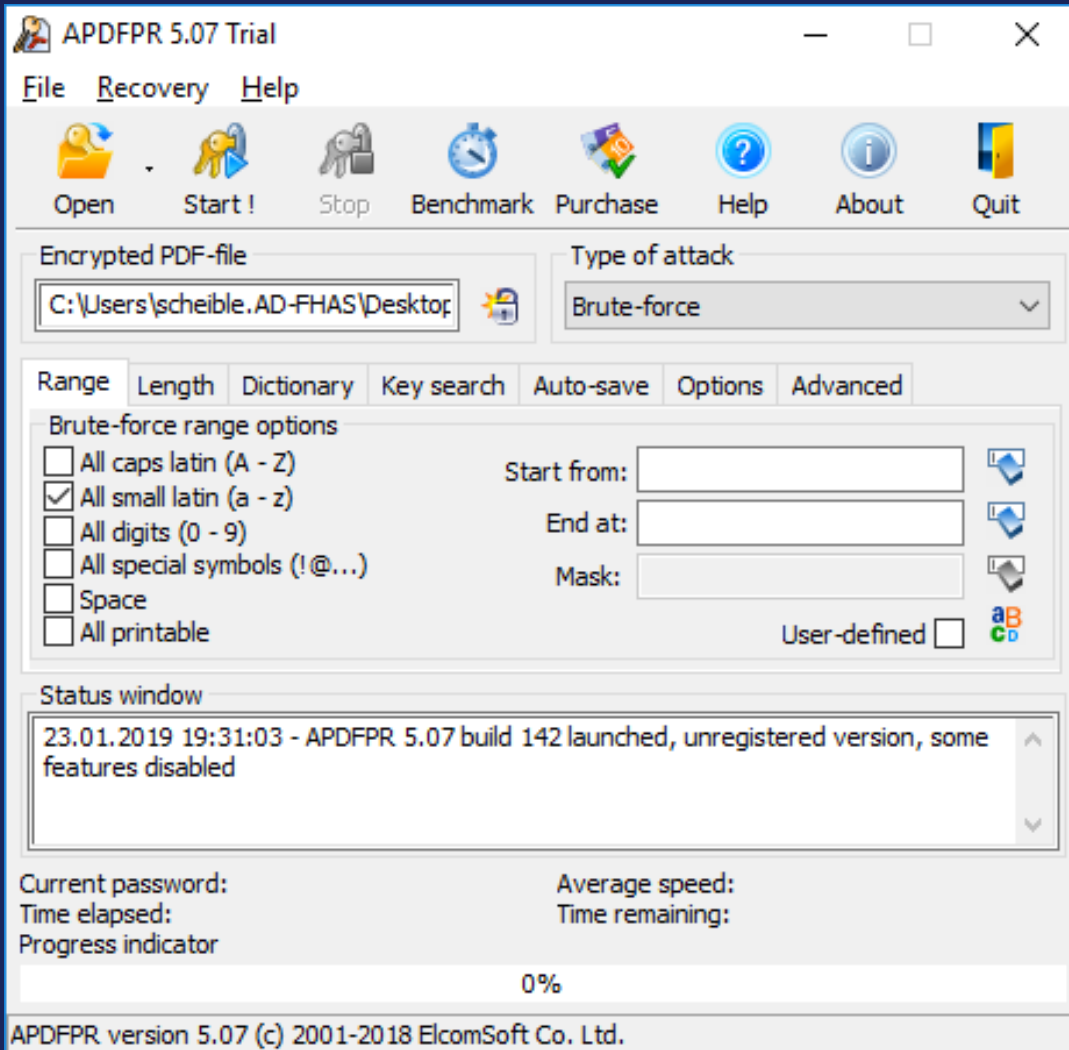
Social Engineering

Passwortsicherheit
Öffentliche Passwörter
Passwörter erraten
[Brute-Force Methode](#)
Bekannte Passwörter
Sperrmuster
Sichere Passwörter

Hardware Hacks

Zukünftige Entwicklung

DEMO Brute-Force Methode



Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering

Passwortsicherheit
Öffentliche Passwörter
Passwörter erraten
[Brute-Force Methode](#)
Bekannte Passwörter
Sperrmuster
Sichere Passwörter

Hardware Hacks

Zukünftige Entwicklung

Bekannte Passwörter

124 lines (115 sloc) | 6.67 KB

Raw

Blame

History



```
1 Top 100 Adobe Passwords with Count
2
3 We do not (yet) have the keys Adobe used to encrypt the passwords of 130,324,429 users affected by
4 their most recent breach. However, thanks to Adobe choosing symmetric key encryption over hashing,
5 selecting ECB mode, and using the same key for every password, combined with a large number of
6 known plaintexts and the generosity of users who flat-out gave us their password in their password
7 hint, this is not preventing us from presenting you with this list of the top 100 passwords
8 selected by Adobe users.
9
10 While we are fairly confident in the accuracy of this list, we have no way to actually verify it
11 right now. We don't have the keys, and Adobe is not letting any of the affected accounts log in
12 until the owners reset their passwords. So, it is possible there is an error or two in here. Caveat
13 emptor and such.
14
15
16
17
18
19
20
21
22
23
24
25
26
```

