



**Hochschule
Albstadt-Sigmaringen**
Albstadt-Sigmaringen University

Fakultät Informatik

IT Sicherheit und Digitale Forensik
Datenschutzforum 2019

Prof. Holger Morgenstern
Tobias Scheible, M.Eng.

Prof. Holger Morgenstern



- Seit 1988 selbstständig im Bereich Hard-/Softwareentwicklung und Beratung
- Diplomstudium Informatik und Physik an der Universität Tübingen
- Seit 2002 öffentlich bestellter und vereidigter Sachverständiger für Technik, Systeme und Anwendungen der Informationsverarbeitung sowie Computerforensik
- Leitungsgremium der Fachgruppe SIDAR in der Gesellschaft für Informatik
- Seit vielen Jahren Mitorganisator und Chair der IMF und dfrws-eu
- Referee Board Member beim Journal of Digital Investigation
- Seit 2013 Professor für IT Sicherheit und praktische Informatik, Spezialgebiete Digitale Forensik, Digitale Ermittlungen, Cybersecurity
- Seit 2014 Dekan der Fakultät Informatik an der Hochschule Albstadt-Sigmaringen
- Forschung: SENTER / LIVE-FOR / GCC (ECTEG / CEPOL) / SEKT / Explainable AI / Cyberpsychology / Internationale Zusammenarbeit in den Bereichen Digitale Forensik, Cybercrime, Cybersecurity

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
 - Forschungsprojekt SEKT



IT Sicherheit und Digitale Forensik

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, ...

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 Sicherheit und Digitale Forensik

Bachelorstudiengänge

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

Masterstudiengänge

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

(auch in individueller Teilzeit möglich)

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 Sicherheit und Digitale Forensik

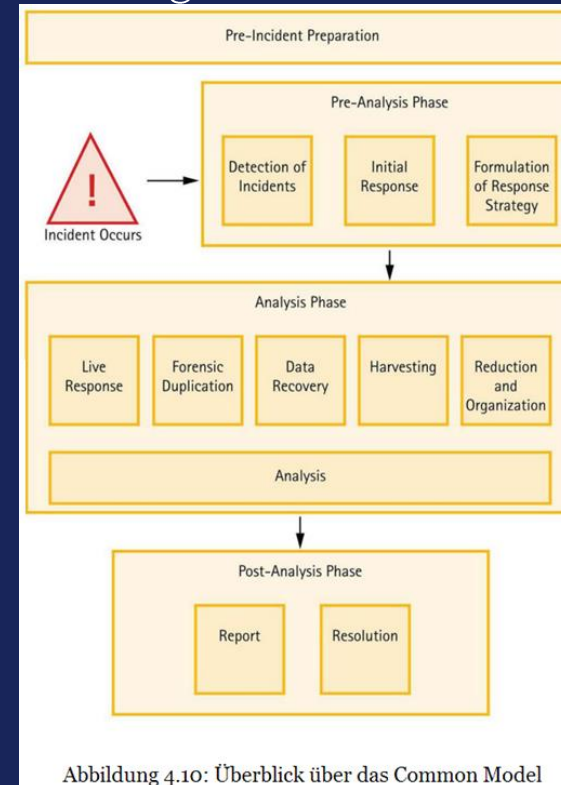
Zahlen & Fakten



Cyber Security / Digitale Forensik

- Fokus unterscheidet sich häufig
 - Cyber Security – IR: Probleme möglichst schnell beheben / abwehren / am Laufen halten
 - Digitale Forensik: Zustand einfrieren / Spuren sichern / “gerichtsfest” aufarbeiten
- Es braucht einen gemeinsamen Rahmen, ein gemeinsames Vorgehensmodell!

The Incident Response Process [Mandia et al.] The Investigative Process Model [Casey p. 102]



Kommende Herausforderungen

- Komplette Digitalisierung und Vernetzung der Welt
- Explodierende Datenmengen
- Mangelnde Kompetenz auf dem untersten Level, Hardware
- Ganz neue Datenspeicher, z.B. DNA (density >5.5 petabits/mm³)
- Künstliche Intelligenz
- Kennen wir die relevanten ethischen Fragen?

heise online › News › 06/2019 › Smart Home: Innenminister planen Zugriff auf Daten von Alexa & Co.

Smart Home: Innenminister planen Zugriff auf Daten von Alexa & Co.

Die Daten aus dem Smart Home und von digitalen Assistenten sollen als Beweismittel vor Gericht einsetzbar sein. Das planen laut einem Bericht die Innenminister.

könnten, heißt es in dem Bericht weiter. Damit die künftig bei Ermittlungen verwendet werden können, sollten nun verfassungsrechtliche Bedenken ausgeräumt werden. Künftig soll eine richterliche Zustimmung dafür ausreichen. Die Innenpolitiker erwarten demnach aber Widerstand der Datenschutzbeauftragten von Bund und Ländern. Der Plan gehe auf einen Antrag aus Schleswig-Holstein zurück, dem die Innenstaatssekretäre von Union und SPD bereits zugestimmt haben.

Agenda

- Cyber Security
 - Suchmaschinen
 - Internet of Things
 - Cybercrime as a Service
 - Live-Hack
- Social Engineering
 - Gefälschte E-Mails
 - Manipulierte Websites
 - Social Hacking
 - Versteckte Informationen
- Passwortsicherheit
 - Öffentliche Passwörter
 - Faktor Mensch
 - Angriffe auf Passwörter
 - Sichere Passwörter
- Hacking Hardware
 - Gadgets
 - Logger
 - USB
 - Funk
 - Netzwerk



Cyber Security

IT Sicherheit und Digitale Forensik

Cyber Security

- Suchmaschinen
- Internet of Things
- Cybercrime as a Service
- Live-Hack

Social Engineering

Passwortsicherheit

Hacking Hardware

00000000



00000000

Launch-Code für die in den USA stationierten Atomraketen

(1962 bis 1977)

Atomraketen: Steuerungstechnik aus den 70ern



IT Sicherheit und Digitale Forensik

Cyber Security

- Suchmaschinen
- Internet of Things
- Cybercrime as a Service
- Live-Hack

Social Engineering

Passwortsicherheit

Hacking Hardware

Suchmaschinen - Hacking mit Google



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>

IT Sicherheit und Digitale Forensik

Cyber Security

[Suchmaschinen](#)

Internet of Things

Cybercrime as a Service

Live-Hack

Social Engineering

Passwortsicherheit

Hacking Hardware

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"`

IT Sicherheit und Digitale Forensik

Cyber Security

[Suchmaschinen](#)

