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 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
- 1988/89 Campus Albstadt
- 2004 Fachhochschule wird in Hochschule umbenannt
- 24 Bachelor- und Masterstudiengänge

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

Fakultät Informatik

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

Zahlen & Fakten

167
Lehrbe-
auftragte

201
Mitarbeiter

57 %
Campus
Albstadt

43 %
Campus
Sigmaringen

67
Verwaltung
und zentrale
Einrichtungen

134
Mitarbeiter
Studiengänge

3.374
Studierende

184
Studentische
Hilfskräfte

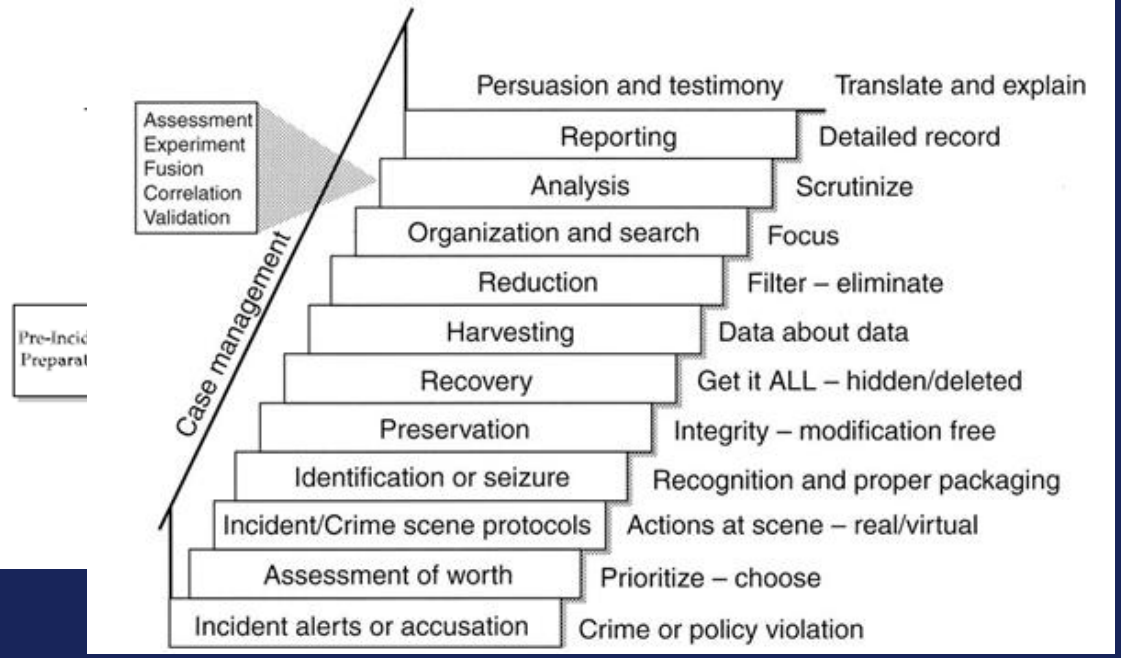
87
Professoren /
Professorinnen

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 Vorgehensmodel!

The Incident Response Process [Mandia et al.]

The Investigative Process Model [Casey p. 102]



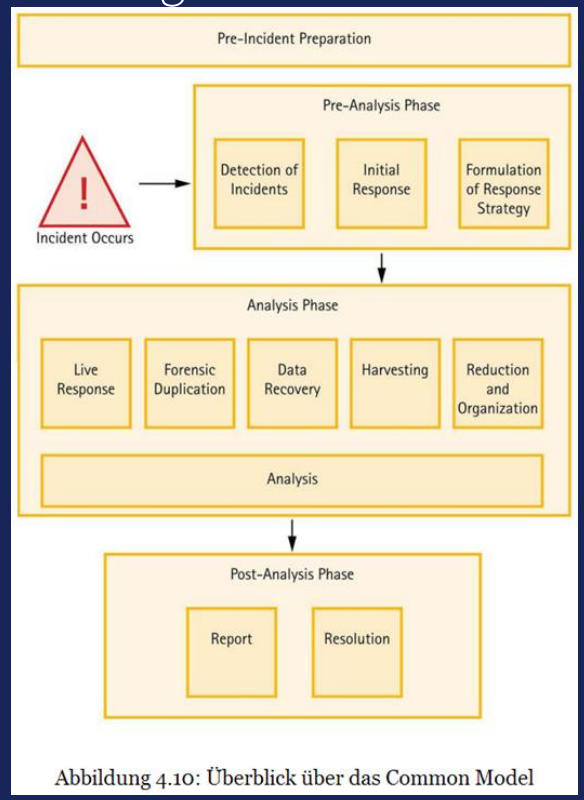


Abbildung 4.10: Überblick über das Common Model

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/mm^3)
- 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

000000000

?