Quelle: github.com (29)

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering

Passwortsicherheit

Öffentliche Passwörter

Passwörter erraten

Brute-Force Methode

Bekannte Passwörter

Spermuster

Sichere Passwörter

Hardware Hacks

Zukünftige Entwicklung

.....
25.01.2019 | Wintertagung 2019 - LBB

Tobias Scheible, M.Eng.

DEMO Bekannte Passwörter

```
Eingabeaufforderung

C:\Users\scheible.AD-FHAS\Desktop>pdfcrack.exe -f test4.pdf -w passwords.txt

PDF version 1.7
Security Handler: Standard
V: 2
R: 3
P: -1028
Length: 128
Encrypted Metadata: True
FileID: 63aef3a5ddbfff4b8aaf1de4be1ba324
U: adb15e3a4c6f960989c449a1f95bc2f19fe957d527330101b4974e37a562d453
O: f6ea4b39b40ac31aeaae65d61ddc7cb4ae20a04a74a9135ccc9c3c359da65ff
found user-password: 'snoopy1'

C:\Users\scheible.AD-FHAS\Desktop>
```

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering

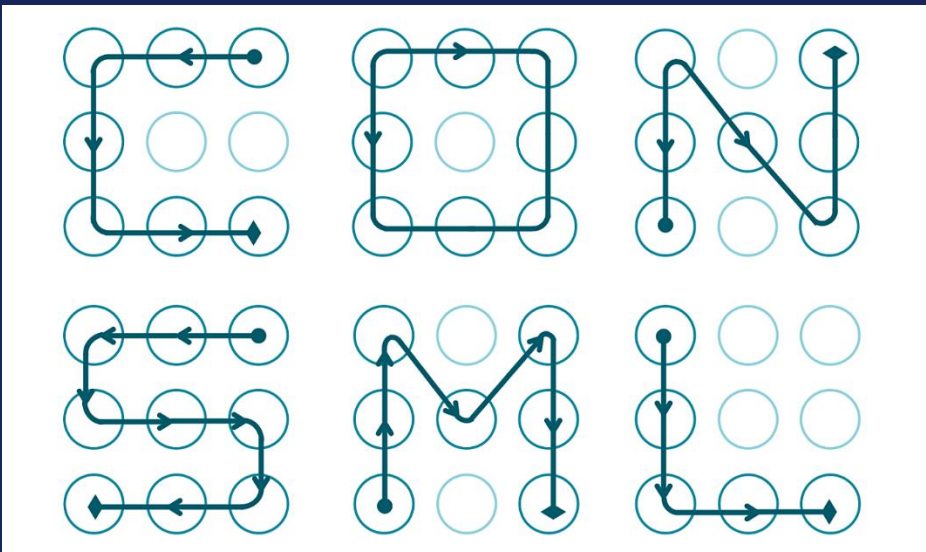
Passwortsicherheit
Öffentliche Passwörter
Passwörter erraten
Brute-Force Methode
Bekannte Passwörter
Sperrmuster
Sichere Passwörter

Hardware Hacks

Zukünftige Entwicklung

Sperrmuster

- Studie von Marte Løge analysierte über 4000 Android Entsperrmuster im Rahmen ihrer Master Thesis.
 - 10 % aller Versuchspersonen nutzen ein Muster, das einem Buchstaben ähnelt
 - 77 % fangen in einer der vier Ecken an; 44 % starten oben links
 - Durchschnittliche Anzahl von fünf verwendeten Knoten
 - Muster von links → rechts oder von oben → unten werden häufig verwendet



Quelle: arstechnica.com (30)

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering

Passwortsicherheit
Öffentliche Passwörter
Passwörter erraten
Brute-Force Methode
Bekannte Passwörter
Sperrmuster
Sichere Passwörter

Hardware Hacks

Zukünftige Entwicklung

25.01.2019 | Wintertagung 2019 - LBB

Tobias Scheible, M.Eng.

Sperrmuster vs. PIN

Länge	Wischmuster Kombinationen	PIN Kombinationen
4	1624	$10^4 = 10000$
5	7152	$10^5 = 100000$
6	26016	$10^6 = 1000000$
7	72912	$10^7 = 10000000$
8	140704	$10^8 = 100000000$
9	140704	$10^9 = 1000000000$

Fünf Versuche möglich, dann 30 Sekunden Wartepause. Dadurch ist ein 5-stelliges Wischmuster in ~ 12 Stunden zu knacken (ein 4- oder 5- stelliges in ~15 Stunden).

