



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

Fakultät Informatik

Cyber Security Workshop
IT Security – anonym und
sicher im Netz
Gymnasium Balingen

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
 - Forschungsschwerpunkte



Web Forensics | Web Application Security | Hacking Hardware | Benutzerzentrierte Didaktik

IT Security (Bachelor) – 4. Semester
Praktikum Cybersecurity

IT Security (Bachelor) – 5. Semester
Digitale Forensik

IT GRC Management – 4. Semester
Grundlagen der digitale Forensik

IT Security & Smart Textiles
Forschungsprojekt SEKT www.projekt-sekt.de

Vorträge & Workshops
LKA, IHK, VDI, Verbände, ...

IT Security – anonym und
sicher im Netz

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)

IT Security – anonym und
sicher im Netz

Zahlen & Fakten



IT Security – anonym und
sicher im Netz

Bachelorstudiengänge

- + IT Security
 - + Technische Informatik
 - + Wirtschaftsinformatik
- (auch in individueller Teilzeit möglich)

Masterstudiengänge

- + Business and Security Analytics
- + Systems Engineering (Schwerpunkt Security)

Weiterbildungsangebote

- + Studium Initiale
- + Hochschulzertifikate
- + TI berufsbegleitend (BEng)
- + Data Science (MSc)
- + Digitale Forensik (MSc)
- + IT GRC Management (MSc)

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

IT Security – anonym und
sicher im Netz

Agenda

- Cyber Security
- World Wide Web
- Social Engineering
- Passwortsicherheit
- Hacking Hardware

Download der Unterlage: <https://hs-as.net/bl.pdf>

IT Security – anonym und sicher im Netz

Cyber Security

World Wide Web

Social Engineering

Passwortsicherheit

Hacking Hardware



Cyber Security

Wann gab es die ersten Computer Viren?

1985

A

1990

B

1995

C

2000

D

IT Security – anonym und
sicher im Netz

Geschichte der Schadsoftware

Gestern

Heute

Morgen

Gestern Die ersten Entwicklungen

■ 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

Gestern 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



Quelle: [wikipedia.org](https://de.wikipedia.org/wiki/PC_Cyborg_Corporation) [2]

Heute Cybercrime as a Service



Heute Cybercrime as a Service

IT Security – anonym und sicher im Netz



Koordinator

Heute 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)

PRAXIS Geklaute Zugangsdaten



[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



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](#)

Recently added breaches

-  772,904,991 [Collection #1 accounts](#)
-  87,633 [FaceUP accounts](#)
-  4,848,734 [Dangdang accounts](#)
-  213,415 [BannerBit accounts](#)

Quelle: haveibeenpwned.com [5]

Morgen 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



IT Security – anonym und
sicher im Netz

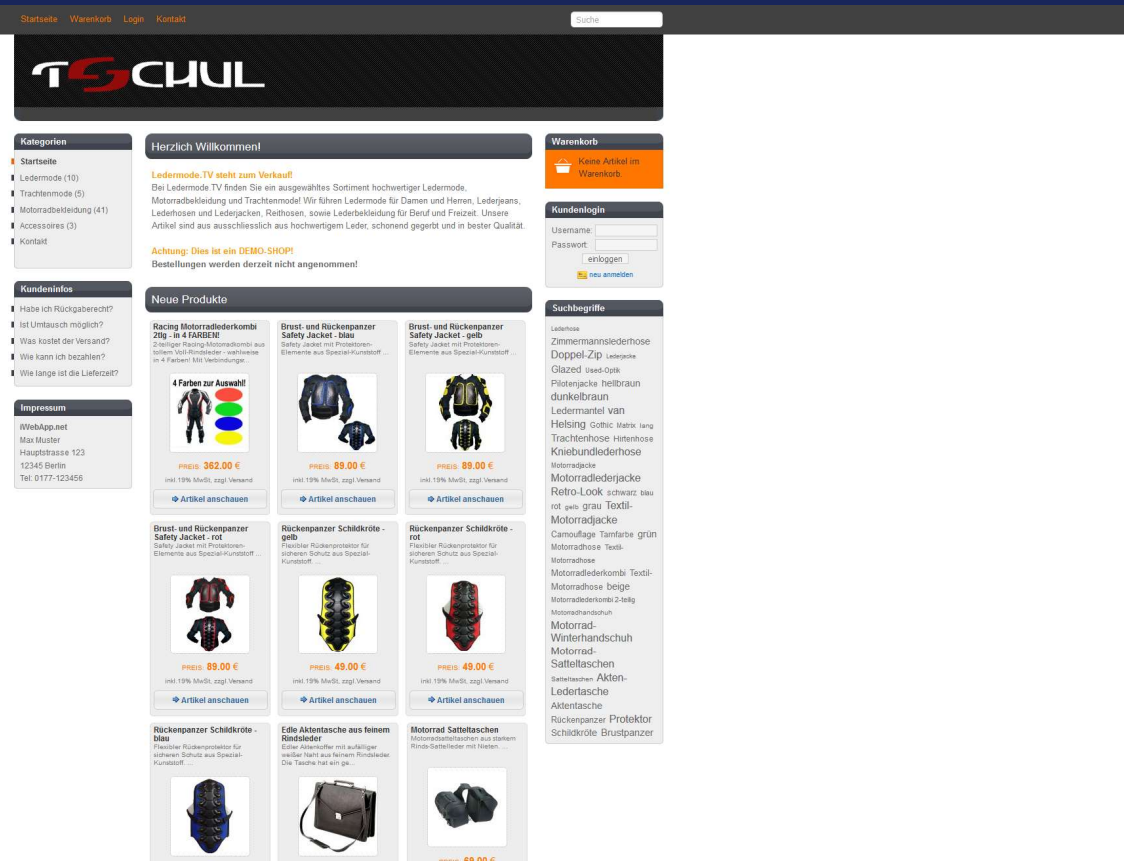
Morgen Ransomware - IoT & Industrieanlagen





World Wide Web

DEMO Live-Hack



The screenshot shows the homepage of the ledermode.tv website. At the top, there is a navigation bar with links for 'Startseite', 'Warenkorb', 'Login', and 'Kontakt', along with a search bar. The main header features the 'TSCHUL' logo. Below the header, there are several sections: 'Kategorien' (Categories) with links to 'Startseite', 'Ledermode (10)', 'Trachtenmode (5)', 'Motorradbekleidung (41)', 'Accessoires (3)', and 'Kontakt'; 'Kundeninfos' (Customer Information) with links to 'Habe ich Rückgaberecht?', 'Ist Umtausch möglich?', 'Was kostet der Versand?', 'Wie kann ich bezahlen?', and 'Wie lange ist die Lieferzeit?'; 'Impressum' (Imprint) with contact details for 'WebApp.net' in Berlin; 'Herzlich Willkommen' (Welcome) with a promotional message about leather goods; 'Warenkorb' (Shopping Cart) showing 'Keine Artikel im Warenkorb'; 'Kundenlogin' (Customer Login) with fields for 'Username' and 'Passwort'; and 'Suchbegriffe' (Search Terms) with a list of product categories. The main content area is titled 'Neue Produkte' (New Products) and displays a grid of motorcycle gear items, each with a product image, title, price, and a 'Artikel anschauen' (View Article) button. The items include: 'Racing Motorradlederkombi 2tlg. in 4 FARBEN!' (€382.00), 'Brust- und Rückenpanzer Safety Jacket - blau' (€89.00), 'Brust- und Rückenpanzer Safety Jacket - gelb' (€89.00), 'Brust- und Rückenpanzer Safety Jacket - rot' (€89.00), 'Rückenpanzer Schildkrote - gelb' (€49.00), 'Rückenpanzer Schildkrote - rot' (€49.00), 'Rückenpanzer Schildkrote - blau' (€49.00), 'Edle Akten tasche aus feinem Rindsleder' (€68.00), and 'Motorrad Satteltaschen' (€68.00).

IT Security – anonym und sicher im Netz

Das World Wide Web

Das World Wide Web ist ein über das Internet abrufbares System von elektronischen Hypertext-Dokumenten, sogenannten Webseiten, welche mit HTML beschrieben werden. Sie sind durch Hyperlinks untereinander verknüpft und werden im Internet über die Protokolle HTTP oder HTTPS übertragen.

- Internet ≠ World Wide Web | Bedroht durch Walled Garden (Apps)
- Datenschutz & Privatsphäre
 - Das Nutzerverhalten von Internetnutzern wird gezielt und möglichst seitenübergreifend aufgezeichnet.
 - Gründe dafür sind die Optimierung von Dienstleitungen, zielgerichtetes Marketing sowie die Profildaten im Allgemeinen.
 - Dies lässt sich nicht vollständig vermeiden, jedoch zumindest etwas einschränken, wenn man auch etwas "Komfort" dabei einbüßt.

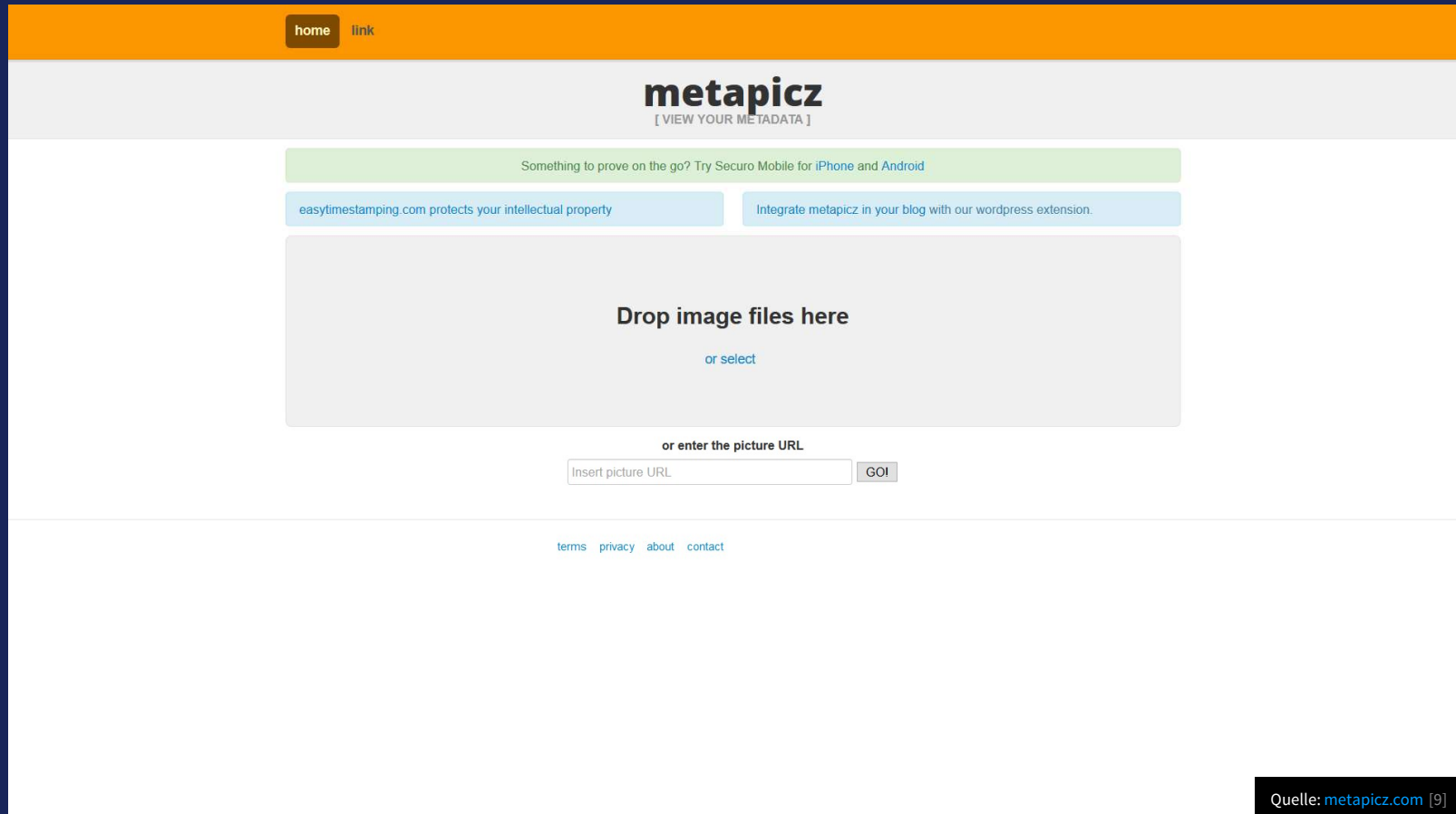
**IT Security – anonym und
sicher im Netz**

PRAXIS Web-Browser absichern

- Laden Sie den Portable Browser Firefox herunter und rufen Sie die Seite <http://mybrowserinfo.com> auf.
- Installieren Sie die folgenden AddOns:
 - uBlock Origin, Canvas Defender & User Agent Switcher
- Weitere Hinweise zur Installation:
 - <https://scheible.it/firefox-web-browser-security-tuning/>
- Prüfen Sie, wie sich die genannten Websites bei aktiviertem / deaktiviertem AddOn unterschiedlich verhalten.