Quelle: heise.de (1)

00000000

Launch-Code für die in den USA stationierten Atomraketen

(1962 bis 1977)

Quelle: heise.de (1)

Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Fakultät Informatik

Atomraketen: Steuerungstechnik aus den 70ern

Quelle: zeit.de (2)

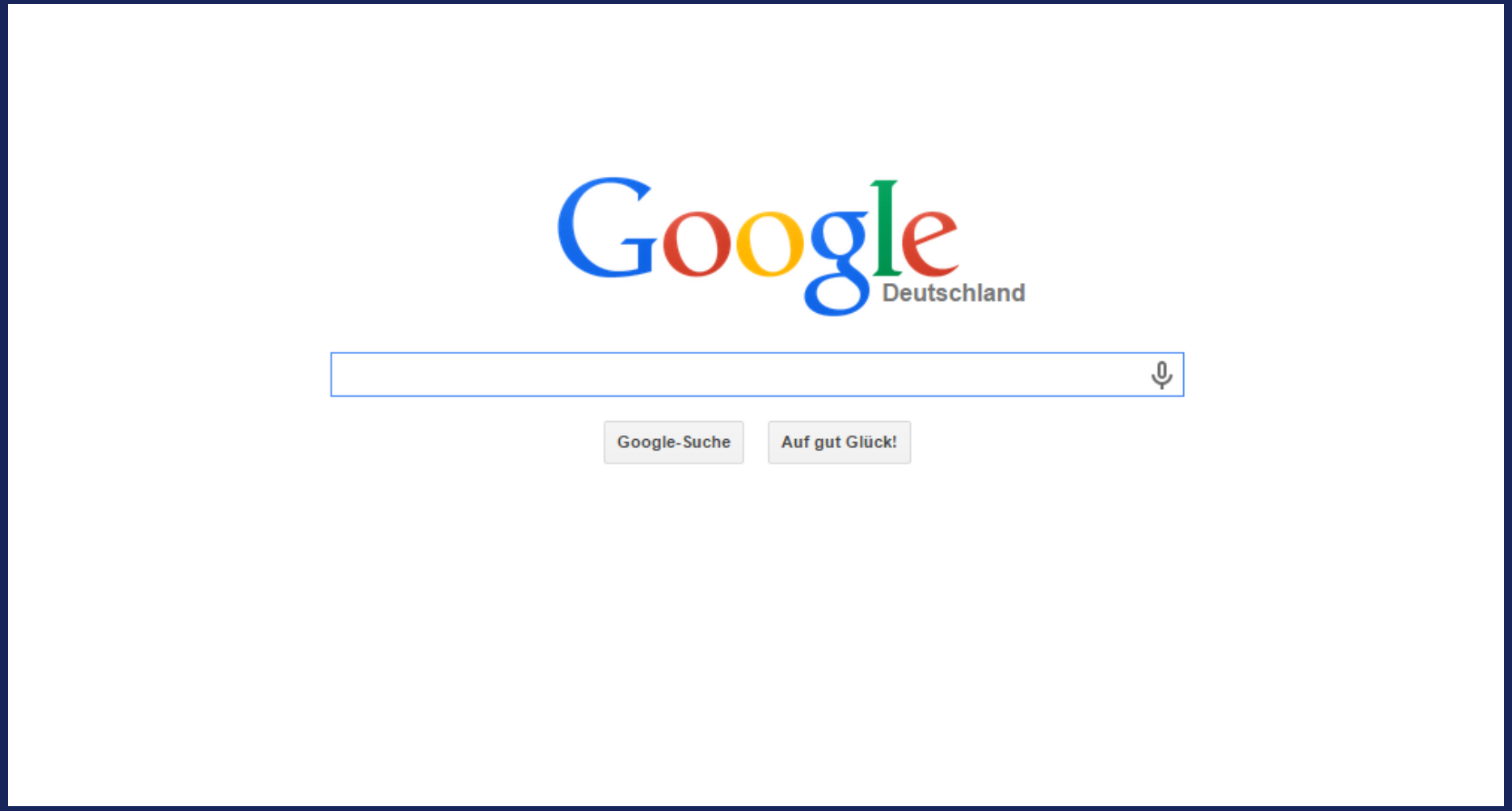
Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Fakultät Informatik

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



Quelle: google.de (3)