Internet of Things

Cybercrime as a Service

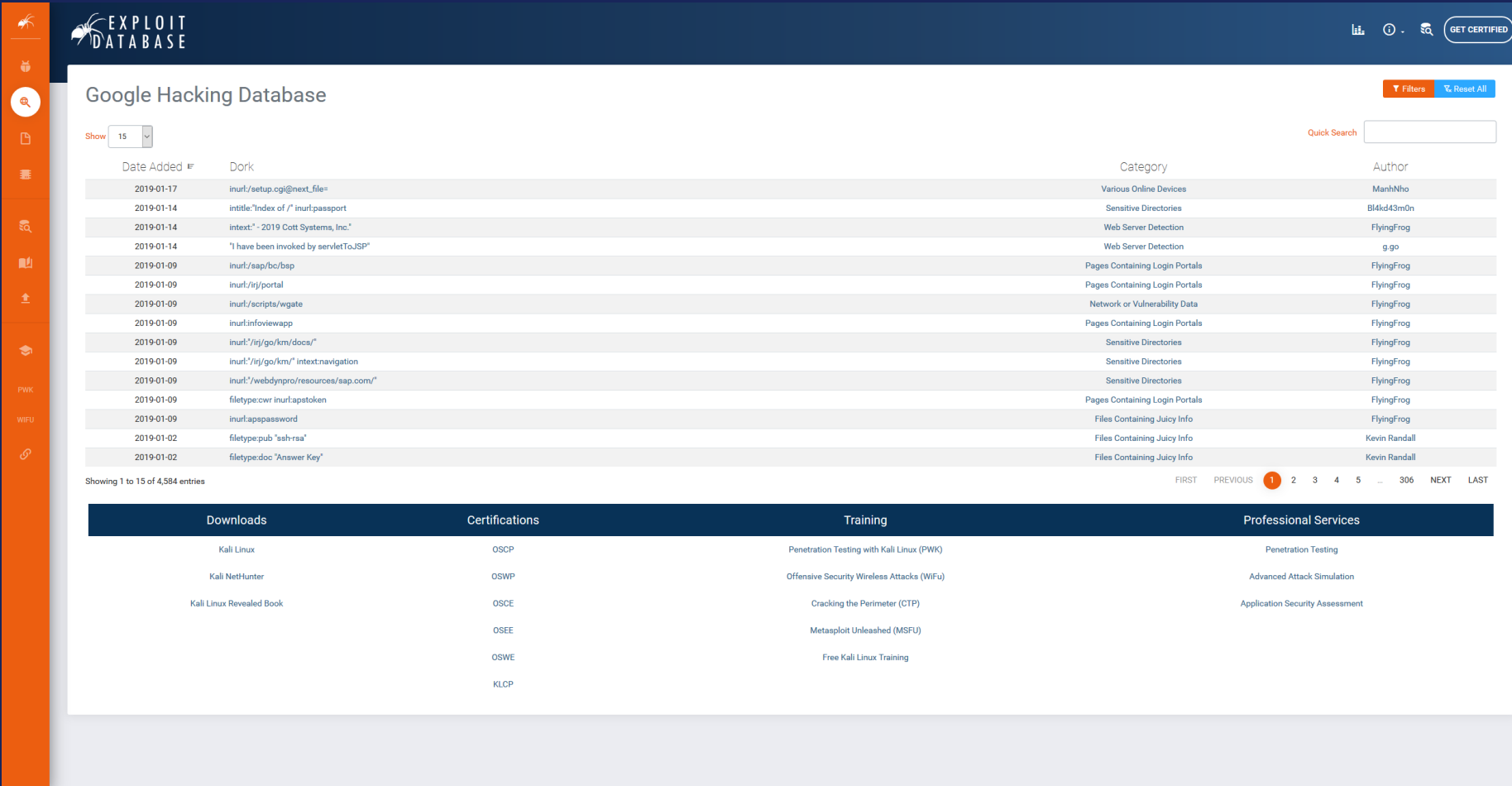
Live-Hack

Social Engineering

Passwortsicherheit

Hacking Hardware

Suchmaschinen - GHDB



EXPLOIT DATABASE

Google Hacking Database

Show 15 Filters

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	g.go
2019-01-09	inurl:/aap/bc/bap	Pages Containing Login Portals	FlyingFrog
2019-01-09	inurl:/rij/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:/rij/go/km/docs/"	Sensitive Directories	FlyingFrog
2019-01-09	inurl:/rij/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:apspassword	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	OSCP	Penetration Testing with Kali Linux (PWK)	Penetration Testing
Kali NetHunter	OSWP	Offensive Security Wireless Attacks (WIFu)	Advanced Attack Simulation
Kali Linux Revealed Book	OSCE	Cracking the Perimeter (CTP)	Application Security Assessment
	OSEE	Metasploit Unleashed (MSFU)	
	OSWE	Free Kali Linux Training	
	KLCP		

IT Sicherheit und Digitale Forensik

Cyber Security

[Suchmaschinen](#)

[Internet of Things](#)

[Cybercrime as a Service](#)

[Live-Hack](#)

Social Engineering

[Passwortsicherheit](#)

[Hacking Hardware](#)


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

IT Sicherheit und Digitale Forensik

Cyber Security

[Suchmaschinen](#)

[Internet of Things](#)

[Cybercrime as a Service](#)

[Live-Hack](#)

Social Engineering

[Passwortsicherheit](#)

[Hacking Hardware](#)

DEMO IoT – Shodan Suche



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', 'Developer Pricing', and 'Enterprise Access'. A green button for 'Login or Register' is on the right. The main heading reads 'The search engine for Security' and 'Shodan is the world's first search engine for Internet-connected devices.' Below this are two buttons: 'Create a Free Account' and 'Getting Started'. The page is divided into four sections with icons: 'Explore the Internet of Things' (cloud icon), 'Monitor Network Security' (eye icon), 'See the Big Picture' (globe icon), and 'Get a Competitive Advantage' (document icon). A blue banner below these sections states '56% of Fortune 100' and '1,000+ Universities' are using Shodan. The next section, 'Analyze the Internet in Seconds', features a world map and a 'Sample Report on Heartbleed' button. The final section, 'Beyond the Web', mentions a public API and shows icons for Chrome and Firefox.

IT Sicherheit und Digitale Forensik

Cyber Security

Suchmaschinen

[Internet of Things](#)

Cybercrime as a Service

Live-Hack

Social Engineering

Passwortsicherheit

Hacking Hardware

Cybercrime as a Service

IT Sicherheit und Digitale Forensik

Cyber Security

Suchmaschinen

Internet of Things

Cybercrime as a Service

Live-Hack

Social Engineering

Passwortsicherheit

Hacking Hardware



Quelle: [youtube.com](#) (7)

06.06.2019 | Datenschutzforum 2019

Prof. Holger Morgenstern
Tobias Scheible, M.Eng.