IT Security – anonym und
sicher im Netz

Versteckte Informationen auslesen



The screenshot shows the metapicz website interface. At the top, there is an orange navigation bar with 'home' and 'link' buttons. Below this is a grey header with the 'metapicz' logo and a link to '[VIEW YOUR METADATA]'. The main content area features a green banner with the text 'Something to prove on the go? Try Securo Mobile for iPhone and Android'. Below the banner are two light blue buttons: 'easytimeslamping.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 containing 'Insert picture URL' and a 'GO!' button. At the bottom of the page, there are links for 'terms', 'privacy', 'about', and 'contact'. A black box in the bottom right corner of the screenshot contains the text 'Quelle: metapicz.com [9]'.

Quelle: metapicz.com [9]

PRAXIS Versteckte Informationen auslesen

- Fotos, die mit dem iPhone, Android Smartphone oder mit einer Digitalkamera gemacht werden, enthalten in der Regel Metadaten. Das sind z. B.:
 - Aufnahmedatum, Autor, ...
 - Kameramodell, Belichtungszeit, Blitzeinstellung...
 - aber auch Geoinformationen / GPS-Koordinaten
- Schauen Sie sich an, ob Sie im Internet Fotos finden, die entsprechende Metadaten enthalten.

<http://metapicz.com>

IT Security – anonym und
sicher im Netz

Wie können versteckte Systeme gefunden werden?

Spezielle Software

A

Suchmaschinen

B

Geheime Datenbanken

C

Darknet

D

IT Security – anonym und
sicher im Netz

Hacking mit Google

Google
Deutschland

Google-Suche

Auf gut Glück!

Hacking mit Google

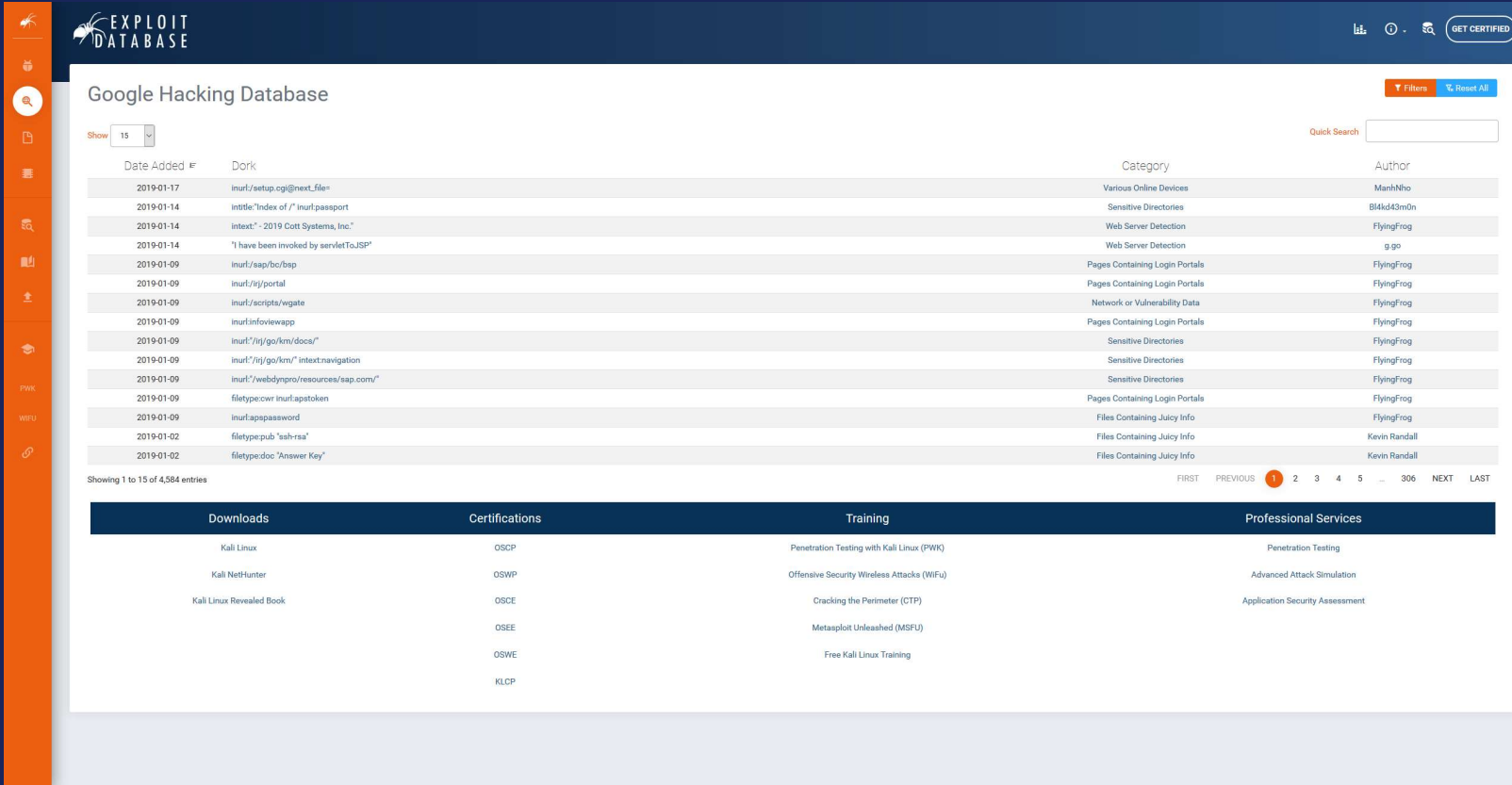
Parameter	Beschreibung
site:	Eine Suche mit dem Suchparameter "site" in Verbindung mit einer Domain oder URL liefert alle Seiten dieser Domain, die verfügbar sind. Beispiel: <i>it security site:hs-albsig.de</i>
intitle:	Eine Suche mit dem Suchparameter "intitle" in Verbindung mit einem Suchbegriff liefert 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 enthält. 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>

IT Security – anonym und
sicher im Netz

PRAXIS 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"`

Hacking mit Google - GHDB



EXPLOIT DATABASE

Google Hacking Database

Show 15

Quick Search

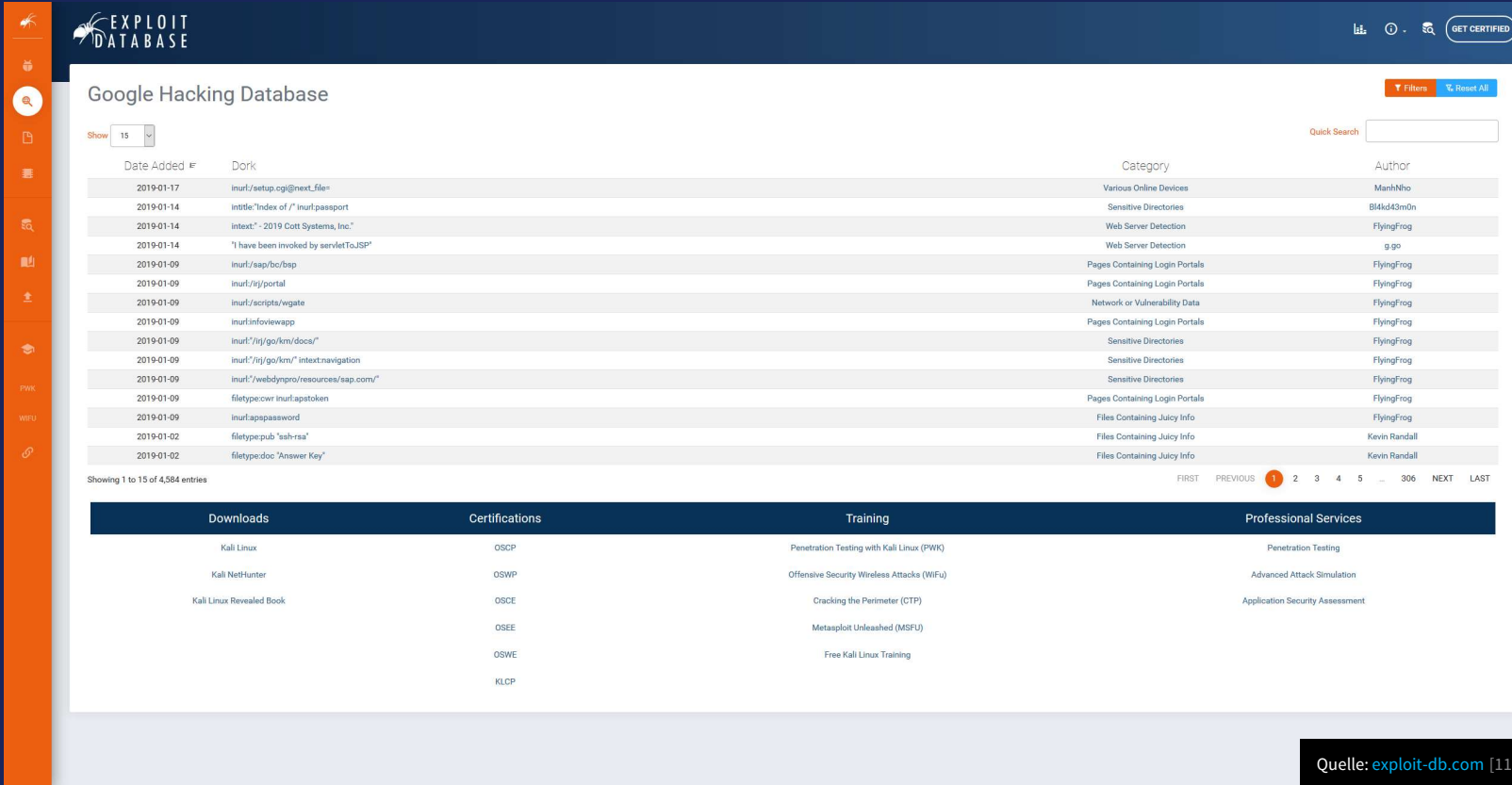
Date Added	Dork	Category	Author
2019-01-17	inurl:/setup.cgi?next_file=	Various Online Devices	ManhNho
2019-01-14	intitle:"Index of /" inurl:passport	Sensitive Directories	Bl4kd43m0n
2019-01-14	intext:"- 2019 Cott Systems, Inc."	Web Server Detection	FlyingFrog
2019-01-14	"I have been invoked by servletToJSP"	Web Server Detection	goge
2019-01-09	inurl:/snp/bc/bsp	Pages Containing Login Portals	FlyingFrog
2019-01-09	inurl:/ij/portal	Pages Containing Login Portals	FlyingFrog
2019-01-09	inurl:/scripts/vgateway	Network or Vulnerability Data	FlyingFrog
2019-01-09	inurl:/info/iewapp	Pages Containing Login Portals	FlyingFrog
2019-01-09	inurl:/ij/go/km/docs/"	Sensitive Directories	FlyingFrog
2019-01-09	inurl:/ij/go/km/" intext:navigation	Sensitive Directories	FlyingFrog
2019-01-09	inurl:/webdynpro/resources/sap.com/"	Sensitive Directories	FlyingFrog
2019-01-09	filetype:cwr inurl:aptoken	Pages Containing Login Portals	FlyingFrog
2019-01-09	inurl:appsapassword	Files Containing Juicy Info	FlyingFrog
2019-01-02	filetype:pub "sah-raa"	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	OSCP	Penetration Testing with Kali Linux (PWK)	Penetration Testing
Kali NetHunter	OSWP	Offensive Security Wireless Attacks (WiFi)	Advanced Attack Simulation
Kali Linux Revealed Book	OSCE	Cracking the Perimeter (CTP)	Application Security Assessment
	OSSE	Metasploit Unleashed (MSFU)	
	OSWE	Free Kali Linux Training	
	KLCP		