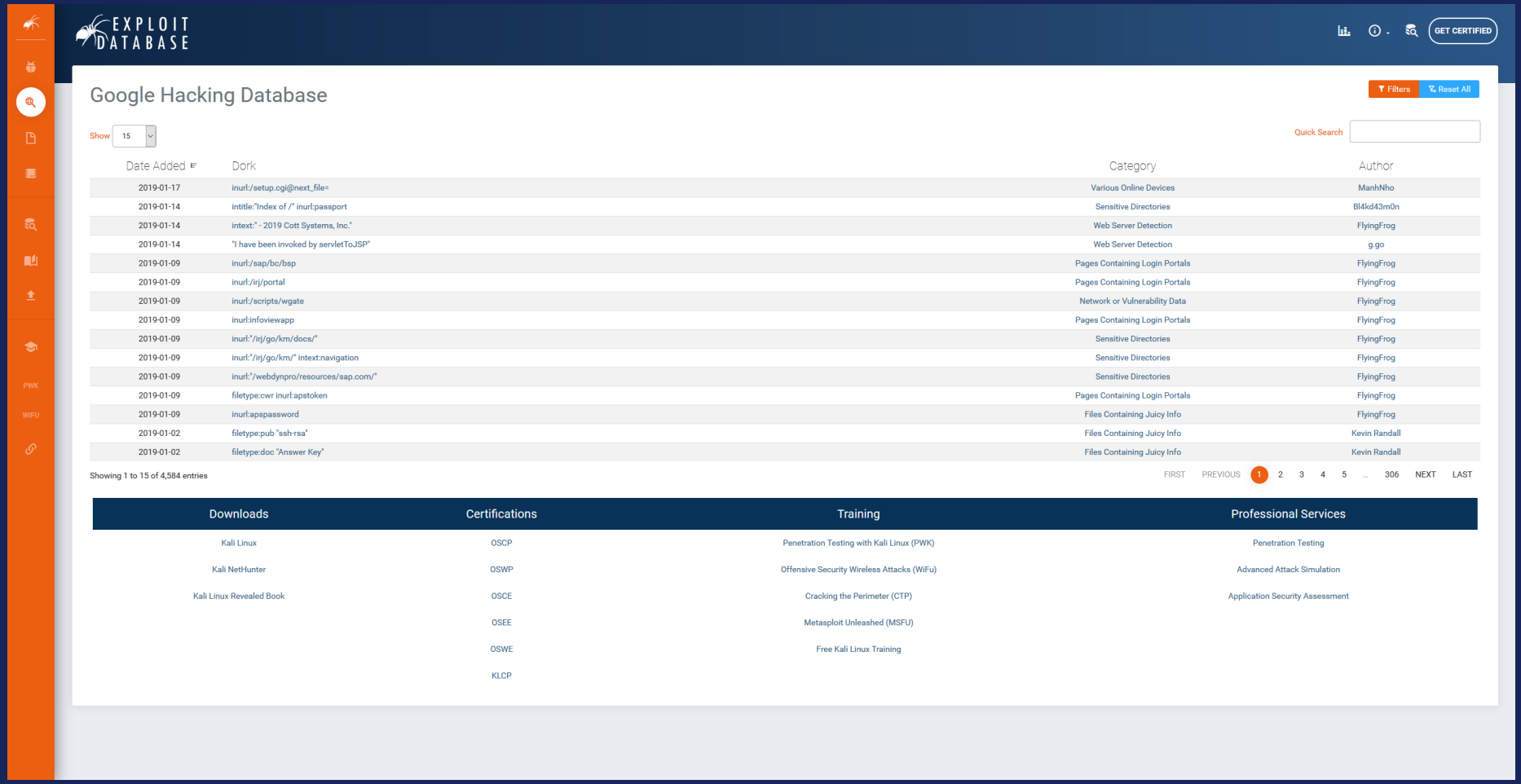
Suchmaschinen - Hacking mit Google

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: *it security site:hs-albsig.de*
intitle:	Eine Suche mit dem Suchparameter "intitle" in Verbindung mit einem Suchbegriff liefert Ergebnisse von Webseiten, deren Titel diesen Suchbegriff enthält. Beispiel: *intitle:"it security"*
inurl:	Eine Suche mit dem Suchparameter "inurl:" in Verbindung mit einem Suchbegriff liefert Ergebnisse von Webseiten, deren URL den Suchbegriff enthalten. Beispiel: *inurl:"it-security"*
intext:	Mit dem Suchparameter "intext" in Verbindung mit einem Suchbegriff werden Webseiten angezeigt, in denen der Begriff im Text der Seite vorkommt. Beispiel: *intext:"it security bachelor"*

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"

Suchmaschinen - GHDB



Quelle: exploit-db.com (4)

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

Quelle: heise.de (5)

DEMO IoT – Shodan Suche

Quelle: shodan.io (6)

Cybercrime as a Service

Quelle: youtube.com (7)