Cybercrime as a Service



Koordinator

IT Sicherheit und Digitale Forensik

Cyber Security

Suchmaschinen

Internet of Things

Cybercrime as a Service

Live-Hack

Social Engineering

Passwortsicherheit

Hacking Hardware

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)

IT Sicherheit und Digitale Forensik

Cyber Security

Suchmaschinen

Internet of Things

Cybercrime as a Service

Live-Hack

Social Engineering

Passwortsicherheit

Hacking Hardware

DEMO Live-Hack

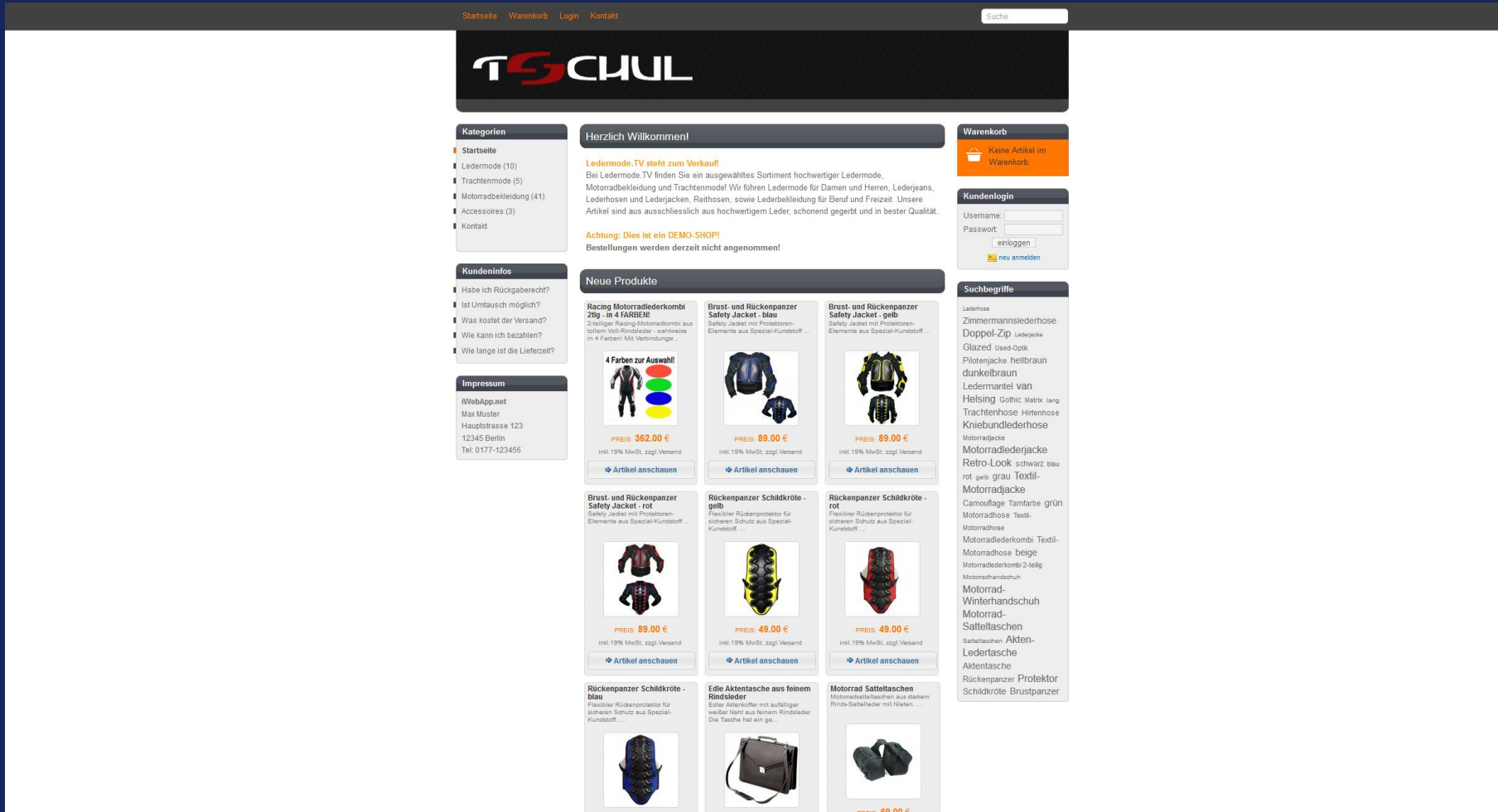
IT Sicherheit und Digitale Forensik

Cyber Security
Suchmaschinen
Internet of Things
Cybercrime as a Service
Live-Hack

Social Engineering

Passwortsicherheit

Hacking Hardware



The screenshot shows the homepage of the website ledermode.tv. The top navigation bar includes links for 'Startseite', 'Warenkorb', 'Login', and 'Kontakt', along with a search bar. The main content area is divided into several sections:

- Kategorien:** A list of product categories including 'Startseite', 'Ledermode (10)', 'Trachtenmode (5)', 'Motorradbekleidung (41)', 'Accessoires (3)', and 'Kontakt'.
- Kundeninfos:** A section with questions like 'Habe ich Rückgaberecht?', 'Ist Umtausch möglich?', 'Was kostet der Versand?', 'Wie kann ich bezahlen?', and 'Wie lange ist die Lieferzeit?'.
- Impressum:** Contact information for 'WebApp.net', including 'Max Muster', 'Hauptstrasse 123', '12345 Berlin', and 'Tel: 0177-123456'.
- Herzlich Willkommen:** A welcome message and a promotional banner for 'Ledermode.TV steht zum Verkauf!'.
- Neue Produkte:** A grid of featured products, each with an image, title, price, and a 'Artikel anschauen' button. Products include:
 - Racing Motorradlederkombi ZIG - in 4 FARBEN!
 - Brust- und Rückenpanzer Safety Jacket - blau
 - Brust- und Rückenpanzer Safety Jacket - gelb
 - 4 Farben zur Auswahl
 - Brust- und Rückenpanzer Safety Jacket - rot
 - Rückenpanzer Schildkröte - gelb
 - Rückenpanzer Schildkröte - rot
 - Rückenpanzer Schildkröte - blau
 - Edle Akteeltasche aus feinem Rindsleder
 - Motorrad Satteltaschen
- Warenkorb:** A section indicating 'Keine Artikel im Warenkorb'.
- Kundenlogin:** A login form with fields for 'Username:' and 'Passwort:', and buttons for 'enloggen' and 'neu anmelden'.
- Suchbegriffe:** A list of search terms related to motorcycle gear, such as 'Lederhose', 'Zimmermannslederhose', 'Doppel-Zip', 'Glazed Used-Optik', 'Pilotenjacke', 'Ledermantel van Helsing', 'Trachtenhose', 'Kniebündlerhose', 'Motorradjacke', 'Motorradlederjacke', 'Retro-Look', 'Motorradjacke', 'Camouflage', 'Motorradhose', 'Motorradlederkombi', 'Motorradhose', 'Motorradlederkombi', 'Motorradhandschuh', 'Motorrad-Winterhandschuh', 'Motorrad-Satteltaschen', 'Satteltaschen', 'Akten-Ledertasche', 'Akteeltasche', 'Rückenpanzer Protetektor', and 'Schildkröte Brustpanzer'.

A person wearing a glowing yellow mask with a skull-like pattern, holding a large playing card (Ace of Clubs) in a dark, neon-lit environment with falling cards and a blue light arch.

Social Engineering

Was ist die häufigste Angriffsmethode?