PRAXIS Hacking mit Google - GHDB



EXPLOIT DATABASE

Google Hacking Database

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 ge
2019-01-09	inurl:/snp/bc/bsp	Pages Containing Login Portals	FlyingFrog
2019-01-09	inurl:/ij/portal	Pages Containing Login Portals	FlyingFrog
2019-01-09	inurl:/scripts/vgate	Network or Vulnerability Data	FlyingFrog
2019-01-09	inurl:infoviewapp	Pages Containing Login Portals	FlyingFrog
2019-01-09	inurl:/ij/go/km/docs/"	Sensitive Directories	FlyingFrog
2019-01-09	inurl:/ij/go/km/" intext:navigation	Sensitive Directories	FlyingFrog
2019-01-09	inurl:/webdynpro/resources/sap.com/"	Sensitive Directories	FlyingFrog
2019-01-09	filetype:cwr inurl:ap token	Pages Containing Login Portals	FlyingFrog
2019-01-09	inurl:appassword	Files Containing Juicy Info	FlyingFrog
2019-01-02	filetype:pub "sah-raa"	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	OSCP	Penetration Testing with Kali Linux (PWK)	Penetration Testing
Kali NetHunter	OSWP	Offensive Security Wireless Attacks (WiFi)	Advanced Attack Simulation
Kali Linux Revealed Book	OSCE	Cracking the Perimeter (CTP)	Application Security Assessment
	OSSE	Metasploit Unleashed (MSFU)	
	OSWE	Free Kali Linux Training	
	KLCP		

Quelle: exploit-db.com [11]

Bug or Feature?

Einloggen auf heise online

 heise online

in heise Security suchen 

 heise Security

News ▾ Hintergrund Tools Foren

Kontakt  

Security > News > 7-Tage-News > 2016 > KW 2 > IP-Kameras von Aldi mit massiven Sicherheitslücken

« Vorige | Nächste »

 Alert!

IP-Kameras von Aldi als Sicherheits-GAU

15.01.2016 10:49 Uhr – Ronald Eikenberg

 vorlesen



Aldi hatte vergangenes Jahr mehrfach IP-Überwachungskameras mit denkbar schlechten Voreinstellungen verkauft. Die Geräte sind zu Hunderten fast ungeschützt über das Internet erreichbar.

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

Dienste

Security-Consulting | Emailcheck
Netzwerkcheck | Browsercheck
Anti-Virus | Krypto-Kampagne

TeslaCrypt 2.0 entschlüsselt

Die Ransomware TeslaCrypt ist geknackt und betroffene Nutzer können auch ohne das Zahlen von Lösegeld wieder Zugriff auf ihre verschlüsselten Daten erlangen. Heise Security hat das erfolgreich ausprobiert. Mehr...



Analysiert: Lego Mindstorms für Cyber-Angriffe missbraucht

In einer deutschen



Forschungseinrichtung arbeiten auch Lego-Roboter im Dienste der Wissenschaft. Eines Tages entwickelten diese jedoch ein gefährliches Eigenleben. Mehr...

Router auf WPS-Lücken testen

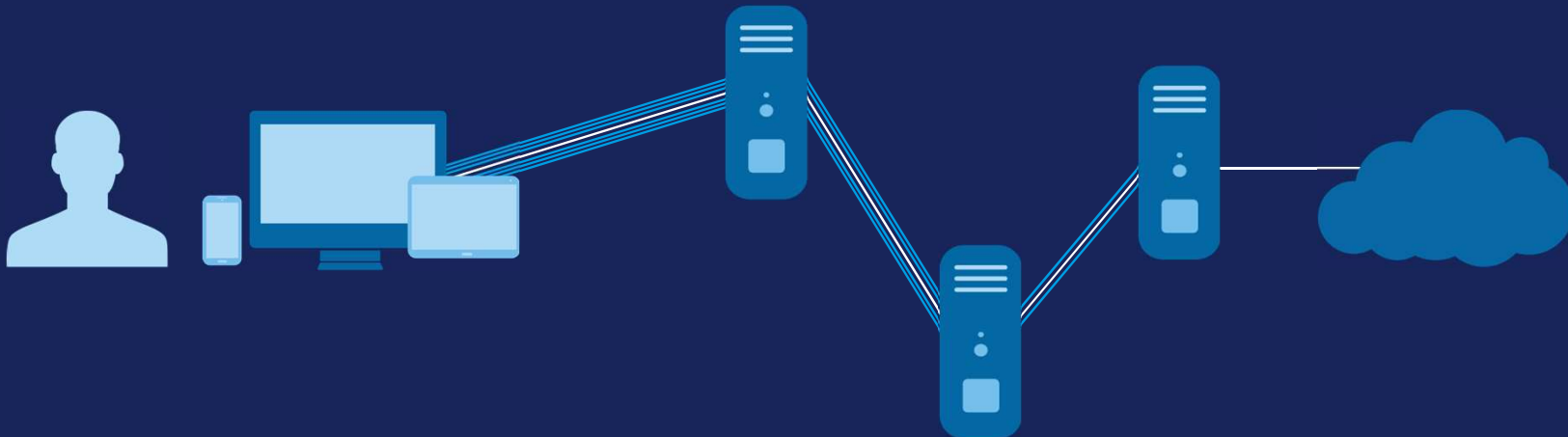
DEMO Suchmaschine für das Internet der Dinge



The screenshot shows the Shodan website homepage. At the top, there is a navigation bar with the Shodan logo, a search bar, and links for 'Explore', 'Enterprise Access', and 'Contact Us'. The main header features the text 'The search engine for the Web' and 'Shodan is the world's first search engine for Internet-connected devices.' Below this, 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 small icon and a brief description. Below this, there is a blue banner with two statistics: '56% of Fortune 100' and '1,000+ Universities'. The bottom section is titled 'Analyze the Internet in Seconds' and features a world map with red dots indicating server locations. A 'Sample Report on Heartbleed' button is also present. At the very bottom, there is a section titled 'Beyond the Web' with a brief description and icons for various browsers.

Tor Netzwerk

- Spendenfinanziertes Opensource-Projekt mit über 5000 Tor-Nodes
- Komplette Browser Bundles für Windows, Mac OS X, Linux, Android
- Zufällige und verschlüsselte Route über drei Tor-Nodes
- Jede Note kennt immer nur den Vorgänger und den Nachfolger
- Wichtig: nur Anonymisierung, keine Verschlüsselung und Integritätsschutz



PRAXIS Tor Netzwerk - Darknet

- Laden Sie den TOR-Browser herunter
 - <https://www.torproject.org/projects/torbrowser.html.en>
- Welche Informationen werden zur Verfügung gestellt?
 - <http://www.utrace.de> und <http://mybrowserinfo.com>
- Surfen Sie auf einer Website und prüfen Sie, welche Verbindungsrouten gewählt wurde
 - Wechseln Sie Ihre Identität
- Öffnen Sie die folgenden Hidden Services (Darknet-Websites):
 - <https://3g2upl4pq6kufc4m.onion>
 - <http://vfqnd6mieccqyiit.onion>

IT Security – anonym und
sicher im Netz

Fazit World Wide Web

- Wenn Sie Fotos online stellen, entfernen Sie alle Metadaten von diesen Fotos.
- Die Surfgeohnheiten können sehr einfach erfasst werden, auch wenn der Verlauf und alle Cookies gelöscht werden. Daher müssen Plugins eingesetzt werden, um die Spuren zu verschleiern.
- Nutzen Sie mehrere Web-Browser (Firefox, Chrome & Edge) für unterschiedliche Aktivitäten. Einen für die dauerhaften Logins, einen für die tägliche Recherche und einen für Medien.
- Nutzen Sie den Tor-Browser, um Ihre Privatsphäre zu schützen, wenn Sie nach sehr privaten Themen im Internet suchen.

A person wearing a glowing yellow mask with a skull-like pattern, standing in a dark, futuristic environment with blue neon lights and floating playing cards. The scene is filled with a sense of mystery and digital intrigue. The person is holding a large playing card, specifically the Ace of Spades, which is prominently displayed in the foreground. The background features a glowing blue archway and various other playing cards floating in the air, creating a surreal and high-tech atmosphere. The overall color palette is dominated by dark blues, blacks, and bright yellows and oranges from the lights and the mask.

Social Engineering

Was ist die häufigste Angriffsmethode?

Ausnutzung von Schwachstellen

A

Physische Attacken

B

Manipulation von Personen

C

Ausnutzung von Fehlern

D

IT Security – anonym und
sicher im Netz

Aktion der Groupe Mutuel



Zürich, Hauptbahnhof

Quelle: [youtube.com](https://www.youtube.com/watch?v=14) [14]

IT Security – anonym und
sicher im Netz

Social Engineering - 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

DPA

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.

Moderner 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

IT Security – anonym und
sicher im Netz

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 @	E-STOXX 50@	MDAX @	Dow Jones	Gold (USD)	EUR/USD	Börsenkurse
8.752,87 -2,93%	2.680,35 -3,90%	17.594,68 -2,83%	15.660,18 -1,60%	1.242,83 -0,30%	1,1315 -0,00%	cm Indikatoren

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

Falsche Chefs zocken Firmen ab

18. August 2015

Den Enkeltrick gibt's auch bei Unternehmen

★★★★☆
0
Kommentare

Versenden
Drucken
Merken
Startseite



Nicht nur gutgläubige Senioren werden Opfer von Trickbetrügern.