Ein 4-stelliger Pin ist in ~17 Stunden knackbar.

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering

Passwortsicherheit

Öffentliche Passwörter

Passwörter erraten

Brute-Force Methode

Bekannte Passwörter

Sperrmuster

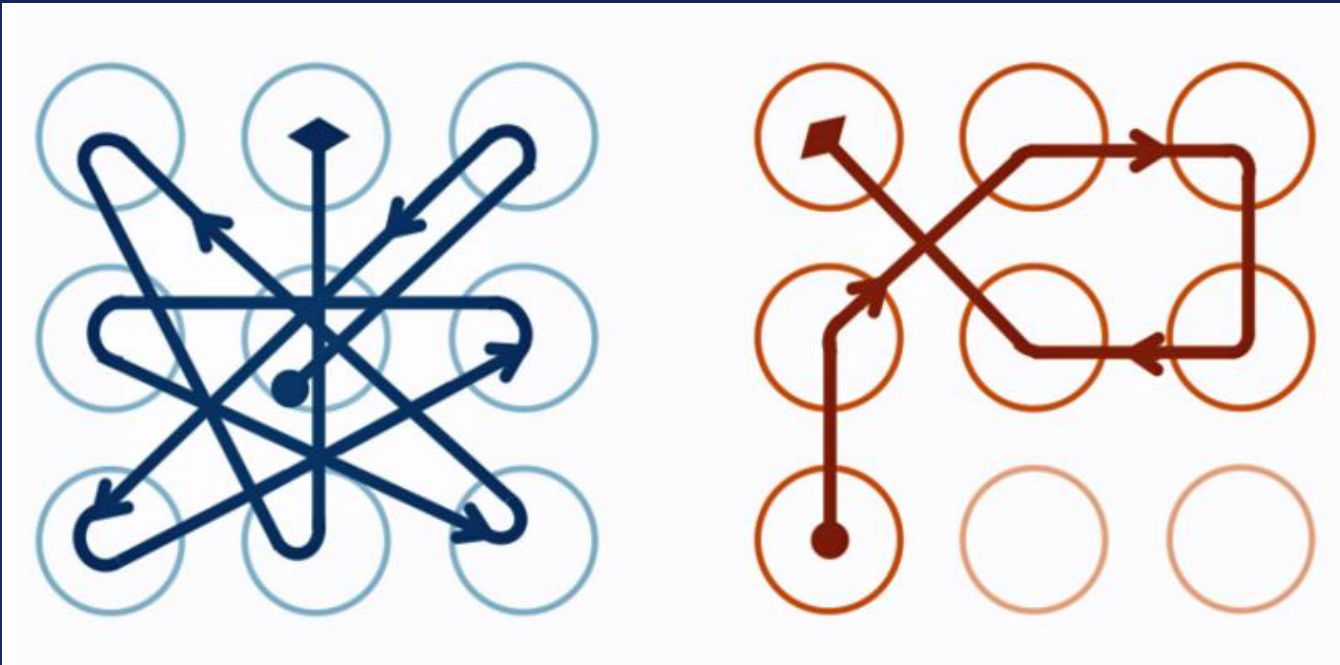
Sichere Passwörter

Hardware Hacks

Zukünftige Entwicklung

Sperrmuster- Gegenmaßnahmen

- Komplizierte Muster verwenden
- Lange PINs, besser Passwörter verwenden



Sperrmuster – Pin Beispiel



Quelle: youtube.com (31)

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering

Passwortsicherheit

Öffentliche Passwörter

Passwörter erraten

Brute-Force Methode

Bekannte Passwörter

Sperrmuster

Sichere Passwörter


Hardware Hacks



Zukünftige Entwicklung

.....
25.01.2019 | Wintertagung 2019 - LBB

Tobias Scheible, M.Eng.

DEMO Sichere Passwörter




[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](#)

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security
Social Engineering

Passwortsicherheit
Öffentliche Passwörter
Passwörter erraten
Brute-Force Methode
Bekannte Passwörter
Sperrmuster
[Sichere Passwörter](#)

Hardware Hacks
Zukünftige Entwicklung

.....
25.01.2019 | Wintertagung 2019 - LBB
Tobias Scheible, M.Eng.

Quelle: haveibeenpwned.com (32)

62

Sichere Passwörter

- Zwei-Faktor-Authentisierung
 - Login mit zwei Faktoren
 - Meistens 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
 - Speichert Passwörter in einem verschlüsselten Container mit einem Masterpasswort
 - Unterstützt bei der Generierung von Passwörtern
 - Verschiedene Lösungen sind vorhanden – z.B. KeePassXC
 - Viele Möglichkeiten zur Erweiterung (Firefox / Chrome Plugin, ...)