Ausnutzung von Schwachstellen

A

Physische Attacken

B

Manipulation von Personen

C

Ausnutzung von Fehlern

D

IT Sicherheit und Digitale Forensik

Gefälschte E-Mails

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) (10)

IT Sicherheit und Digitale Forensik

Cyber Security

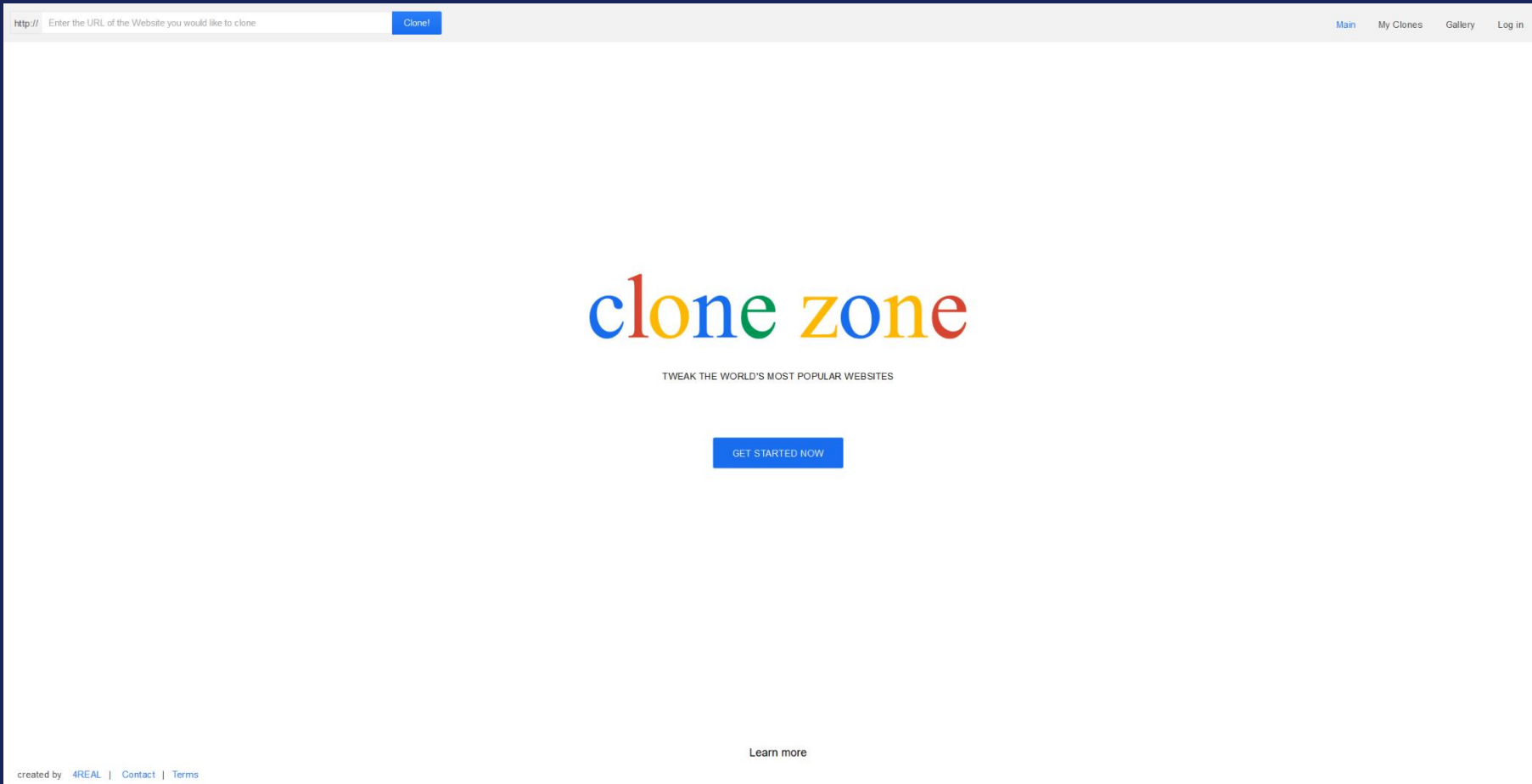
Social Engineering

- [Gefälschte E-Mails](#)
- [Manipulierte Websites](#)
- [Social Hacking](#)
- [Versteckte Informationen](#)

Passwortsicherheit

Hacking Hardware

DEMO Manipulierte Websites



The screenshot shows the homepage of the Clone Zone website. 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 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 is the tagline "TWEAK THE WORLD'S MOST POPULAR WEBSITES" and a prominent blue "GET STARTED NOW" button. At the bottom left, there is a footer with the text "created by 4REAL | Contact | Terms". At the bottom center, there is a "Learn more" link.

IT Sicherheit und Digitale Forensik

Cyber Security

Social Engineering

Gefälschte E-Mails

[Manipulierte Websites](#)

Social Hacking

Versteckte Informationen

Passwortsicherheit

Hacking Hardware

Manipulierte Websites



IT Sicherheit und Digitale Forensik

Cyber Security

Social Engineering

Gefälschte E-Mails

Manipulierte Websites

Social Hacking

Versteckte Informationen

Passwortsicherheit

Hacking Hardware

Social Hacking - 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 Sicherheit und Digitale Forensik