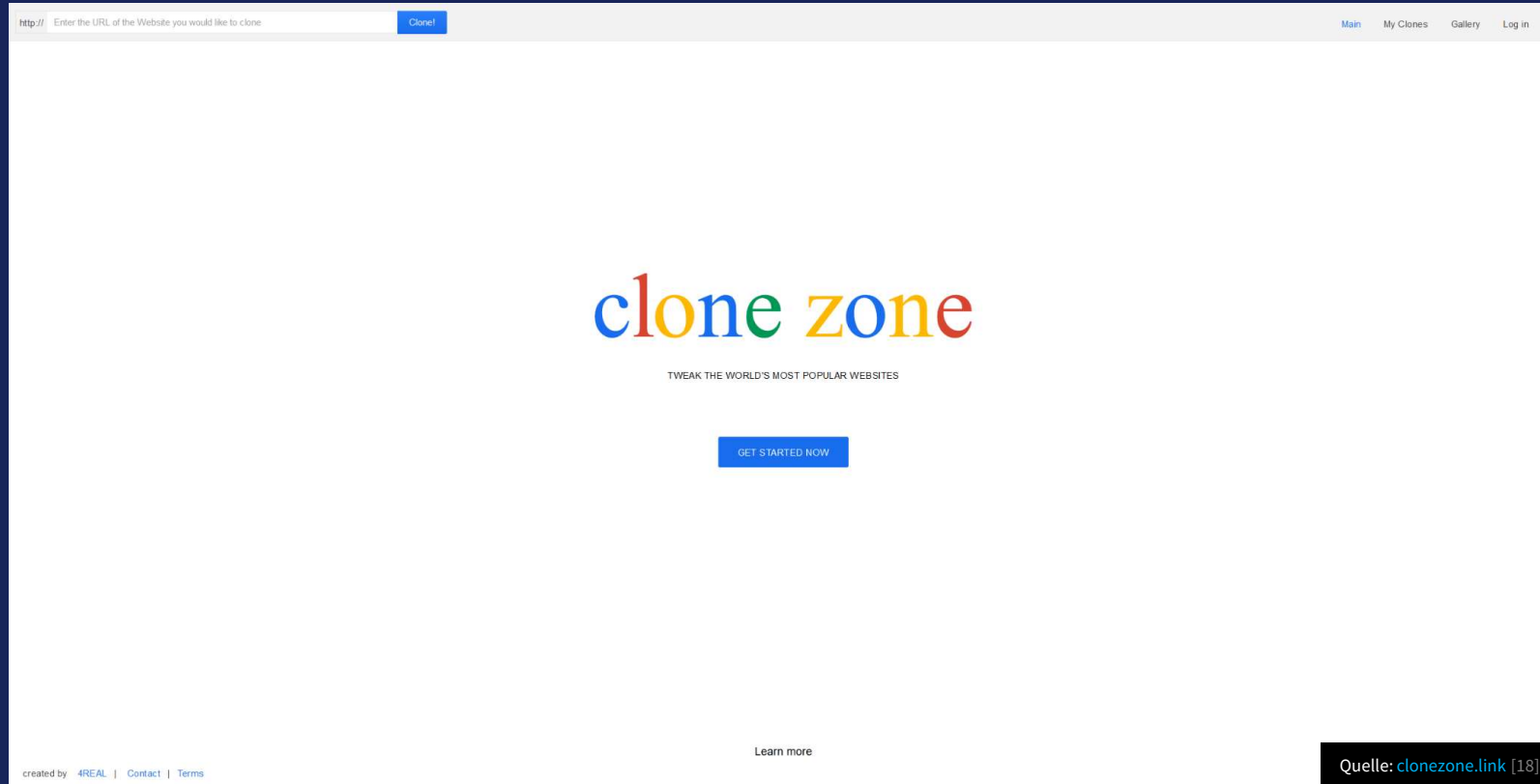
Bild: dpa

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

IT Security – anonym und sicher im Netz

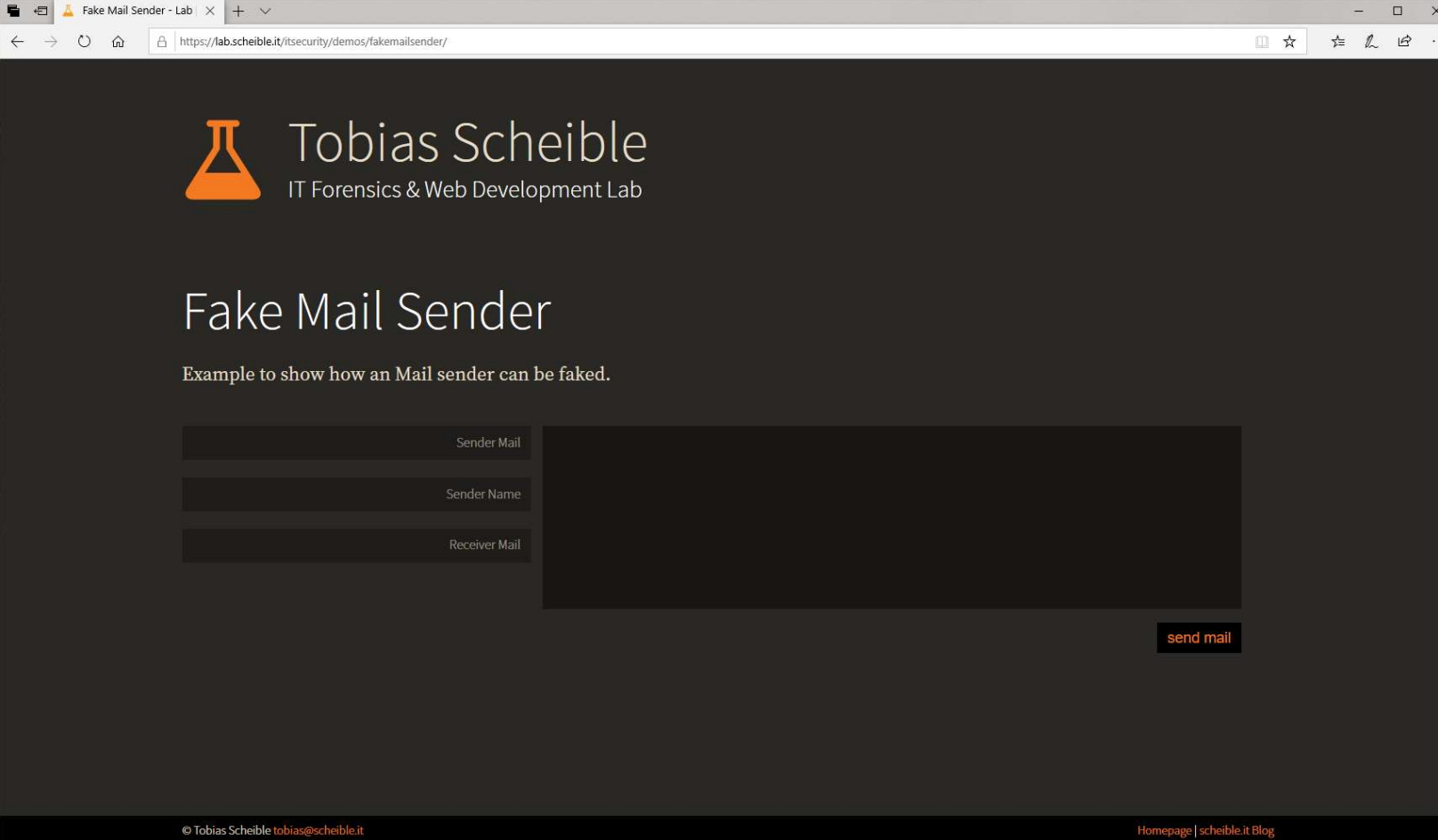
PRAXIS Website manipulieren



The screenshot shows the CloneZone website interface. At the top, there is a search bar with the placeholder text "Enter the URL of the Website you would like to clone" and a blue "Clone!" button. To the right of the search bar, there are navigation links: "Main", "My Clones", "Gallery", and "Log in". The main content area features the "clone zone" logo in a colorful, lowercase font. Below the logo, the text "TWEAK THE WORLD'S MOST POPULAR WEBSITES" is displayed. A prominent blue button labeled "GET STARTED NOW" is centered below the text. At the bottom left, there is a footer with the text "created by 4REAL | Contact | Terms". At the bottom right, there is a "Learn more" link and a dark box containing the text "Quelle: clonezone.link [18]".

IT Security – anonym und
sicher im Netz

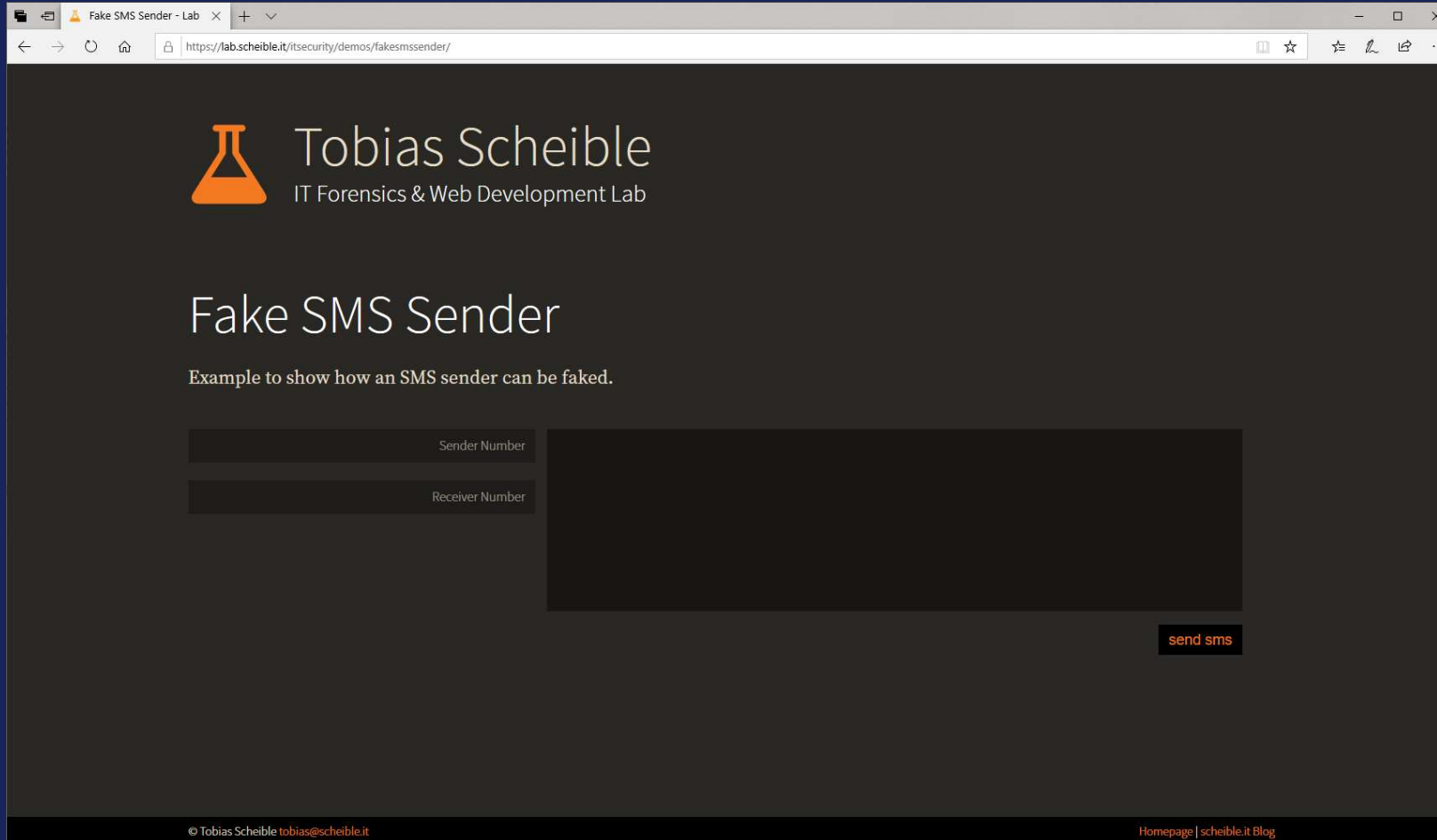
DEMO E-Mail-Versand manipulieren



The screenshot shows a web browser window with the URL <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 are three input fields: "Sender Mail", "Sender Name", and "Receiver Mail". A large, empty text area is positioned to the right of these fields. At the bottom right of the form area, there is a "send mail" button. The footer of the page contains the copyright notice "© Tobias Scheible tobias@scheible.it" and the links "Homepage | scheible.it Blog".