Cybercrime as a Service

Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Fakultät Informatik

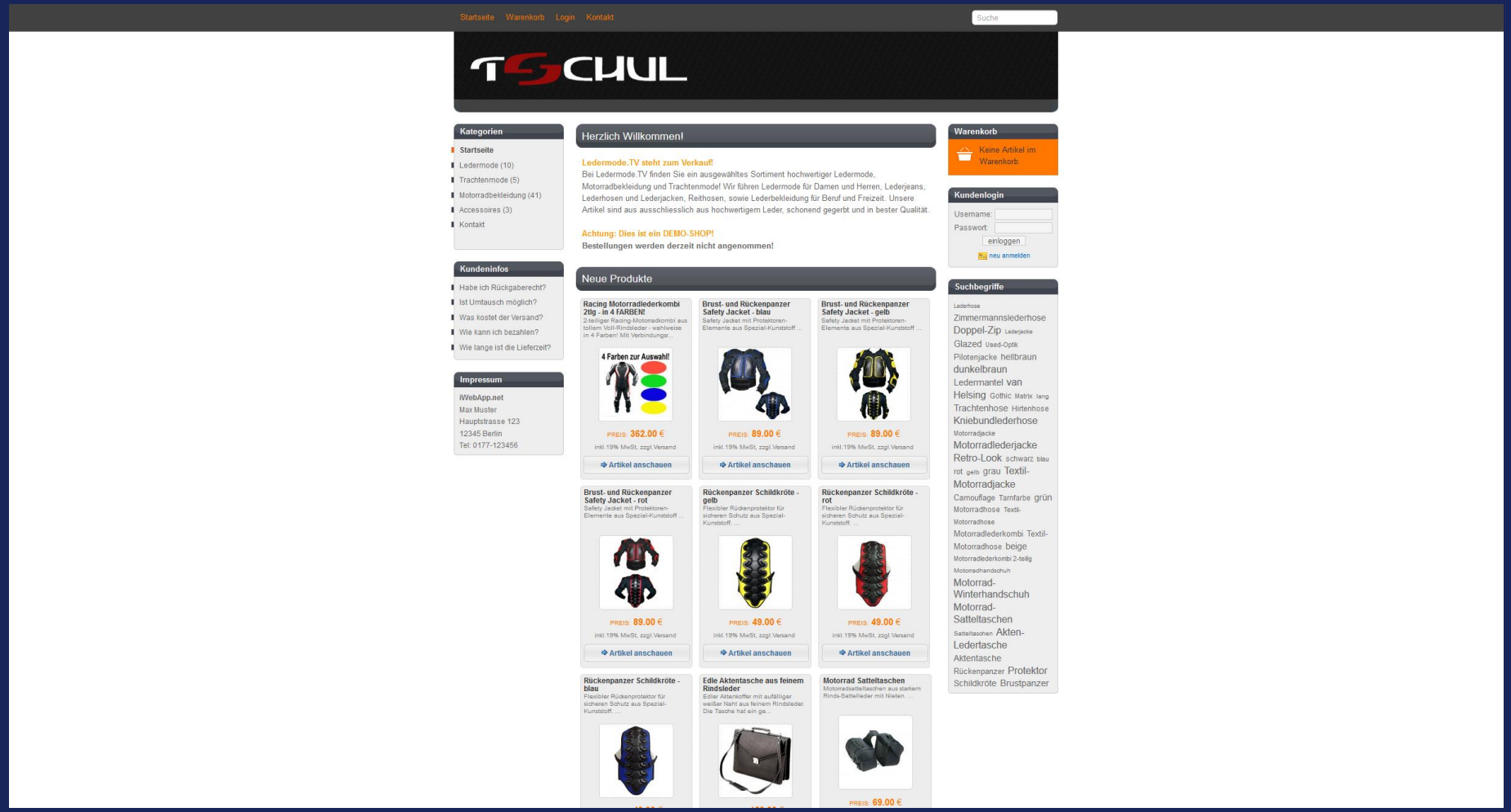
Cybercrime as a Service - Ransomware Locky

- 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)

Quelle: wikipedia.org (8)

DEMO Live-Hack



Quelle: ledermode.tv (9)

Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Fakultät Informatik

IT Sicherheit und Digitale Forensik

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

Social Engineering

Passwortsicherheit

Hacking Hardware

Social Engineering

Was ist die häufigste Angriffsmethode?