Cyber Security

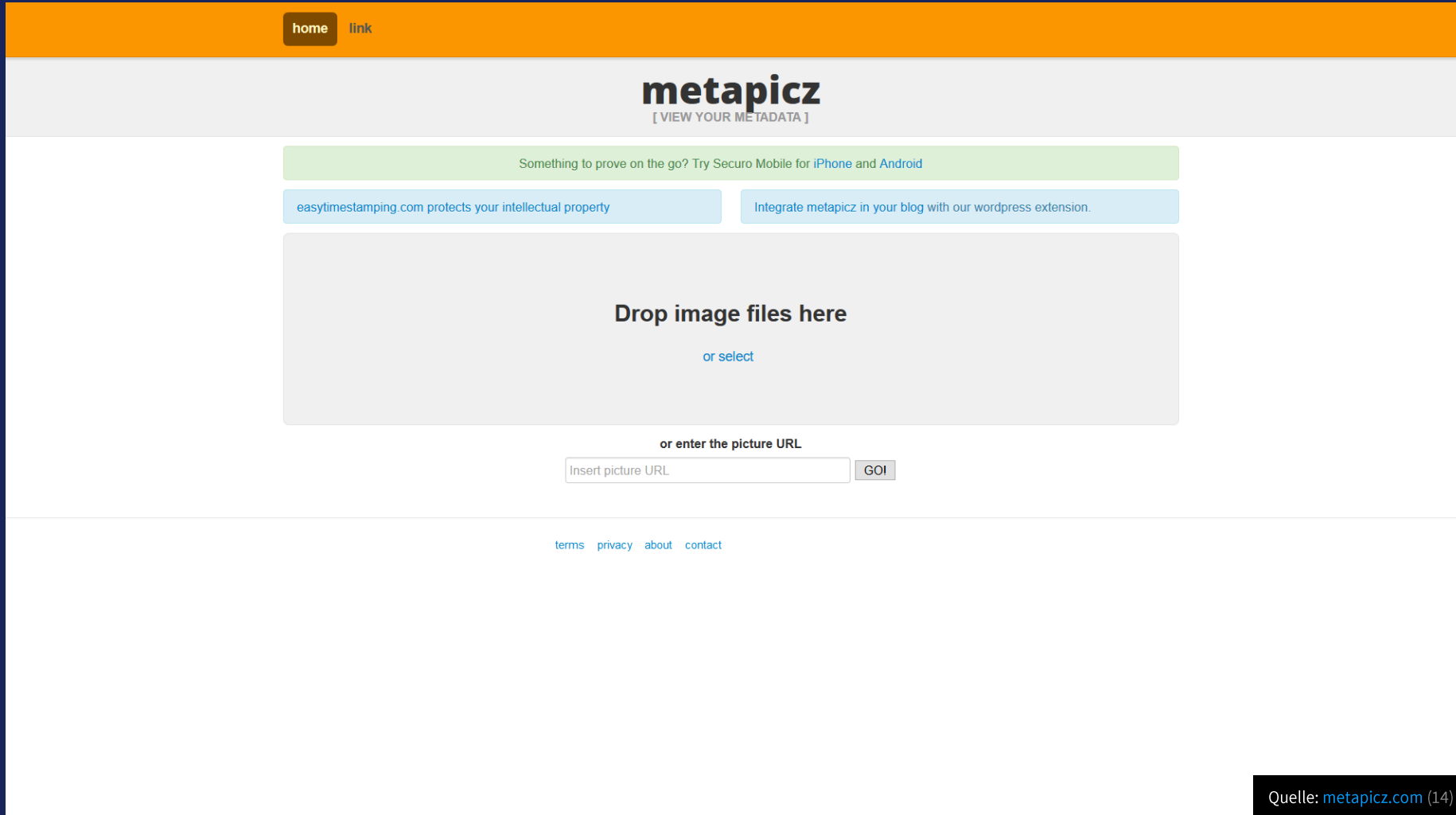
Social Engineering

- Gefälschte E-Mails
- Manipulierte Websites
- Social Hacking
- Versteckte Informationen

Passwortsicherheit

Hacking Hardware

DEMO 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 the tagline '[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: '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 'or select' below it. Below this box is a form with the label 'or enter the picture URL', 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 small black box in the bottom right corner of the screenshot contains the text 'Quelle: metapicz.com (14)'.

IT Sicherheit und Digitale Forensik

Cyber Security

Social Engineering

Gefälschte E-Mails

Manipulierte Websites

Social Hacking

Versteckte Informationen

Passwortsicherheit

Hacking Hardware

Quelle: metapicz.com (14)

06.06.2019 | Datenschutzforum 2019

Prof. Holger Morgenstern
Tobias Scheible, M.Eng.

A person wearing a dark hoodie and a glowing orange mask with a stitched mouth and X-shaped eyes. A glowing blue circle is visible on the front of the hoodie. The background is a city at night with bokeh lights and a railing.

Passwortsicherheit

Öffentliche Passwörter

I wonder what the code could be...



Quelle: pics-for-fun.com (15)



Quelle: de.pinterest.com (16)

IT Sicherheit und Digitale Forensik

Cyber Security

Social Engineering

Passwortsicherheit

[Öffentliche Passwörter](#)

Faktor Mensch

Angriffe auf Passwörter

Sichere Passwörter

Hacking Hardware

06.06.2019 | Datenschutzforum 2019

Prof. Holger Morgenstern
Tobias Scheible, M.Eng.

Öffentliche Passwörter - Interview



Quelle: youtube.com (17)

IT Sicherheit und Digitale Forensik

Cyber Security

Social Engineering

Passwortsicherheit

Öffentliche Passwörter

Faktor Mensch

Angriffe auf Passwörter

Sichere Passwörter

Hacking Hardware

06.06.2019 | Datenschutzforum 2019

Prof. Holger Morgenstern
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

IT Sicherheit und Digitale Forensik

Cyber Security

Social Engineering

Passwortsicherheit

Öffentliche Passwörter

Faktor Mensch

Angriffe auf Passwörter

Sichere Passwörter

Hacking Hardware

Faktor Mensch - Angriff auf TV5 Monde



IT Sicherheit und Digitale Forensik

Cyber Security

Social Engineering

Passwortsicherheit

Öffentliche Passwörter

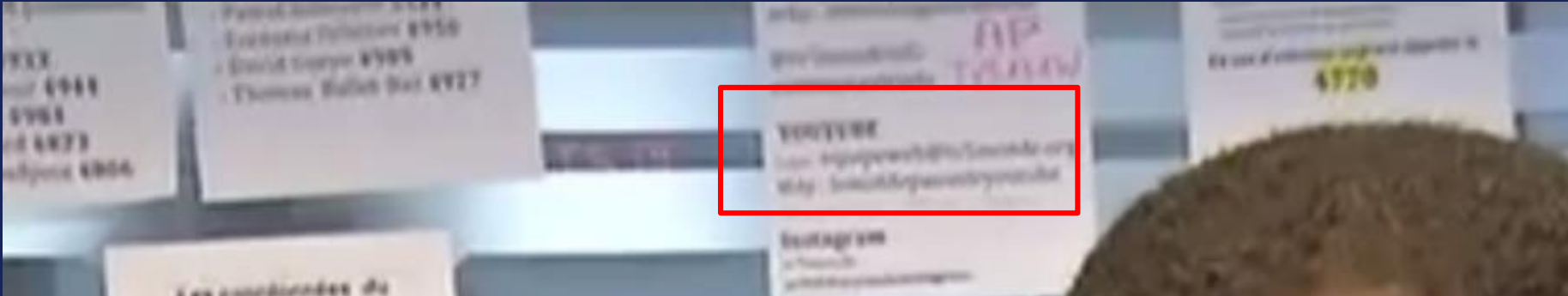
Faktor Mensch

Angriffe auf Passwörter

Sichere Passwörter

Hacking Hardware

Faktor Mensch - Angriff auf TV5 Monde



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



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

IT Sicherheit und Digitale Forensik

Cyber Security

Social Engineering

Passwortsicherheit

Öffentliche Passwörter

[Faktor Mensch](#)

Angriffe auf Passwörter

Sichere Passwörter

Hacking Hardware

Faktor Mensch



Quelle: [vice.com](https://www.vice.com) (19)

IT Sicherheit und Digitale Forensik

Cyber Security

Social Engineering

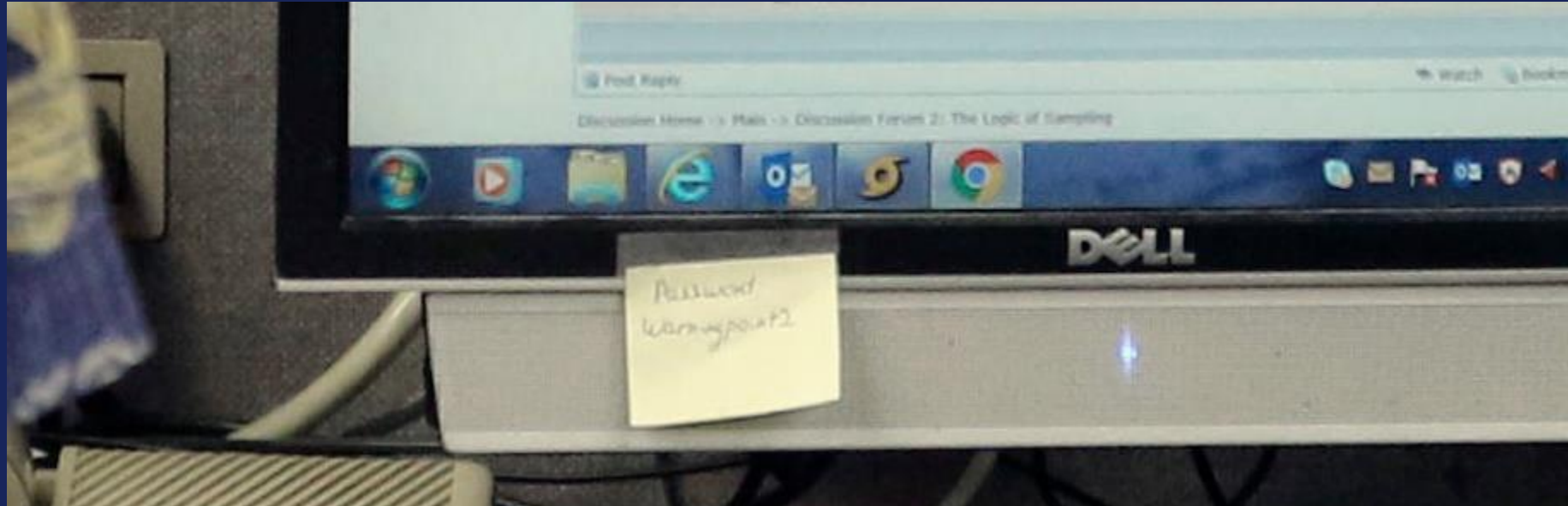
Passwortsicherheit
Öffentliche Passwörter
Faktor Mensch
Angriffe auf Passwörter
Sichere Passwörter