IT Security – anonym und
sicher im Netz

DEMO SMS-Versand manipulieren



Fake SMS Sender

Example to show how an SMS sender can be faked.

Sender Number

Receiver Number

send sms

© Tobias Scheible tobias@scheible.it

Homepage | [scheible.it Blog](#)

IT Security – anonym und
sicher im Netz

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.
- Tipp: Auf einem anderen Kanal nachfragen, ob es wirklich stimmt.

A person wearing a grey hoodie and a black mask with white, jagged, tooth-like patterns around the mouth and eyes. The person is standing in a dark room illuminated by green neon lights. The background shows a wall with some graffiti, including the word "DEATH" and "GIRL".

Passwortsicherheit

00000000



Wofür wurde der Pin-Code verwendet?

Fort Knox

A

Alcatraz

B

Area 51

C

Atomraketen

D

IT Security – anonym und
sicher im Netz

00000000

Launch-Code für die in den USA stationierten Atomraketen

(1962 bis 1977)

Faktor Mensch

I wonder what the code could be...



Quelle: pics-for-fun.com [20]



Quelle: de.pinterest.com [21]

IT Security – anonym und
sicher im Netz

Passwortsicherheit

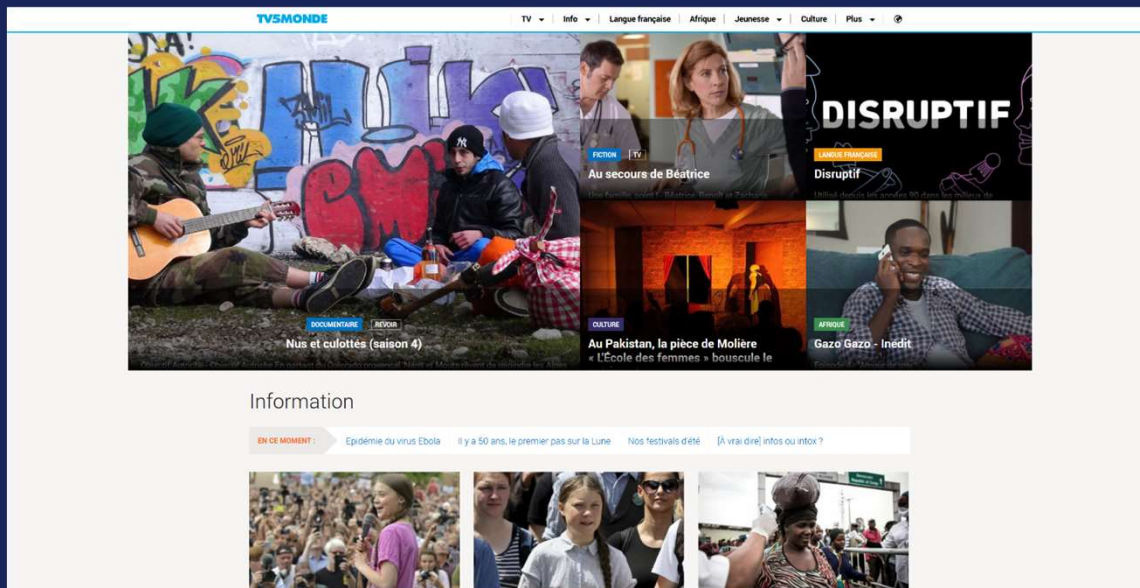
IT Security – anonym und
sicher im Netz



Quelle: youtube.com [22]

Angriff auf den Fernsehsender TV5

- 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



IT Security – anonym und
sicher im Netz

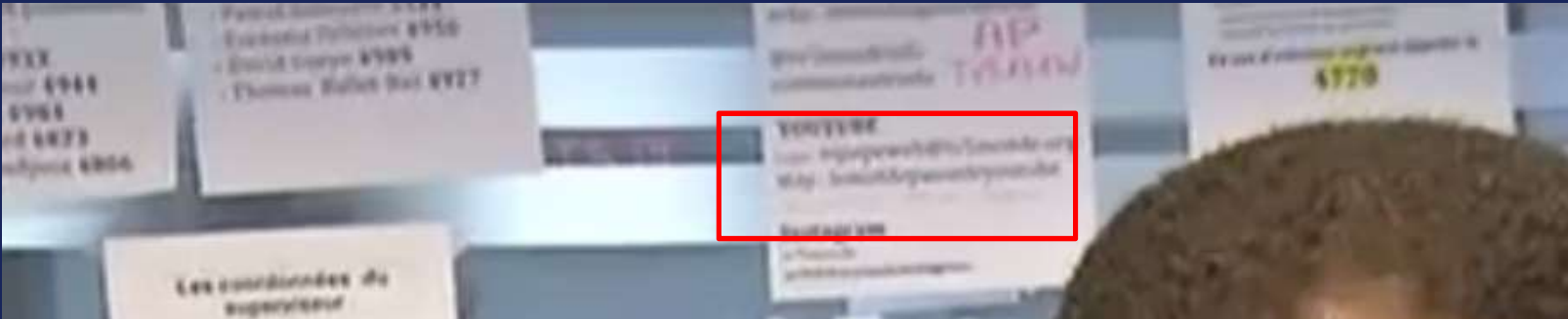
Angriff auf den Fernsehsender TV5



Quelle: [heise.de](https://www.heise.de) [23]

IT Security – anonym und
sicher im Netz

Angriff auf den Fernsehsender TV5



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



Quelle: [heise.de](https://www.heise.de) [23]

IT Security – anonym und
sicher im Netz

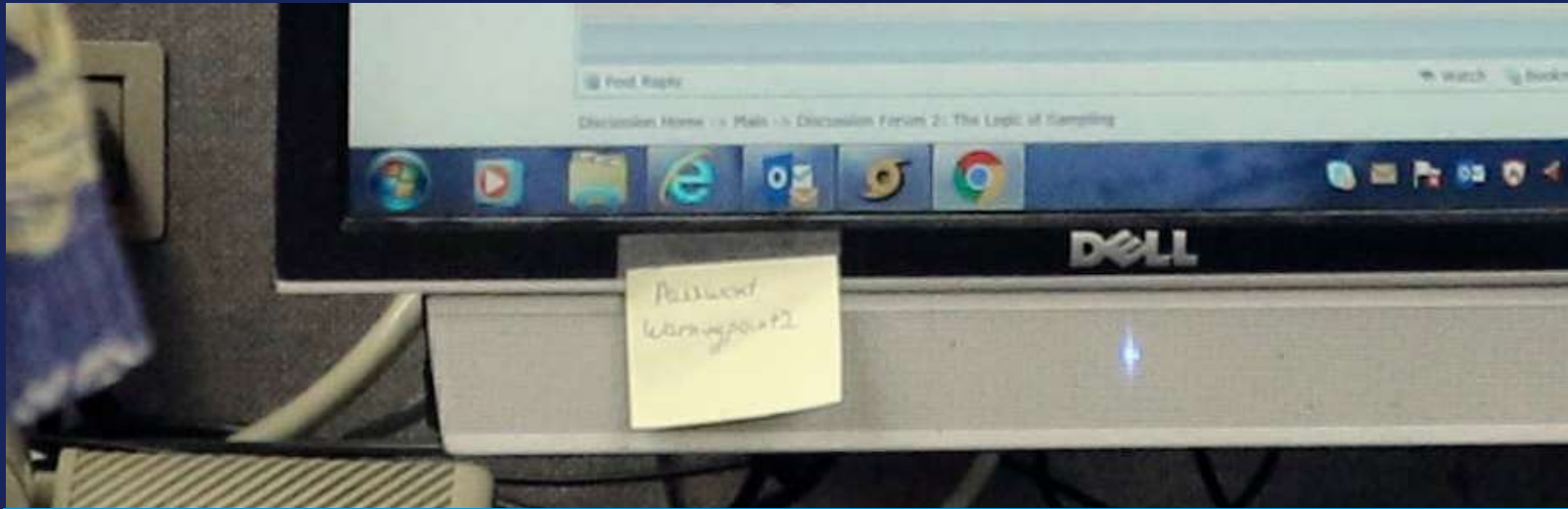
Faktor Mensch



Quelle: [vice.com](https://www.vice.com) [24]

IT Security – anonym und
sicher im Netz

Faktor Mensch



Klassiker – Post-it Zettel auf Monitor
Passwort: warningpoint2

Angriffe auf Passwörter

Passwörter
erraten

Brute-Force
Methode

Bekannte
Passwörter

IT Security – anonym und
sicher im Netz

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.

IT Security – anonym und
sicher im Netz

PRAXIS Passwörter erraten

- Versuchen Sie, die geschützten Dokumente zu knacken
 - Laden Sie die Test-Dateien herunter und analysieren Sie den Lebenslauf
 - Probieren Sie verschiedene Passwortkombinationen aus
 - Versuchen Sie, die PDF-Dateien zu öffnen

Wie lauten die Passwörter der Dateien? Finden Sie mindestens eines heraus.

IT Security – anonym und sicher im Netz

Cyber Security

Passwortsicherheit

Faktor Mensch

[Passwörter erraten](#)

Brute-Force Methode

Bekannte Passwörter

Sperrmuster




Sichere Passwörter

Anonym im Internet

Gefälschte Informationen

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 [25]

IT Security – anonym und
sicher im Netz

.....
24.07.2019 | Gymnasium Balingen

Tobias Scheible, M.Eng.

Was ist das häufigste Passwort?