Ausnutzung von Schwachstellen

A

Physische Attacken

B

Manipulation von Personen

C

Ausnutzung von Fehlern

D

Gefälschte E-Mails

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

Login | Registrierung

SPIEGEL ONLINE **SCHULSPIEGEL**

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

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

Gefälschte E-Mail: Schulfrei ermogelt

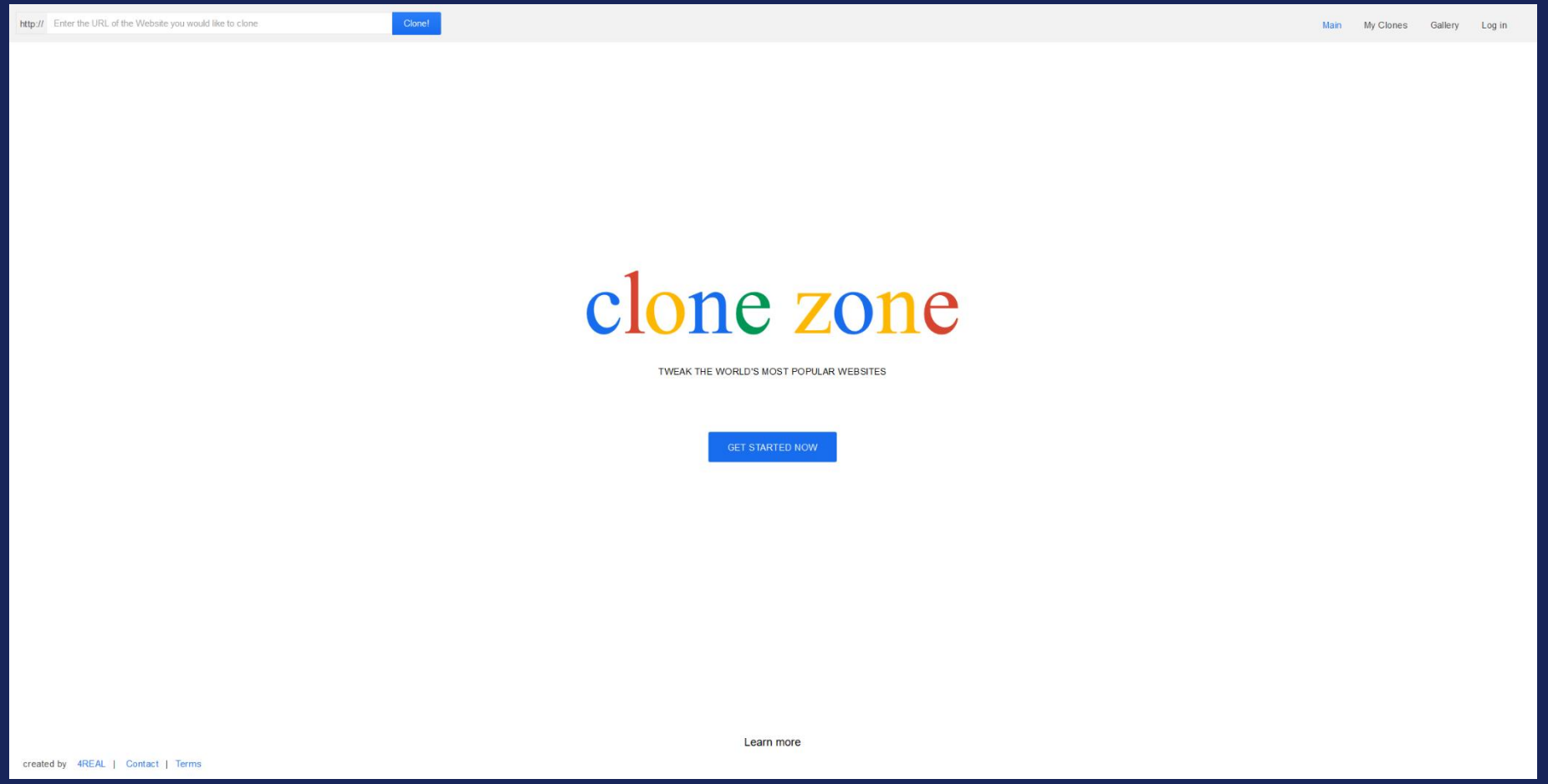
DPA

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 (10)

DEMO Manipulierte Websites



Quelle: clonezone.link (11)

Manipulierte Websites

Quelle: youtube.com (12)