Hacking Hardware

06.06.2019 | Datenschutzforum 2019

Prof. Holger Morgenstern
Tobias Scheible, M.Eng.

Faktor Mensch



Klassiker – Post-it Zettel auf Monitor
Passwort: warningpoint2

Quelle: [vice.com](https://www.vice.com) (19)

IT Sicherheit und Digitale Forensik

Cyber Security

Social Engineering

Passwortsicherheit

Öffentliche Passwörter

[Faktor Mensch](#)

Angriffe auf Passwörter

Sichere Passwörter

Hacking Hardware

06.06.2019 | Datenschutzforum 2019

Prof. Holger Morgenstern
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.

IT Sicherheit und Digitale Forensik

Cyber Security

Social Engineering

Passwortsicherheit

Öffentliche Passwörter

Faktor Mensch

[Angriffe auf Passwörter](#)

Sichere Passwörter

Hacking Hardware

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 Sicherheit und Digitale Forensik

Cyber Security

Social Engineering

Passwortsicherheit

Öffentliche Passwörter

Faktor Mensch

[Angriffe auf Passwörter](#)

Sichere Passwörter

Hacking Hardware

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 (20)

IT Sicherheit und Digitale Forensik

Cyber Security

Social Engineering

Passwortsicherheit

Öffentliche Passwörter

Faktor Mensch

[Angriffe auf Passwörter](#)

Sichere Passwörter

Hacking Hardware

06.06.2019 | Datenschutzforum 2019

Prof. Holger Morgenstern
Tobias Scheible, M.Eng.

Sichere Passwörter

- Möglichst lange Passwörter verwenden
- 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, ...)

IT Sicherheit und Digitale Forensik

Cyber Security

Social Engineering

Passwortsicherheit

Öffentliche Passwörter

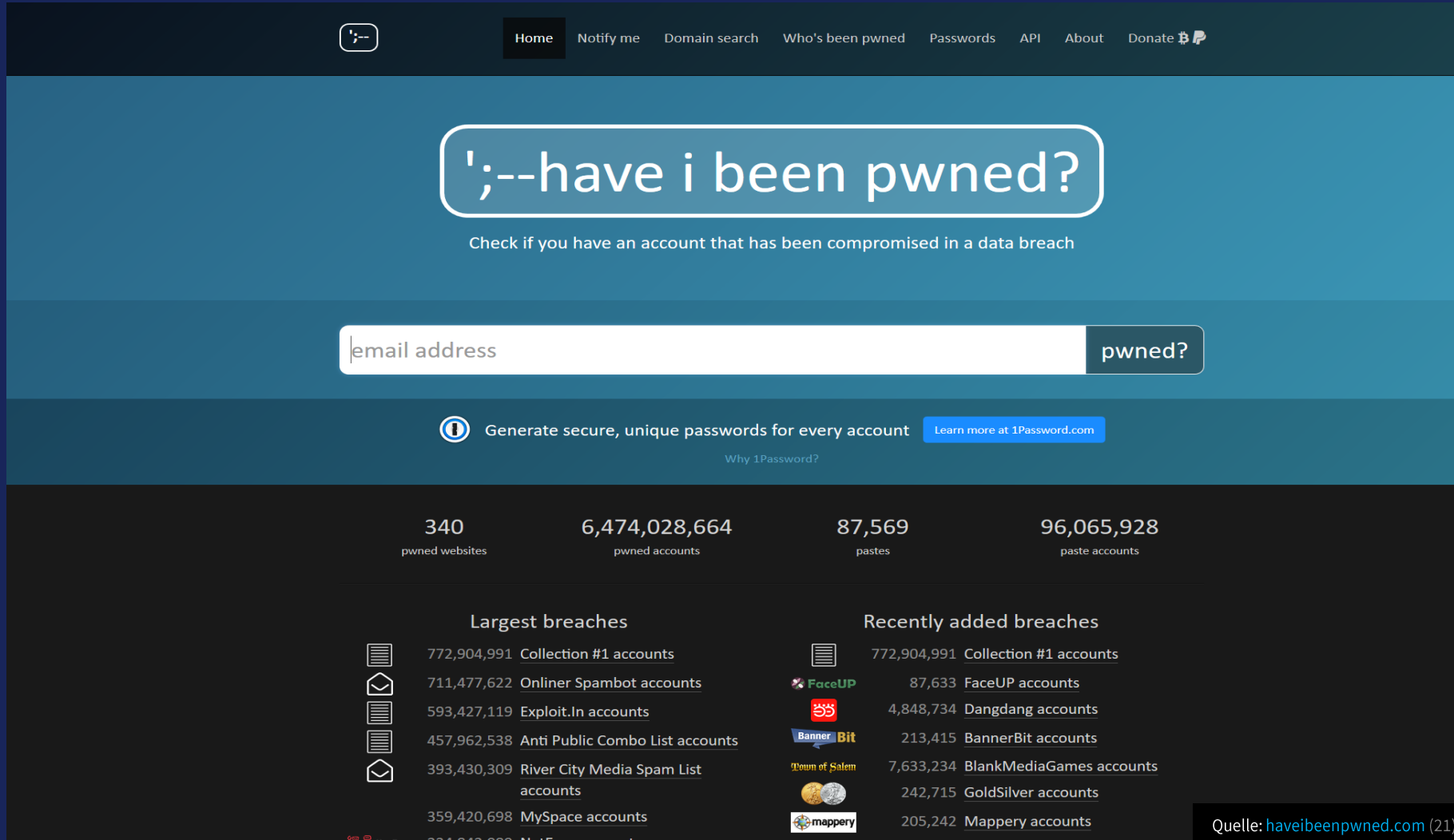
Faktor Mensch

Angriffe auf Passwörter

Sichere Passwörter

Hacking Hardware

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

email address pwned?

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

Why 1Password?