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering

Passwortsicherheit
Öffentliche Passwörter
Passwörter erraten
Brute-Force Methode
Bekannte Passwörter
Sperrmuster
[Sichere Passwörter](#)

Hardware Hacks

Zukünftige Entwicklung

Sichere Passwörter - Passwortkarten

Nr:		Kategorie:								
	abc	def	ghi	jkl	mno	pqr	stu	vwx	yz	#
1										
2										
3										
4										
5										
6										
7										
8										

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering

Passwortsicherheit

Öffentliche Passwörter

Passwörter erraten

Brute-Force Methode

Bekannte Passwörter

Sperrmuster

Sichere Passwörter

Hardware Hacks

Zukünftige Entwicklung

Sichere Passwörter - Passwortkarten

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering

Passwortsicherheit
 Öffentliche Passwörter
 Passwörter erraten
 Brute-Force Methode
 Bekannte Passwörter
 Sperrmuster
[Sichere Passwörter](#)

Hardware Hacks

Zukünftige Entwicklung

25.01.2019 | Wintertagung 2019 - LBB

Tobias Scheible, M.Eng.

Nr: *1* Kategorie: *Online-Banking*

	abc	def	ghi	jkl	mno	pqr	stu	vwx	yz	#
1	<i>x!</i>	<i>Q*</i>	<i>S<</i>	<i>bL</i>	<i>Pn</i>	<i>X:</i>	<i>V=</i>	<i>dd</i>	<i>n3</i>	<i>9K</i>
2	<i>T8</i>	<i>wb</i>	<i>eT</i>	<i>98</i>	<i>C,</i>	<i>6<</i>	<i>ff</i>	<i>aO</i>	<i>X></i>	<i>Hm</i>
3	<i>Bd</i>	<i>dD</i>	<i>C)</i>	<i>7c</i>	<i>gz</i>	<i>er</i>	<i>q]</i>	<i>p=</i>	<i>t&</i>	<i>1P</i>
4	<i>ne</i>	<i>a@</i>	<i>e-</i>	<i>W8</i>	<i>k-</i>	<i>G2</i>	<i>>d</i>	<i>PE</i>	<i>z3</i>	<i>z:</i>
5	<i>V.</i>	<i>H></i>	<i>d*</i>	<i>W-</i>	<i>Wl</i>	<i>J8</i>	<i>Qi</i>	<i>U,</i>	<i>ld</i>	<i>7R</i>
6	<i>5=</i>	<i>mF</i>	<i>2n</i>	<i>XY</i>	<i>m:</i>	<i>f<</i>	<i>YH</i>	<i>mo</i>	<i>h4</i>	<i>7-</i>
7	<i>vT</i>	<i>ej</i>	<i>R:</i>	<i>+<</i>	<i>Vg</i>	<i>Nh</i>	<i>a9</i>	<i>6;</i>	<i>dJ</i>	<i>N{</i>
8	<i>d6</i>	<i>G7</i>	<i>p)</i>	<i>ek</i>	<i>pJ</i>	<i>mb</i>	<i>y2</i>	<i>e?</i>	<i>Jm</i>	<i>Rv</i>

Sichere Passwörter - Passwortkarten

Link: sparkasse.de

Passwort:

Nr: 1 Kategorie: *Online-Banking*

	abc	def	ghi	jkl	mno	pqr	stu	vwx	yz	#
1	<i>x!</i>	<i>Q*</i>	<i>S<</i>	<i>bL</i>	<i>Pn</i>	<i>X:</i>	<i>V=</i>	<i>dd</i>	<i>n3</i>	<i>9K</i>
2	<i>T8</i>	<i>wb</i>	<i>eT</i>	<i>98</i>	<i>C,</i>	<i>6<</i>	<i>ff</i>	<i>aO</i>	<i>X></i>	<i>Hm</i>
3	<i>Bd</i>	<i>dD</i>	<i>C)</i>	<i>7c</i>	<i>gz</i>	<i>er</i>	<i>q]</i>	<i>p=</i>	<i>t&</i>	<i>1P</i>
4	<i>ne</i>	<i>a@</i>	<i>e-</i>	<i>W8</i>	<i>k-</i>	<i>G2</i>	<i>>d</i>	<i>PE</i>	<i>z3</i>	<i>z:</i>
5	<i>V.</i>	<i>H></i>	<i>d*</i>	<i>W-</i>	<i>WI</i>	<i>J8</i>	<i>Qi</i>	<i>U,</i>	<i>ld</i>	<i>7R</i>
6	<i>5=</i>	<i>mF</i>	<i>2n</i>	<i>XY</i>	<i>m:</i>	<i>f<</i>	<i>YH</i>	<i>mo</i>	<i>h4</i>	<i>7-</i>
7	<i>vT</i>	<i>ej</i>	<i>R:</i>	<i>+<</i>	<i>Vg</i>	<i>Nh</i>	<i>a9</i>	<i>6;</i>	<i>dJ</i>	<i>N{</i>
8	<i>d6</i>	<i>G7</i>	<i>p)</i>	<i>ek</i>	<i>pJ</i>	<i>mb</i>	<i>y2</i>	<i>e?</i>	<i>Jm</i>	<i>Rv</i>