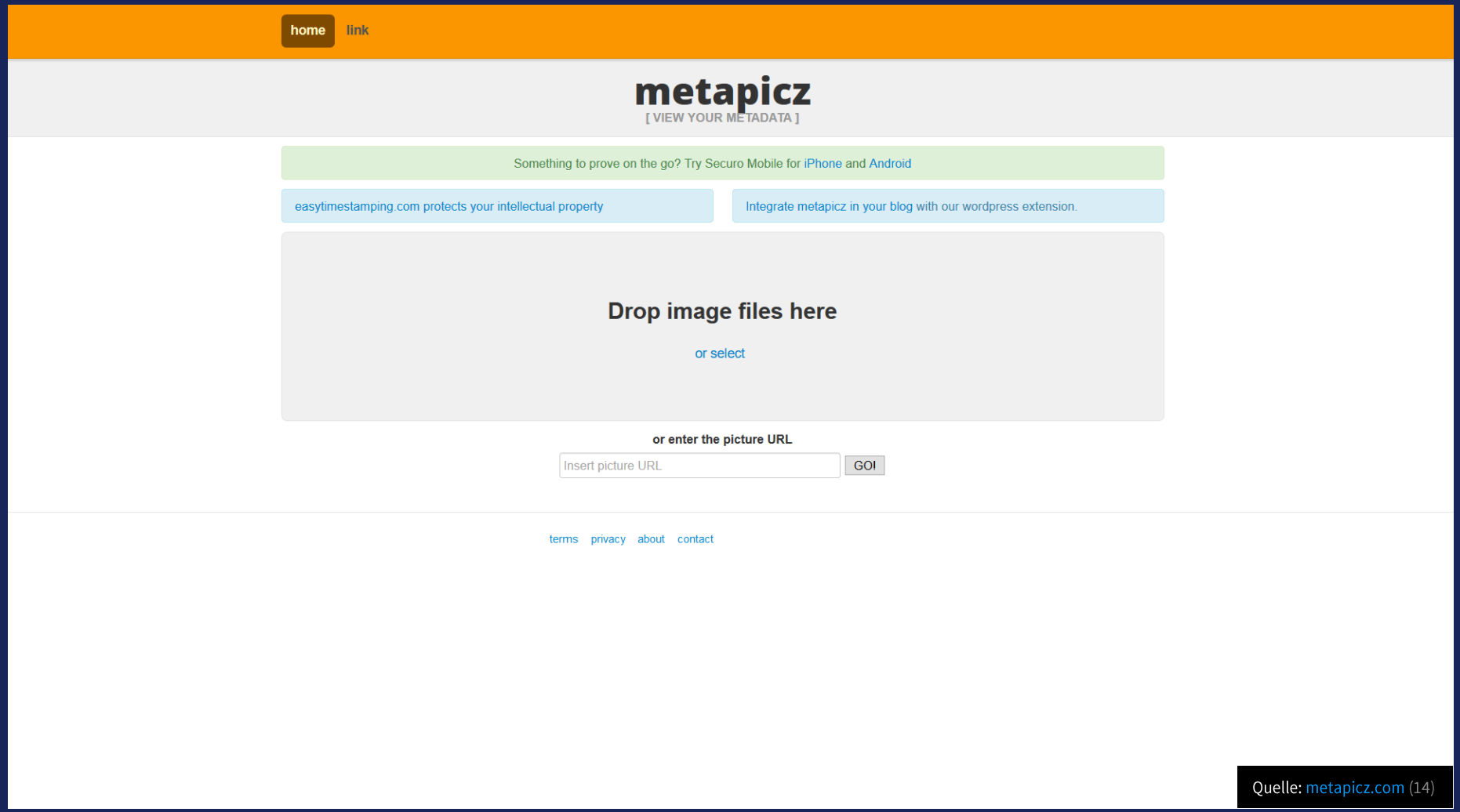
Social Hacking - Gefängnisausbruch

- 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

Quelle: heise.de (13)

DEMO Versteckte Informationen auslesen



Quelle: metapicz.com (14)

Passwortsicherheit

Öffentliche Passwörter

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

Quelle: : de.pinterest.com (16)

Öffentliche Passwörter - Interview

Quelle: youtube.com (17)

Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Fakultät Informatik

IT Sicherheit und Digitale Forensik

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

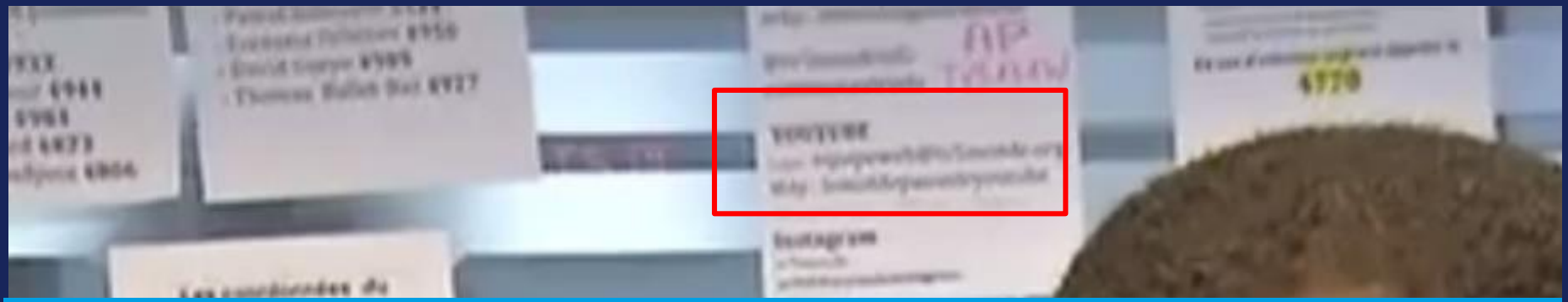
=> Spekulationen über öffentlich einsehbare Passwörter