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

Largest breaches

772,904,991	Collection #1 accounts
711,477,622	Onliner Spambot accounts
593,427,119	Exploit.In accounts
457,962,538	Anti Public Combo List accounts
393,430,309	River City Media Spam List accounts
359,420,698	MySpace accounts
234,842,089	NetEase accounts

Recently added breaches

772,904,991	Collection #1 accounts
87,633	FaceUP accounts
4,848,734	Dangdang accounts
213,415	BannerBit accounts
7,633,234	BlankMediaGames accounts
242,715	GoldSilver accounts
205,242	Mappery accounts

Quelle: haveibeenpwned.com (21)

IT Sicherheit und Digitale Forensik

Cyber Security

Social Engineering

Passwortsicherheit

Öffentliche Passwörter

Faktor Mensch

Angriffe auf Passwörter

[Sichere Passwörter](#)

Hacking Hardware



Hacking Hardware

Gadgets – Spionage Kamera



Gadgets – GSM Wanze



Logger - Keylogger



Logger - Screenlogger



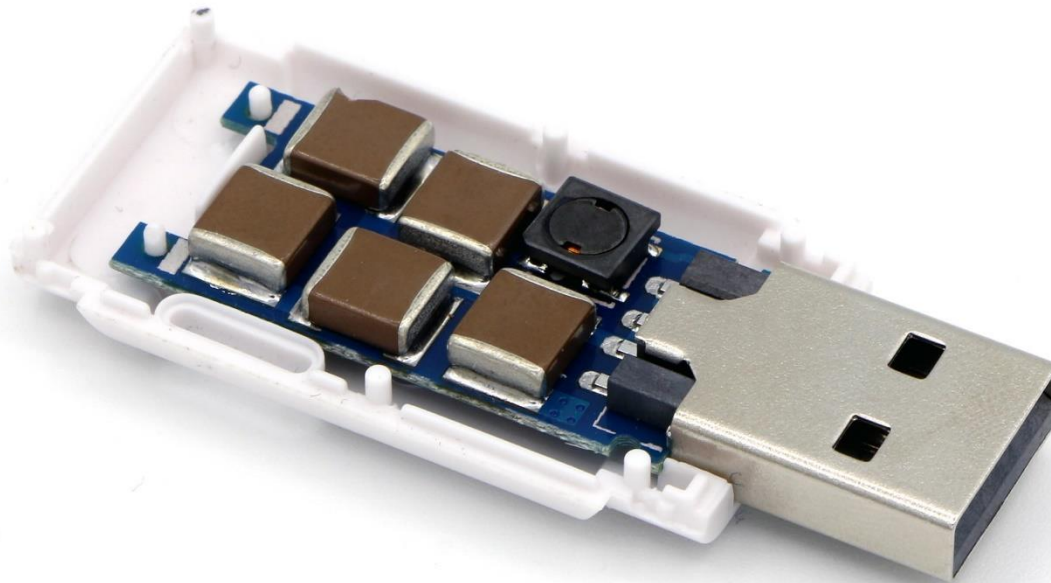
USB – BadUSB (Rubber Ducky)



USB – BadUSB (USBNinja)