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering

Passwortsicherheit

Öffentliche Passwörter

Passwörter erraten

Brute-Force Methode

Bekannte Passwörter

Sperrmuster

Sichere Passwörter

Hardware Hacks

Zukünftige Entwicklung

Sichere Passwörter - Passwortkarten

Link: sparkasse.de

Passwort: **V=**

Nr: 1		Kategorie: Online-Banking								
	abc	def	ghi	jkl	mno	pqr	stu	vwx	yz	#
1	x!	Q*	S<	bL	Pn	X:	V=	dd	n3	9K
2	T8	wb	eT	98	C,	6<	ff	aO	X>	Hm
3	Bd	dD	C)	7c	gz	er	q]	p=	t&	1P
4	ne	a@	e-	W8	k-	G2	>d	PE	z3	z:
5	V.	H>	d*	W-	WI	J8	Qi	U,	Id	7R
6	5=	mF	2n	XY	m:	f<	YH	mo	h4	7-
7	vT	ej	R:	+<	Vg	Nh	a9	6;	dJ	N{
8	d6	G7	p)	ek	pJ	mb	y2	e?	Jm	Rv

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering

Passwortsicherheit

Öffentliche Passwörter

Passwörter erraten

Brute-Force Methode

Bekannte Passwörter

Sperrmuster

Sichere Passwörter

Hardware Hacks

Zukünftige Entwicklung

Sichere Passwörter - Passwortkarten

Link: [sparkasse.de](https://www.sparkasse.de)

Passwort: [V=6<](#)

Nr: 1		Kategorie: Online-Banking								
	abc	def	ghi	jkl	mno	pqr	stu	vwx	yz	#
1	x!	Q*	S<	bL	Pn	X:	V=	dd	n3	9K
2	T8	wb	eT	98	C,	6<	ff	aO	X>	Hm
3	Bd	dD	C)	7c	gz	er	q]	p=	t&	1P
4	ne	a@	e-	W8	k-	G2	>d	PE	z3	z:
5	V.	H>	d*	W-	Wl	J8	Qi	U,	ld	7R
6	5=	mF	2n	XY	m:	f<	YH	mo	h4	7-
7	vT	ej	R:	+<	Vg	Nh	a9	6;	dJ	N{
8	d6	G7	p)	ek	pJ	mb	y2	e?	Jm	Rv

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering

Passwortsicherheit

Öffentliche Passwörter

Passwörter erraten

Brute-Force Methode

Bekannte Passwörter

Sperrmuster

[Sichere Passwörter](#)

Hardware Hacks

Zukünftige Entwicklung

Sichere Passwörter - Passwortkarten

Link: sparkasse.de

Passwort: V=6<Bd

Nr: 1		Kategorie: Online-Banking								
	abc	def	ghi	jkl	mno	pqr	stu	vwx	yz	#
1	x!	Q*	S<	bL	Pn	X:	V=	dd	n3	9K
2	T8	wb	eT	98	C,	6<	ff	aO	X>	Hm
3	Bd	dD	C)	7c	gz	er	q]	p=	t&	1P
4	ne	a@	e-	W8	k-	G2	>d	PE	z3	z:
5	V.	H>	d*	W-	Wl	J8	Qi	U,	ld	7R
6	5=	mF	2n	XY	m:	f<	YH	mo	h4	7-
7	vT	ej	R:	+<	Vg	Nh	a9	6;	dJ	N{
8	d6	G7	p)	ek	pJ	mb	y2	e?	Jm	Rv

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering

Passwortsicherheit

Öffentliche Passwörter

Passwörter erraten

Brute-Force Methode

Bekannte Passwörter

Sperrmuster

Sichere Passwörter

Hardware Hacks

Zukünftige Entwicklung

Sichere Passwörter - Passwortkarten

Link: sparkasse.de

Passwort: **V=6<BdG2**

Nr: 1		Kategorie: Online-Banking								
	abc	def	ghi	jkl	mno	pqr	stu	vwx	yz	#
1	x!	Q*	S<	bL	Pn	X:	V=	dd	n3	9K
2	T8	wb	eT	98	C,	6<	ff	aO	X>	Hm
3	Bd	dD	C)	7c	gz	er	q]	p=	t&	1P
4	ne	a@	e-	W8	k-	G2	>d	PE	z3	z:
5	V.	H>	d*	W-	Wl	J8	Qi	U,	ld	7R
6	5=	mF	2n	XY	m:	f<	YH	mo	h4	7-
7	vT	ej	R:	+<	Vg	Nh	a9	6;	dJ	N{
8	d6	G7	p)	ek	pJ	mb	y2	e?	Jm	Rv