password

A

123456

B

adobe123

C

qwerty

D

IT Security – anonym und
sicher im Netz

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             Plaintext
18             -----
19             123456
20             123456789
21             password
22             adobe123
23             12345678
24             qwerty
25             1234567
26             111111
```

Quelle: github.com [25]

Wie häufig kam das Passwort 123456 vor?

ca. 500.000

A

ca. 1.000.000

B

ca. 2.000.000

C

ca. 3.000.000

D

IT Security – anonym und
sicher im Netz

Bekannte Passwörter

124 lines (115 sloc) | 6.67 KB

Raw

Blame

History



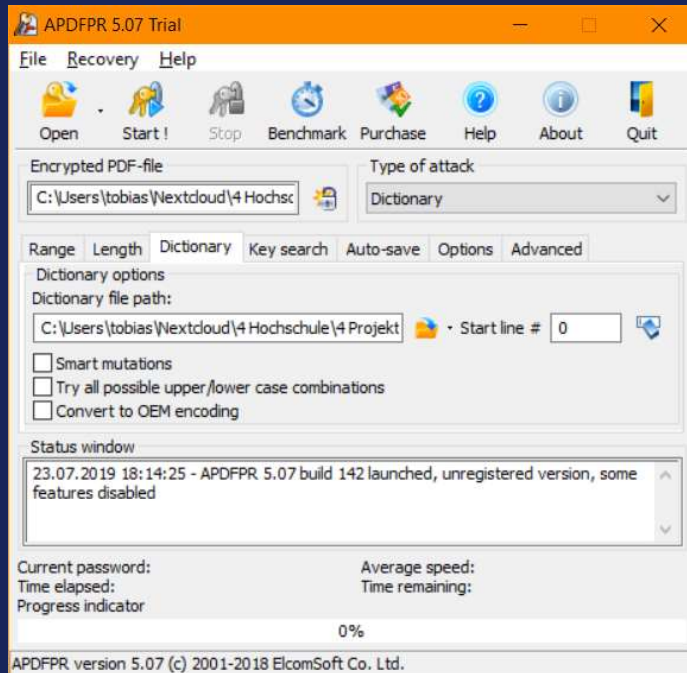
```
1 Top 100 Adobe Passwords with Count
2
3 We do not (yet) have the keys Adobe used to encrypt the passwords of 130,324,429 users affected by
4 their most recent breach. However, thanks to Adobe choosing symmetric key encryption over hashing,
5 selecting ECB mode, and using the same key for every password, 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 #      Count      Ciphertext      Plaintext
18 -----
19 1.    1911938    EQ7fIpT7i/Q=    123456
20 2.     446162    j9p+HwtWWT86aMjgZFLzYg==    123456789
21 3.     345834    L8qbAD3j13jioxG6CatHBw==    password
22 4.     211659    BB4e6X+b2xLioxG6CatHBw==    adobe123
23 5.     201580    j9p+HwtWWT/ioxG6CatHBw==    12345678
24 6.     130832    5dju7ZCI2ws=    qwerty
25 7.     124253    dQi0aswPYvQ=    1234567
26 8.     113884    7LqYzKVe8I=    111111
```

Quelle: github.com [25]

PRAXIS Bekannte Passwörter

- Laden Sie die Software herunter und knacken Sie die PDF-Dateien.
- Verwenden Sie als Wörterbuch die TXT-Datei aus der ZIP-Datei



IT Security – anonym und sicher im Netz

Cyber Security

Passwortsicherheit

- Faktor Mensch
- Passwörter erraten
- Brute-Force Methode
- Bekannte Passwörter
- Sperrmuster
- Sichere Passwörter

Anonym im Internet

Gefälschte Informationen

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.

IT Security – anonym und
sicher im Netz

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

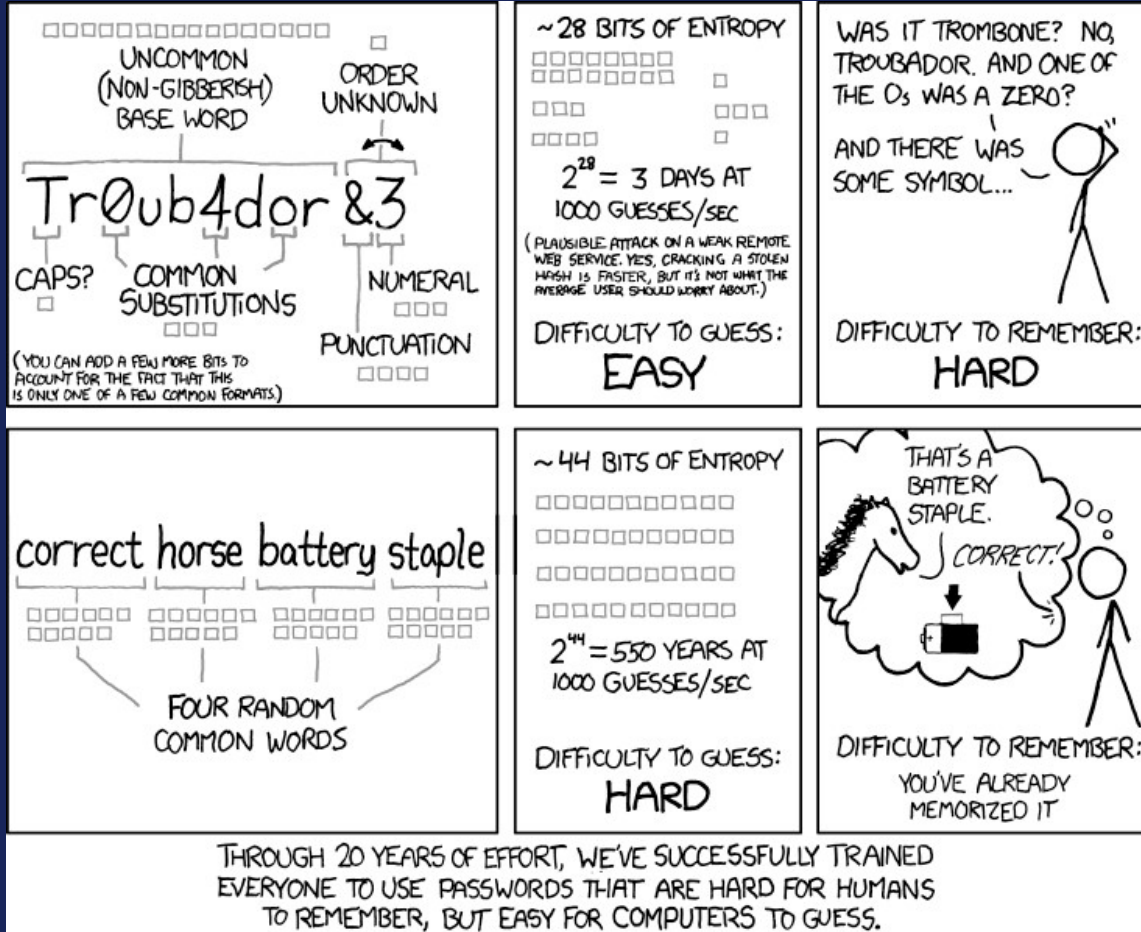
- 101 verschiedene Zeichen

- Beispiele

- Kleinbuchstaben $26^4 = 456.976$
- Kleinbuchstaben + Zahlen $36^4 = 1.679.616$
- Alle Buchstaben + Zahlen $69^4 = 22.667.121$
- Alle Zeichen $101^4 = 104.060.401$

IT Security – anonym und
sicher im Netz

Brute-Force Methode



UNCOMMON (NON-GIBBERISH) BASE WORD ORDER UNKNOWN
 Tr0ub4dor&3
 CAPS? COMMON SUBSTITUTIONS NUMERAL PUNCTUATION
 (YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)

~28 BITS OF ENTROPY
 $2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$
 (PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
 DIFFICULTY TO GUESS: **EASY**
 DIFFICULTY TO REMEMBER: **HARD**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?
 AND THERE WAS SOME SYMBOL...
 DIFFICULTY TO REMEMBER: **HARD**

correct horse battery staple
 FOUR RANDOM COMMON WORDS

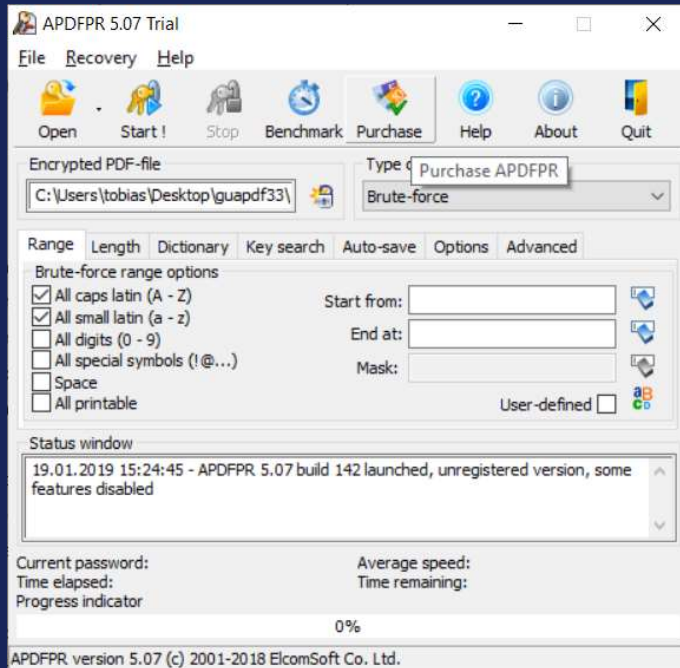
~44 BITS OF ENTROPY
 $2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$
 DIFFICULTY TO GUESS: **HARD**
 THAT'S A BATTERY STAPLE.
 CORRECT!
 DIFFICULTY TO REMEMBER: **YOU'VE ALREADY MEMORIZED IT**

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

IT Security – anonym und sicher im Netz

PRAXIS Brute-Force Methode