USB - USBKill



Funk - Störsender

IT Sicherheit und Digitale Forensik

Cyber Security

Social Engineering

Passwortsicherheit

Hacking Hardware

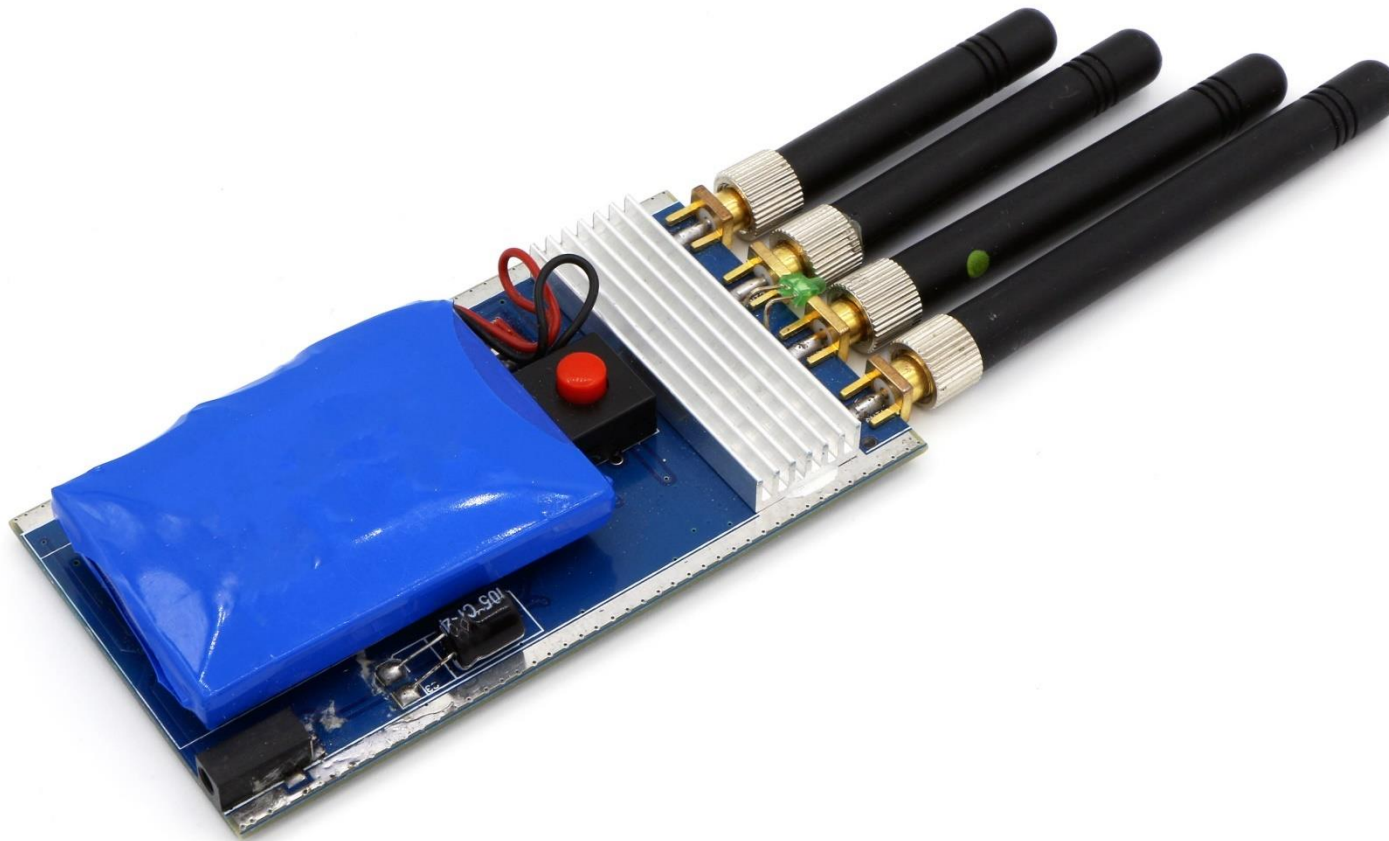
Gadgets

Logger

USB

Funk

Netzwerk



Funk - Software Defined Radio



Netzwerk – WiFi Deauther

IT Sicherheit und Digitale Forensik

Cyber Security

Social Engineering

Passwortsicherheit

Hacking Hardware

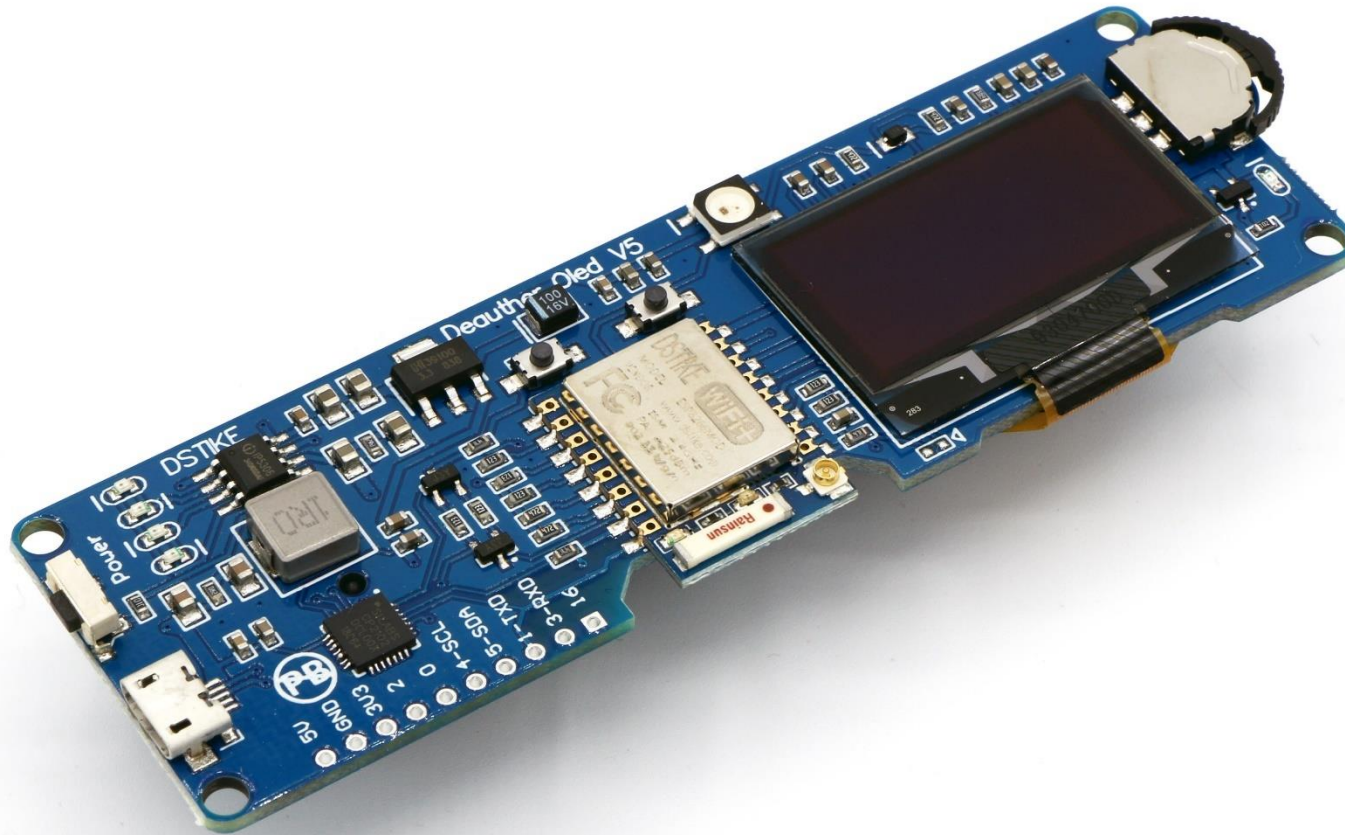
Gadgets

Logger

USB

Funk

Netzwerk



Netzwerk - Packet-Squirrel

IT Sicherheit und Digitale Forensik

Cyber Security

Social Engineering

Passwortsicherheit

Hacking Hardware

Gadgets

Logger

USB

Funk

Netzwerk



Vielen Dank für Ihre Aufmerksamkeit



Noch Fragen?

Quellen

- 1) 00000000: Passwort für US-Atomraketen, <http://www.heise.de/security/meldung/00000000-Passwort-fuer-US-Atomraketen-2060077.html>, abgerufen am 05.06.2019
- 2) Mit Floppy Disks Atombomben überwachen, <http://www.zeit.de/politik/ausland/2016-05/us-militaer-pcs-technologie-veraltet-rechnungshof>, abgerufen am 05.06.2019
- 3) Google, <https://google.de>, abgerufen am 05.06.2019
- 4) Google Hacking Database, <https://www.exploit-db.com/google-hacking-database>, abgerufen am 05.06.2019
- 5) IP-Kameras von Aldi als Sicherheits-GAU, <http://www.heise.de/security/meldung/IP-Kameras-von-Aldi-als-Sicherheits-GAU-3069735.html>, abgerufen am 05.06.2019
- 6) Shodan, <https://www.shodan.io>, abgerufen am 05.06.2019
- 7) Anuncio - gwapo's, <https://www.youtube.com/watch?v=5M9k7wfiWil>, abgerufen am 05.06.2019
- 8) Locky, <https://de.wikipedia.org/wiki/Locky>, abgerufen am 05.06.2019
- 9) iWebapp, <http://www.shop.ledermode.tv>, abgerufen am 05.06.2019
- 10) Gefälschte E-Mail - Schulfrei ermogelt, <http://www.spiegel.de/schulspiegel/schulfrei-in-niedersachsen-wegen-gefaelschter-e-mail-a-1071105.html>, abgerufen am 05.06.2019
- 11) Clone Zone, <http://clonezone.link>, abgerufen am 05.06.2019
- 12) Legisdigit@ - Groupe Mutuel Versicherungen - <https://www.youtube.com/watch?v=WvRL5I1eU3E>, abgerufen am 05.06.2019
- 13) Gefängnisausbruch mittels E-Mail-Betrug, <http://www.heise.de/newsticker/meldung/Gefaengnisausbruch-mittels-E-Mail-Betrug-2587303.html>, abgerufen am 05.06.2019
- 14) online metadata and exif viewer, <http://metapicz.com>, abgerufen am 05.06.2019

Quellen

- 15) Code, <http://pics-for-fun.com/wonder-what-the-code-could-be/>, abgerufen am 05.06.2019
- 16) And the valuables are in the closet on the top shelf in a box marked, <https://de.pinterest.com/pin/3025924727584002/>, abgerufen am 05.06.2019
- 17) What is Your Password?, <https://www.youtube.com/watch?v=opRMrEfAlil>, abgerufen am 05.06.2019
- 18) 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 05.06.2019
- 19) The Agency That Messed Up Hawaii's Nuclear Alert Keeps Passwords on Post-Its, https://www.vice.com/en_us/article/qvwmx5/the-agency-that-messed-up-hawaiis-nuclear-alert-keeps-passwords-on-post-its-vgtrn, abgerufen am 05.06.2019
- 20) Top 100 Adobe Passwords with Count, <https://github.com/morontt/symfobroute/blob/master/adobe-top100.txt>, abgerufen am 05.06.2019
- 21) Have I Been Pwned: Check if your email has been compromised in a data breach, <https://haveibeenpwned.com>, abgerufen am 05.06.2019