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering

Passwortsicherheit

- Öffentliche Passwörter
- Passwörter erraten
- Brute-Force Methode
- Bekannte Passwörter
- Sperrmuster
- Sichere Passwörter

Hardware Hacks

Zukünftige Entwicklung

Sichere Passwörter - Passwortkarten

Link: sparkasse.de

Passwort: V=6<BdG2W-

Nr: 1		Kategorie: Online-Banking								
	abc	def	ghi	jkl	mno	pqr	stu	vwx	yz	#
1	x!	Q*	S<	bL	Pn	X:	V=	dd	n3	9K
2	T8	wb	eT	98	C,	6<	ff	aO	X>	Hm
3	Bd	dD	C)	7c	gz	er	q]	p=	t&	1P
4	ne	a@	e-	W8	k-	G2	>d	PE	z3	z:
5	V.	H>	d*	W-	Wl	J8	Qi	U,	ld	7R
6	5=	mF	2n	XY	m:	f<	YH	mo	h4	7-
7	vT	ej	R:	+<	Vg	Nh	a9	6;	dJ	N{
8	d6	G7	p)	ek	pJ	mb	y2	e?	Jm	Rv

Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering

Passwortsicherheit

Öffentliche Passwörter
Passwörter erraten
Brute-Force Methode
Bekannte Passwörter
Sperrmuster
[Sichere Passwörter](#)

Hardware Hacks

Zukünftige Entwicklung

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 überall, wo es geht, eine Zwei-Faktor-Authentisierung.



Hardware Hacks

DEMO Probe Requests Scanner



Cyber Security

Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering

Passwortsicherheit

Hardware Hacks

Probe Requests Scanner

Hardware Tools

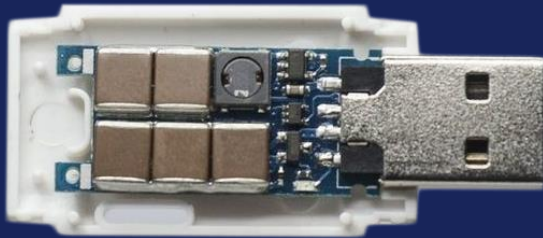
BadUSB

Zukünftige Entwicklung

25.01.2019 | Wintertagung 2019 - LBB

Tobias Scheible, M.Eng.