- Verwenden Sie wieder die Software und knacken Sie die PDF-Dateien.
- Notieren Sie jeweils die benötigte Zeit für die unterschiedlichen Dateien.



IT Security – anonym und
sicher im Netz

Sichere Passwörter

Individuelle &
lange Passwörter

Zwei-Faktor-
Authentifizierung

Bekannte
Passwörter

IT Security – anonym und
sicher im Netz

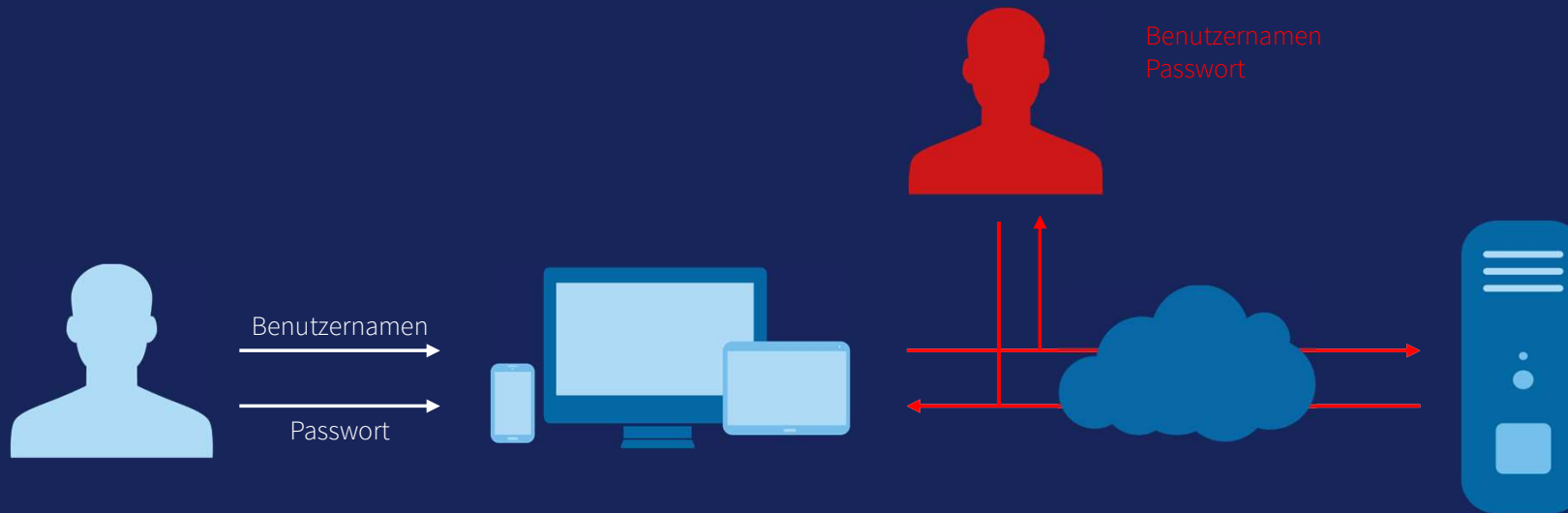
Individuelle & lange Passwörter

- Mythen
 - Passwörter brauchen möglichst viele Sonderzeichen
 - Häufige Passwortwechsel erhöhen die Sicherheit
 - Die Zwei-Faktor-Authentifizierung ist kompliziert und unnötig
 - Am besten merkt man sich Passwörter mit Stift und Papier
 - Biometrische Passwörter sind sicherer als Textpasswörter
- Möglichst lange Passwörter verwenden
- Bei jedem Dienst ein anderes Passwort verwenden
- Bildliches Szenario als Merkhilfe
- Eigenen Dialekt miteinfließen lassen

IT Security – anonym und
sicher im Netz

Zwei-Faktor-Authentifizierung

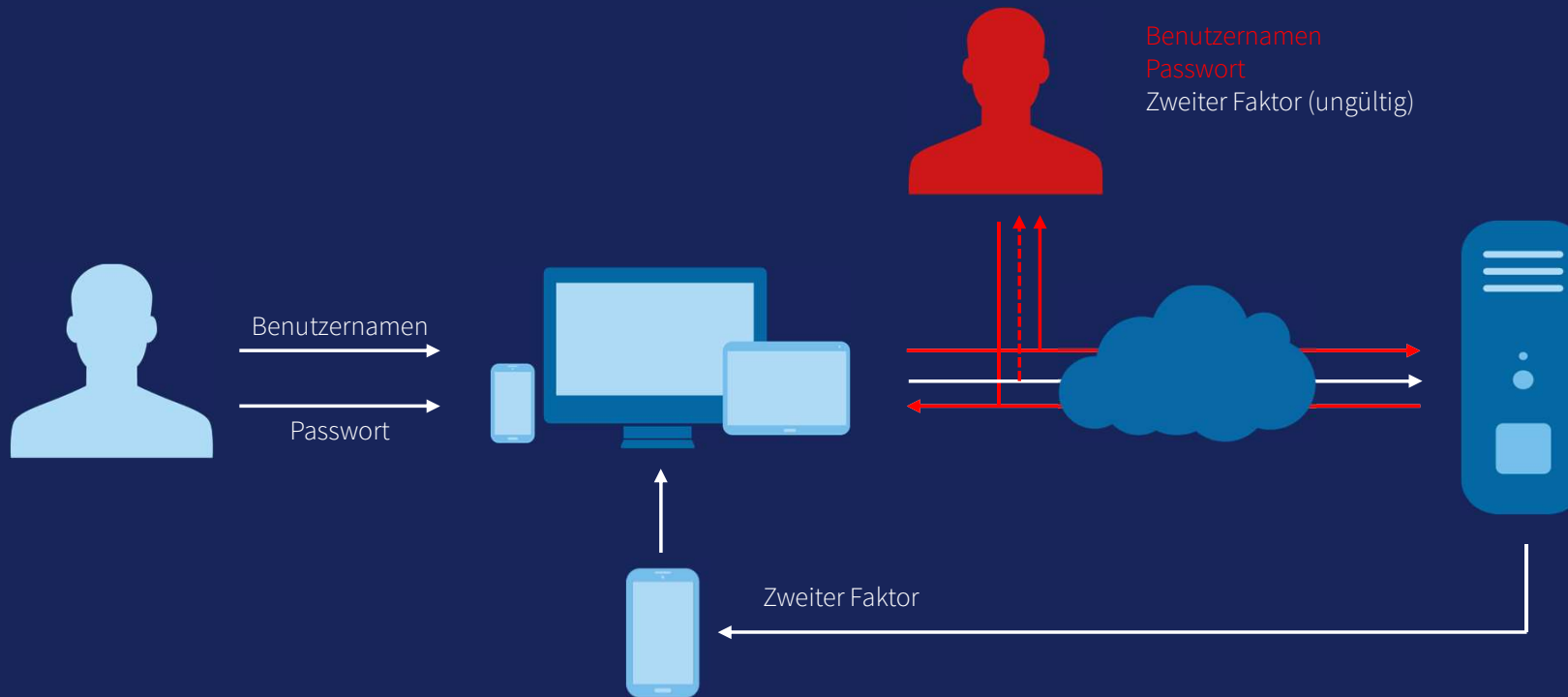
- Klassische Authentifizierung



IT Security – anonym und
sicher im Netz

Zwei-Faktor-Authentifizierung

- Klassische Authentifizierung



IT Security – anonym und
sicher im Netz

Passwortmanager

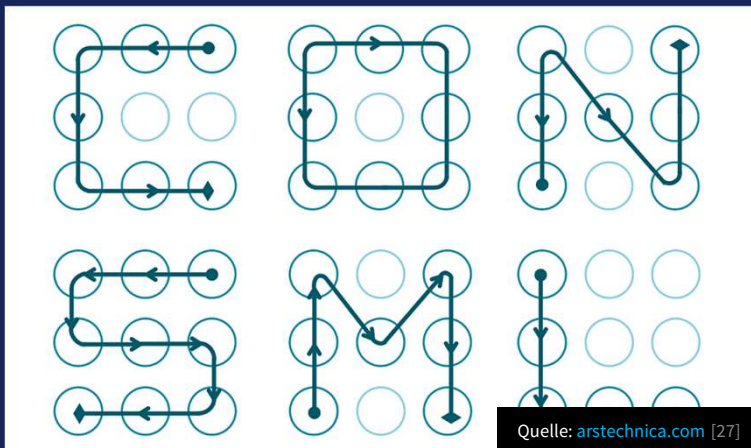
Wer viele Online-Accounts hat, für den empfiehlt sich ein Passwort-Verwaltungsprogramm. Diese Programme können neben der Passwort-Verwaltung auch starke Passwörter generieren. Sie müssen sich dann nur noch ein gutes Masterpasswort überlegen und merken.

- 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, ...)

**IT Security – anonym und
sicher im Netz**

Bad Lock Patterns

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



IT Security – anonym und
sicher im Netz

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.

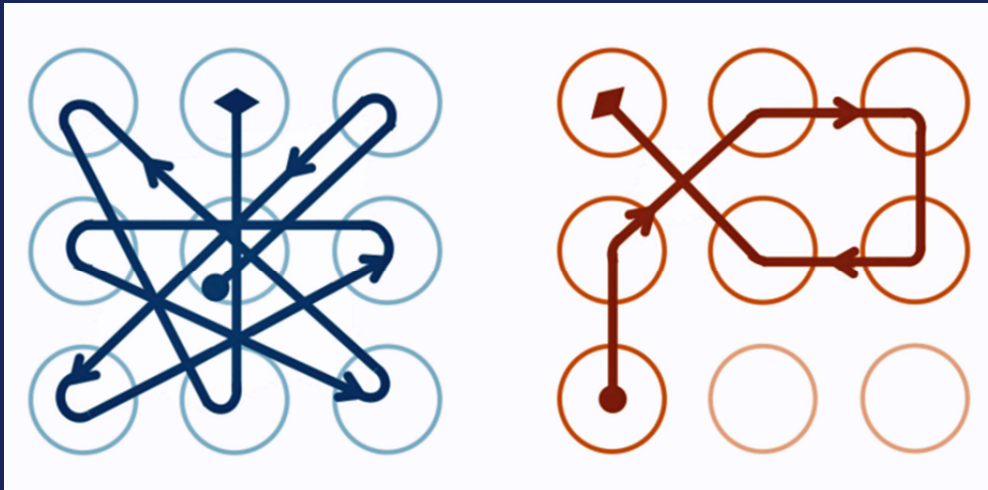
IT Security – anonym und
sicher im Netz

Sperrmuster - Brute-Force



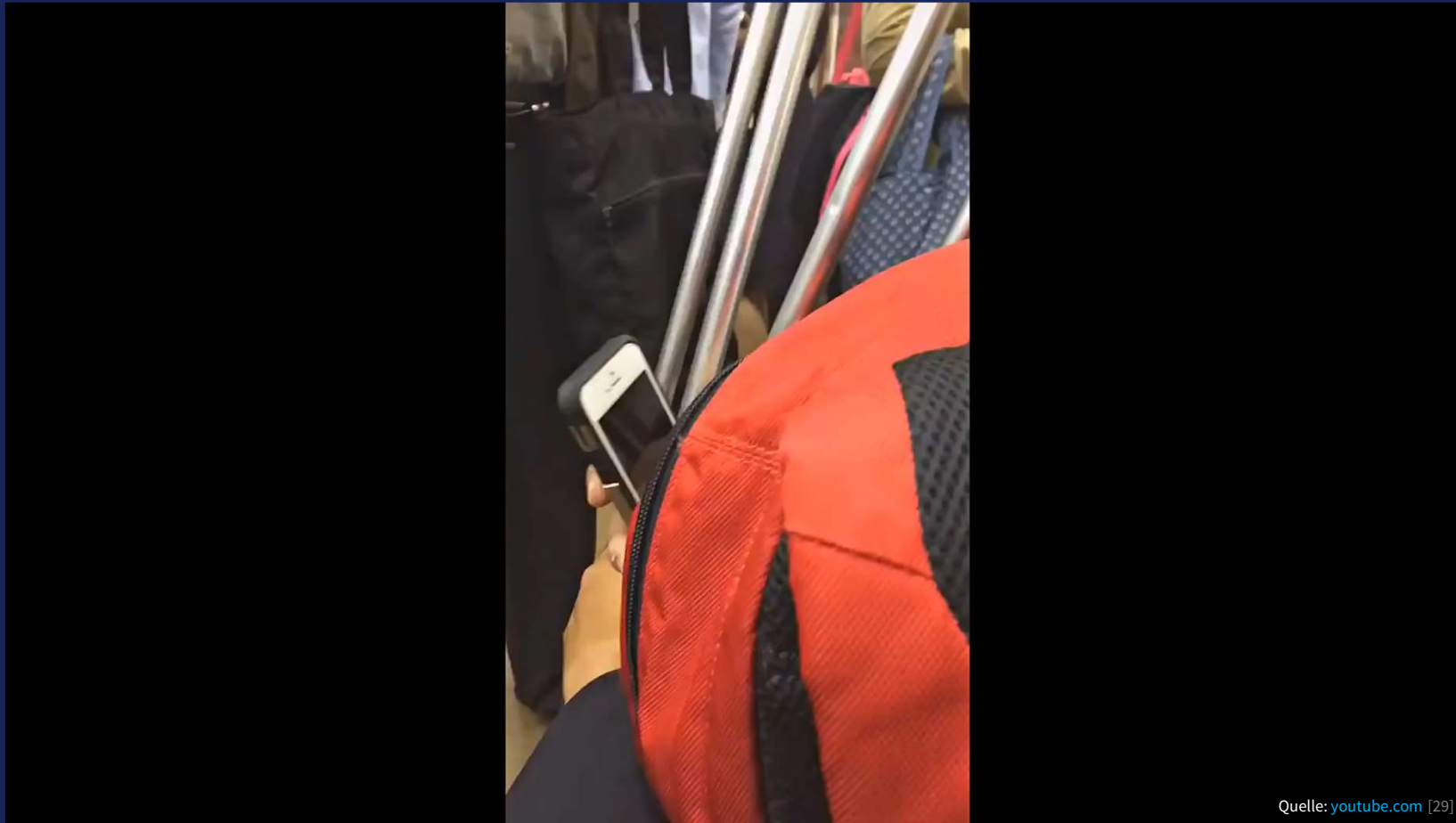
Bad Lock Patterns - Gegenmaßnahmen

- Komplizierte Muster verwenden
- Allerdings sind weitere mögliche Angriffsvektoren vorhanden:
 - Angriffe über ADB (Android Debug Bridge)
- Lange PINs verwenden



IT Security – anonym und
sicher im Netz

Bad Lock Patterns - Gegenmaßnahmen



Quelle: [youtube.com](https://www.youtube.com/watch?v=...) [29]

IT Security – anonym und
sicher im Netz

.....
24.07.2019 | Gymnasium Balingen

Tobias Scheible, M.Eng.

Passwortkarten

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

Passwortkarten

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>

Passwortkarten

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

IT Security – anonym und
sicher im Netz

Passwortkarten

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

IT Security – anonym und
sicher im Netz

Passwortkarten

Link: sparkasse.de

Passwort: *V=6<*

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>

IT Security – anonym und
sicher im Netz

Passwortkarten

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

IT Security – anonym und
sicher im Netz

Passwortkarten

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

IT Security – anonym und
sicher im Netz

Passwortkarten

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

IT Security – anonym und
sicher im Netz

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-Authentifizierung.



Hacking Hardware

Gadgets – Spionage Kamera



Gadgets – GSM Wanze