Quelle: heise.de (18)

Faktor Mensch - Angriff auf TV5 Monde

Quelle: heise.de (18)

Faktor Mensch - Angriff auf TV5 Monde

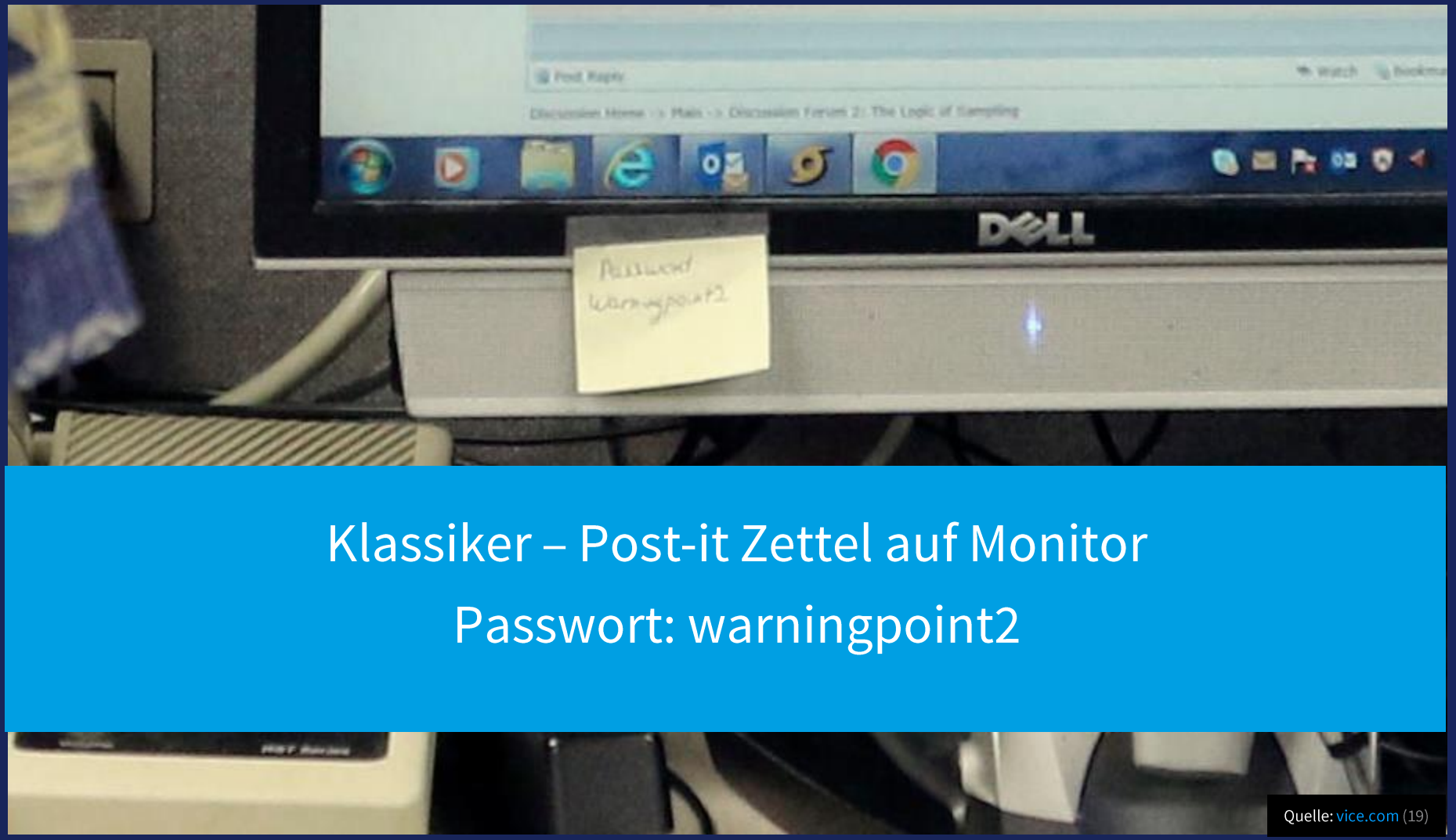


YouTube Passwort: "lemotdepassedeyoutube"
(etwa "dasyoutubepasswort")

Faktor Mensch

Quelle: vice.com (19)

Faktor Mensch



Klassiker – Post-it Zettel auf Monitor

Passwort: warningpoint2

Quelle: vice.com (19)

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.

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.