Hardware Tools



Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering

Passwortsicherheit

Hardware Hacks

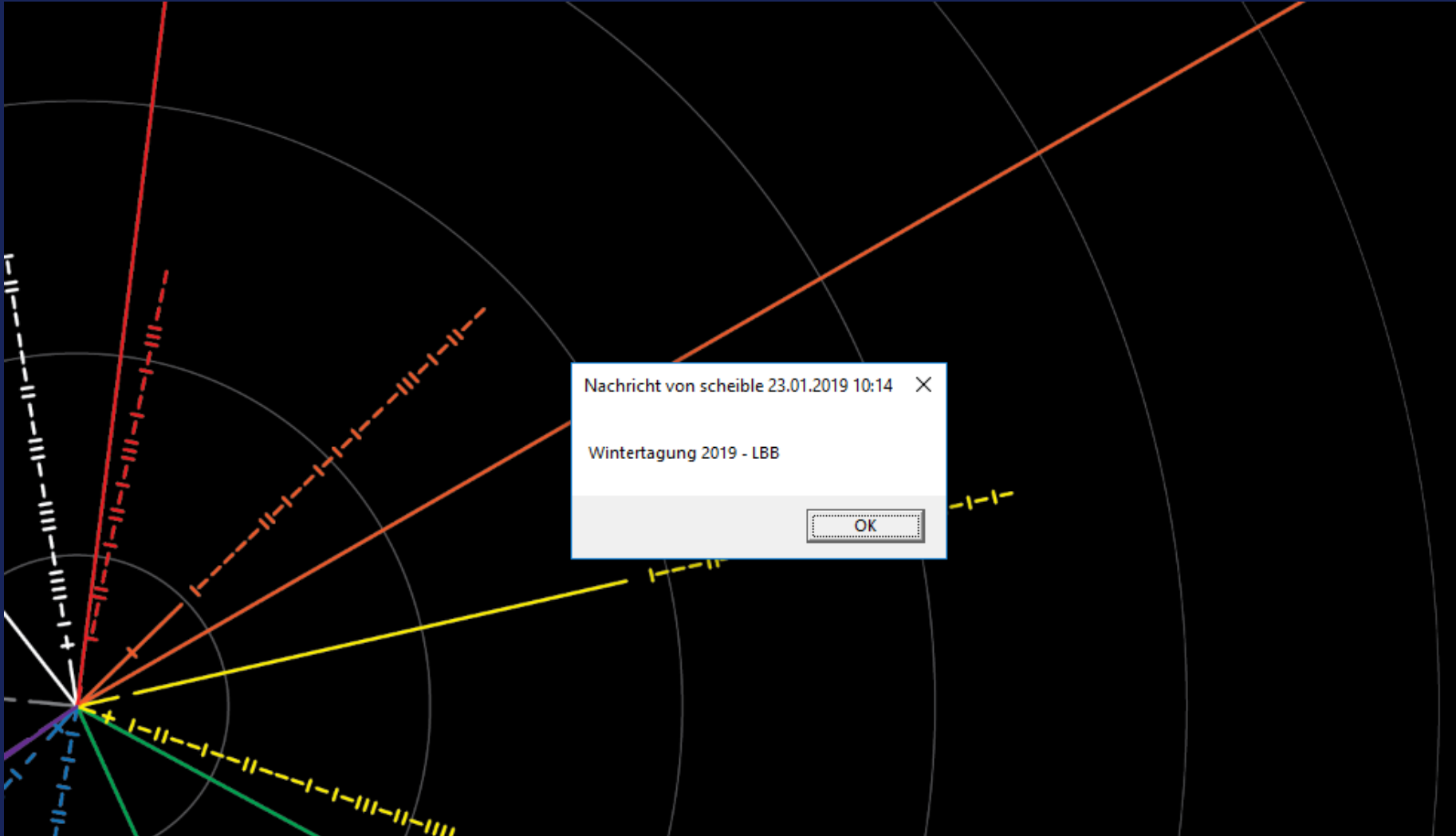
Probe Requests Scanner

[Hardware Tools](#)

BadUSB

Zukünftige Entwicklung

DEMO BadUSB



Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering

Passwortsicherheit

Hardware Hacks

Probe Requests Scanner

Hardware Tools

[BadUSB](#)

Zukünftige Entwicklung

FAZIT Hardware Hacks

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

The background is a complex digital interface. It features a central circular gauge with a padlock icon in the middle, surrounded by concentric circles and tick marks. The left side has an orange-to-yellow gradient with various UI elements like buttons labeled 'EJECT', 'ON', 'OFF', and 'OPN STATUS'. The right side has a blue gradient with more UI elements and a small window. At the bottom, there are horizontal bands of binary code (0s and 1s) in blue and red. The overall theme is futuristic technology and security.

Zukünftige Entwicklung

11001010100101 11001010100101 11001010100101

11001010100101

IoT – Internet of Things

- Ein Bot-Netz, das sich aus IoT-Geräten zusammensetzt
- Es wurde genutzt, um DDOS-Angriffe auszuführen
- Konnte auch gemietet werden
- Seiteneffekte:
 - Es wurde versucht, Router über eine Schnittstelle zur Fernwartung zu übernehmen
 - Durch eine fehlerhafte Umsetzung „stürzten“ die Router ab
 - 900.000 Router der Deutschen Telekom waren nicht mehr erreichbar



Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security
Social Engineering
Passwortsicherheit
Hardware Hacks

Zukünftige Entwicklung
[IoT – Internet of Things](#)
[IoT – Ransomware](#)

IoT – Ransomware



Cyber Security
Angreifer & Bedrohungen verstehen

Cyber Security

Social Engineering

Passwortsicherheit

Hardware Hacks

Zukünftige Entwicklung
IoT – Internet of Things
IoT – Ransomware

Vielen Dank für Ihre Aufmerksamkeit



Noch 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 23.01.2019
- (2) Mit Floppy Disks Atombomben überwachen, <http://www.zeit.de/politik/ausland/2016-05/us-militaer-pcs-technologie-veraltet-rechnungshof>, abgerufen am 23.01.2019
- (3) Was ist eigentlich die Geschichte der Malware?, <https://www.gdata.de/ratgeber/was-ist-eigentlich-die-geschichte-der-malware>, abgerufen am 23.01.2019
- (4) AIDS (Schadprogramm), [https://de.wikipedia.org/wiki/AIDS_\(Schadprogramm\)](https://de.wikipedia.org/wiki/AIDS_(Schadprogramm)), abgerufen am 23.01.2019
- (5) Doxing - eine alte Hacker-Waffe trifft den deutschen Mainstream, <https://www.sueddeutsche.de/digital/hack-doxing-privatsphaere-1.4278901>, abgerufen am 23.01.2019
- (6) online metadata and exif viewer, <http://metapicz.com>, abgerufen am 23.01.2019
- (7) Millionen Passwörter im Netz veröffentlicht, <https://www.zeit.de/digital/datenschutz/2019-01/datenleak-email-passwoerter-internet-it-sicherheit>, abgerufen am 23.01.2019
- (8) iWebapp, <http://www.shop.ledermode.tv>, abgerufen am 23.01.2019
- (9) Google, <https://google.de>, abgerufen am 23.01.2019
- (10) Google Hacking Database, <https://www.exploit-db.com/google-hacking-database>, abgerufen am 23.01.2019
- (11) IP-Kameras von Aldi als Sicherheits-GAU, <http://www.heise.de/security/meldung/IP-Kameras-von-Aldi-als-Sicherheits-GAU-3069735.html>, abgerufen am 23.01.2019
- (12) Shodan, <https://www.shodan.io>, abgerufen am 23.01.2019
- (13) Shodan, <https://www.shodan.io>, abgerufen am 23.01.2019