Logger - Keylogger



Logger - Screenlogger



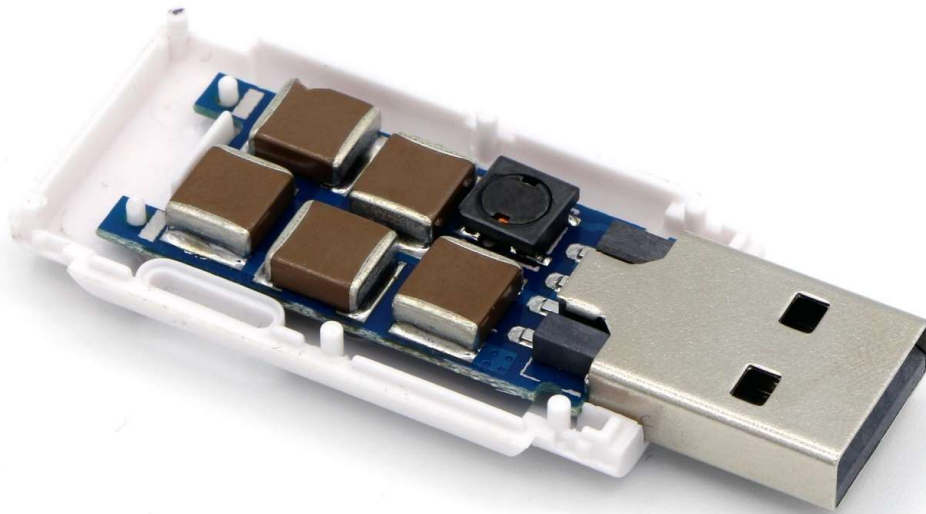
USB – BadUSB (Rubber Ducky)



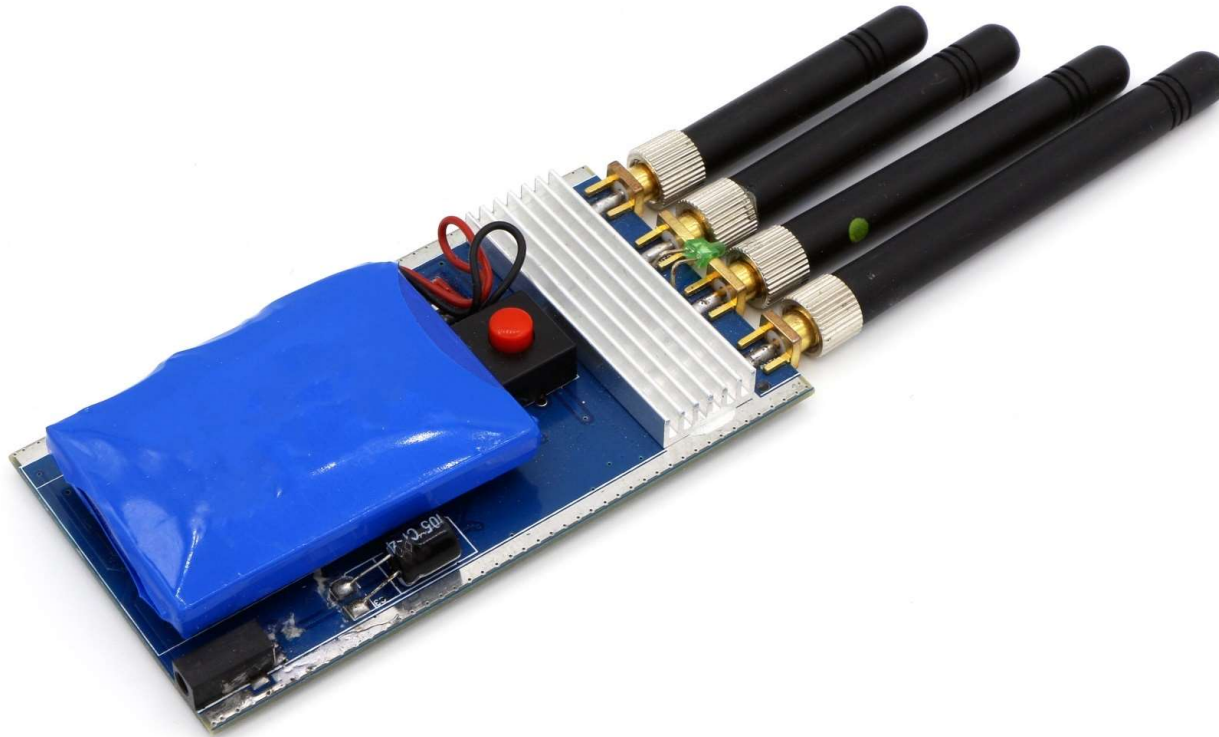
USB – BadUSB (USBNinja)



USB - USBKill



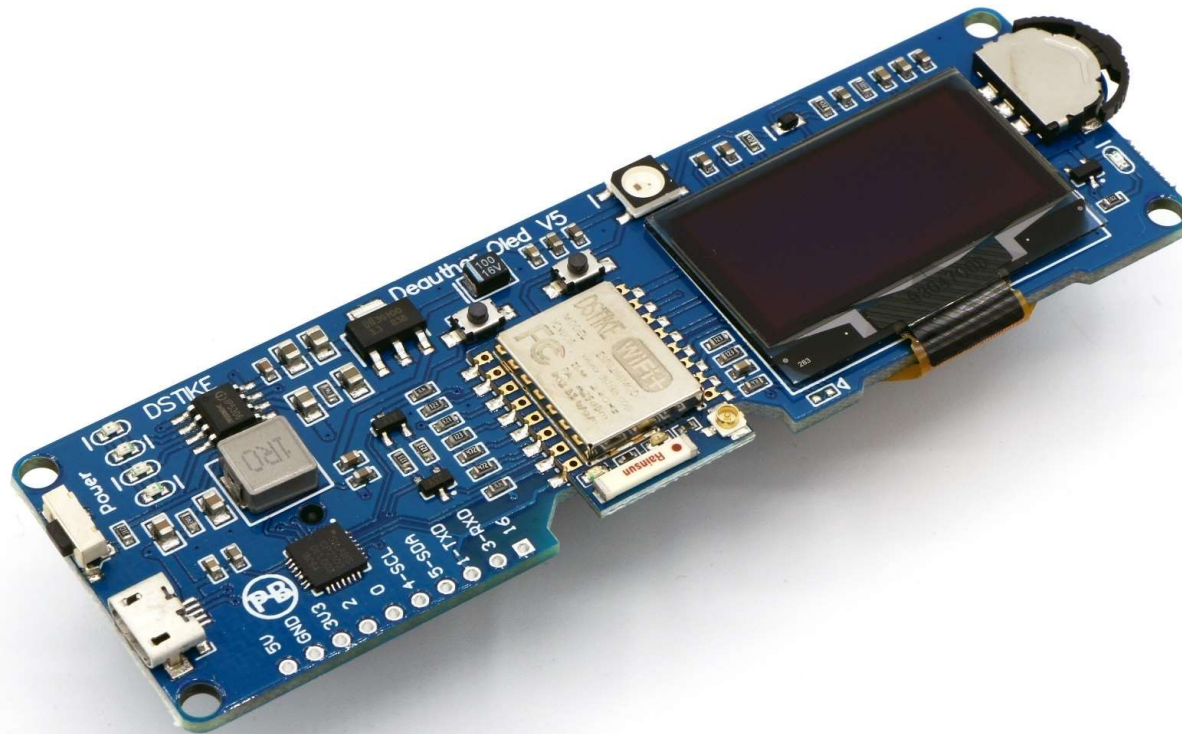
Funk - Störsender



Funk - Software Defined Radio



Netzwerk – WiFi Deauther



Netzwerk - Packet-Squirrel





Vielen Dank für Ihre Aufmerksamkeit

Präsentation demnächst online unter: <https://scheible.it>

Quellen

- (1) <https://www.gdata.de/ratgeber/was-ist-eigentlich-die-geschichte-der-malware>, abgerufen am 23.07.2019
- (2) [https://de.wikipedia.org/wiki/AIDS_\(Schadprogramm\)](https://de.wikipedia.org/wiki/AIDS_(Schadprogramm)), abgerufen am 23.07.2019
- (3) <https://www.youtube.com/watch?v=5M9k7wfiWil>, abgerufen am 23.07.2019
- (4) <https://de.wikipedia.org/wiki/Locky>, abgerufen am 23.07.2019
- (5) <https://haveibeenpwned.com>, abgerufen am 23.07.2019
- (6) <https://securityaffairs.co/wordpress/53871/iot/deutsche-telekom-hack.html>, abgerufen am 23.07.2019
- (7) <https://www.computerworld.com/article/3105001/security/hackers-demonstrated-first-ransomware-for-iot-thermostats-at-def-con.html>, abgerufen am 23.07.2019
- (8) <http://www.shop.ledermode.tv/>, abgerufen am 23.07.2019
- (9) <http://metapicz.com/>, abgerufen am 23.07.2019
- (10) <http://google.de/>, abgerufen am 23.07.2019
- (11) <https://www.exploit-db.com/google-hacking-database>, abgerufen am 23.07.2019
- (12) <http://www.heise.de/security/meldung/IP-Kameras-von-Aldi-als-Sicherheits-GAU-3069735.html>, abgerufen am 23.07.2019
- (13) <https://shodan.io/>, abgerufen am 23.07.2019
- (14) <https://www.youtube.com/watch?v=WvRL5I1eU3E>, abgerufen am 23.07.2019
- (15) <http://www.spiegel.de/schulspiegel/schulfrei-in-niedersachsen-wegen-gefaelschter-e-mail-a-1071105.html>, abgerufen am 23.07.2019
- (16) <http://www.heise.de/newsticker/meldung/Gefaengnisausbruch-mittels-E-Mail-Betrug-2587303.html>, abgerufen am 23.07.2019
- (17) <https://www.wiwo.de/erfolg/management/falsche-chefs-zocken-firmen-ab-den-enkeltrick-gibts-auch-bei-unternehmen/12201572.html>, abgerufen am 23.07.2019
- (18) <http://clonezone.link/>

Quellen

- (19) <http://www.heise.de/security/meldung/00000000-Passwort-fuer-US-Atomraketen-2060077.html> , abgerufen am 23.07.2019
- (20) <http://pics-for-fun.com/wonder-what-the-code-could-be/> , abgerufen am 23.07.2019
- (21) <https://de.pinterest.com/pin/3025924727584002/> , abgerufen am 23.07.2019
- (22) <https://www.youtube.com/watch?v=opRMrEfAlil> , abgerufen am 23.07.2019
- (23) <http://www.heise.de/newsticker/meldung/Passwoerter-im-TV-Bild-Spekulationen-zu-TV5-Attacke-2598298.html> , abgerufen am 23.07.2019
- (24) https://www.vice.com/en_us/article/qvwmx5/the-agency-that-messed-up-hawaiis-nuclear-alert-keeps-passwords-on-post-its-vgtrn , abgerufen am 23.07.2019
- (25) <https://github.com/morontt/symfobruite/blob/master/adobe-top100.txt> , abgerufen am 23.07.2019
- (26) <https://xkcd.com/936/> , abgerufen am 23.07.2019
- (27) <https://arstechnica.com/information-technology/2015/08/new-data-uncovers-the-surprising-predictability-of-android-lock-patterns/> , abgerufen am 23.07.2019
- (28) <https://www.youtube.com/watch?v=WFaFL4mAzpQ> , abgerufen am 23.07.2019
- (29) <https://www.youtube.com/watch?v=RybQ3EBmkfM> , abgerufen am 23.07.2019