Quellen

- (14) Low Orbit Ion Cannon (LOIC), https://en.wikipedia.org/wiki/Low_Orbit_Ion_Cannon#/media/File:LOIC-0.png, abgerufen am 23.01.2019
- (15) LOIC - Low Orbit Ion Cannon, <http://m.1mobile.com/genius.mohammad.loic.html>, abgerufen am 23.01.2019
- (16) Anuncio - gwapo's, <https://www.youtube.com/watch?v=5M9k7wfiWiI>, abgerufen am 23.01.2019
- (17) Locky, <https://de.wikipedia.org/wiki/Locky>, abgerufen am 23.01.2019
- (18) Gefälschte E-Mail - Schulfrei ermogelt, <http://www.spiegel.de/schulspiegel/schulfrei-in-niedersachsen-wegen-gefaelschter-e-mail-a-1071105.html>, abgerufen am 23.01.2019
- (19) Legisdigit@ - Groupe Mutuel Versicherungen - <https://www.youtube.com/watch?v=WvRL5I1eU3E>, abgerufen am 23.01.2019
- (20) Gefängnisausbruch mittels E-Mail-Betrug, <http://www.heise.de/newsticker/meldung/Gefaengnisausbruch-mittels-E-Mail-Betrug-2587303.html>, abgerufen am 23.01.2019
- (21) Clone Zone, <http://clonezone.link>, abgerufen am 23.01.2019
- (22) 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 23.01.2019
- (23) Code, <http://pics-for-fun.com/wonder-what-the-code-could-be/>, abgerufen am 23.01.2019
- (24) And the valuables are in the closet on the top shelf in a box marked, <https://de.pinterest.com/pin/3025924727584002/>, abgerufen am 23.01.2019
- (25) What is Your Password?, <https://www.youtube.com/watch?v=opRMrEfAlil>, abgerufen am 23.01.2019
- (26) 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 23.01.2019

Quellen

- (27) 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-hawaiiis-nuclear-alert-keeps-passwords-on-post-its-vgtrn, abgerufen am 23.01.2019
- (28) Password Strength, <https://xkcd.com/936/>, abgerufen am 23.01.2019
- (29) Top 100 Adobe Passwords with Count, <https://github.com/morontt/symfobroute/blob/master/adobe-top100.txt>, abgerufen am 23.01.2019
- (30) New data uncovers the surprising predictability of Android lock patterns, <https://arstechnica.com/information-technology/2015/08/new-data-uncovers-the-surprising-predictability-of-android-lock-patterns/>, abgerufen am 23.01.2019
- (31) The Longest iPhone 6 Unlock Code In History (He Gotta Be Cheating), <https://www.youtube.com/watch?v=brzU7i2sAcY>, abgerufen am 23.01.2019
- (32) Have I Been Pwned: Check if your email has been compromised in a data breach, <https://haveibeenpwned.com>, abgerufen am 23.01.2019
- (33) The Original USB KeyLogger 8MB Black, <http://www.amazon.com/KeyGrabber-USB-KeyLogger-8MB-Black/dp/B004TUBOKW>, abgerufen am 23.01.2019
- (34) Pocket Jammer, <http://www.pki-electronic.com/products/jamming-systems/pocket-jammer/>, abgerufen am 23.01.2019
- (35) Mobile Mini GSM Alarmanlage Quadband mit Rückruffunktion, <https://www.amazon.de/Mobile-Alarmanlage-Quadband-Rückruffunktion-Geräuschaktivierungs-Lautstärke-Schwarz/dp/B00RC7SF8S>, abgerufen am 23.01.2019
- (36) USB Rubber Ducky, <https://hakshop.com/products/usb-rubber-ducky-deluxe>, abgerufen am 23.01.2019
- (37) How do USB killers work?, <https://www.quora.com/How-do-USB-killers-work>, abgerufen am 23.01.2019
- (38) UK police arrested the alleged mastermind of the MIRAI attack on Deutsche Telekom, <http://securityaffairs.co/wordpress/56604/cyber-crime/mirai-attack-deutsche-telekom.html>, abgerufen am 23.01.2019
- (39) Hackers demonstrated first ransomware for IoT thermostats at DEF CON, <https://www.computerworld.com/article/3105001/security/hackers-demonstrated-first-ransomware-for-iot-thermostats-at-def-con.html>, abgerufen am 23.01.2019