Bekannte Passwörter

124 lines (115 sloc) | 6.67 KB

Raw | Blame | History

```
Top 100 Adobe Passwords with Count

We do not (yet) have the keys Adobe used to encrypt the passwords of 130,324,429 users affected by
their most recent breach. However, thanks to Adobe choosing symmetric key encryption over hashing,
selecting ECB mode, and using the same key for every password, combined with a large number of
known plaintexts and the generosity of users who flat-out gave us their password in their password
hint, this is not preventing us from presenting you with this list of the top 100 passwords
selected by Adobe users.

While we are fairly confident in the accuracy of this list, we have no way to actually verify it
right now. We don't have the keys, and Adobe is not letting any of the affected accounts log in
until the owners reset their passwords. So, it is possible there is an error or two in here. Caveat
emptor and such.
```

Quelle: github.com (20)

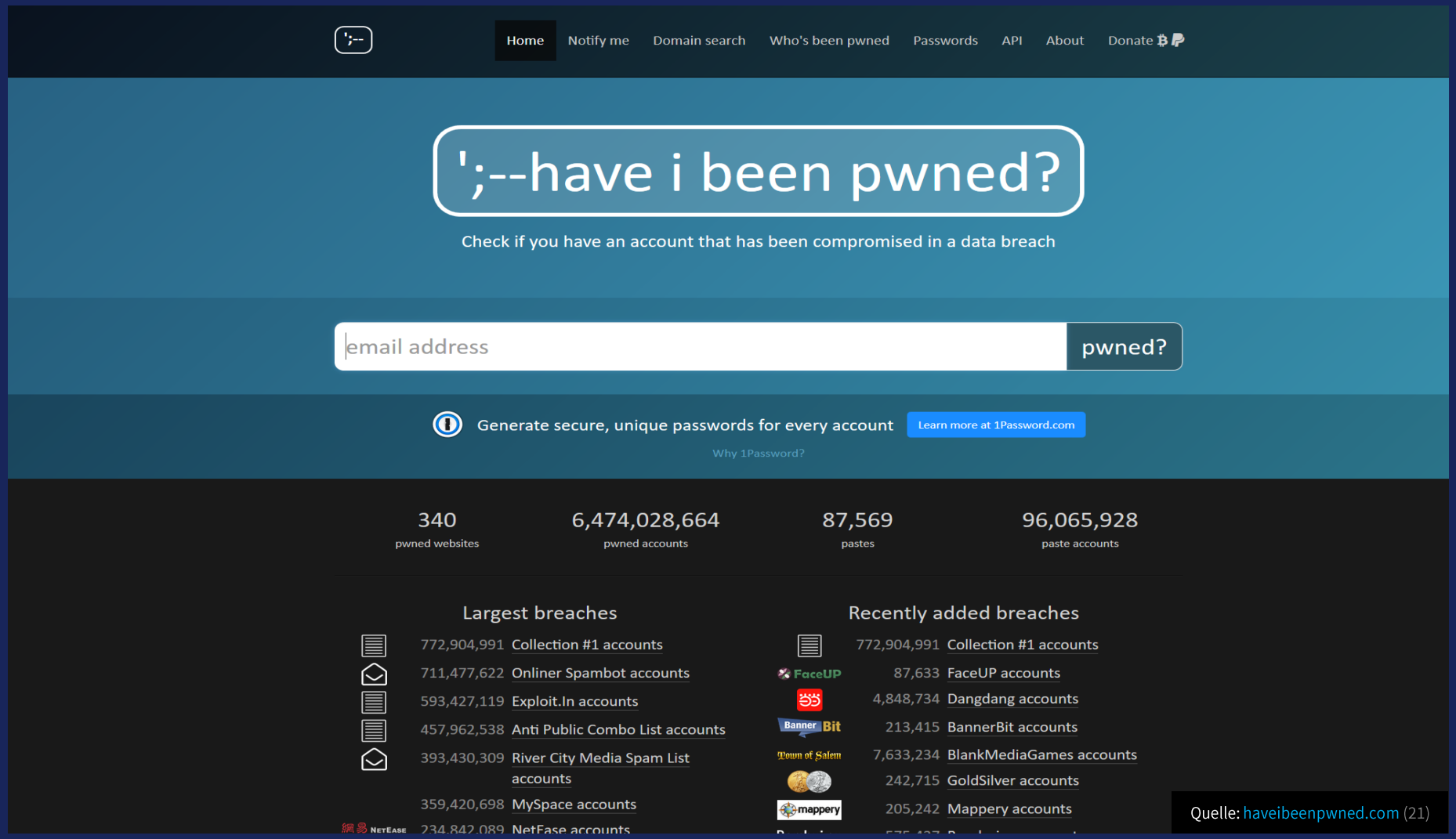
Sichere Passwörter

- 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, …)

DEMO Sichere Passwörter



Quelle: haveibeenpwned.com (21)

Hacking Hardware

Gadgets – Spionage Kamera

Gadgets – GSM Wanze

Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Fakultät Informatik

Logger - Keylogger

Logger - Screenlogger

USB – BadUSB (Rubber Ducky)

IT Sicherheit und Digitale Forensik

Cyber Security

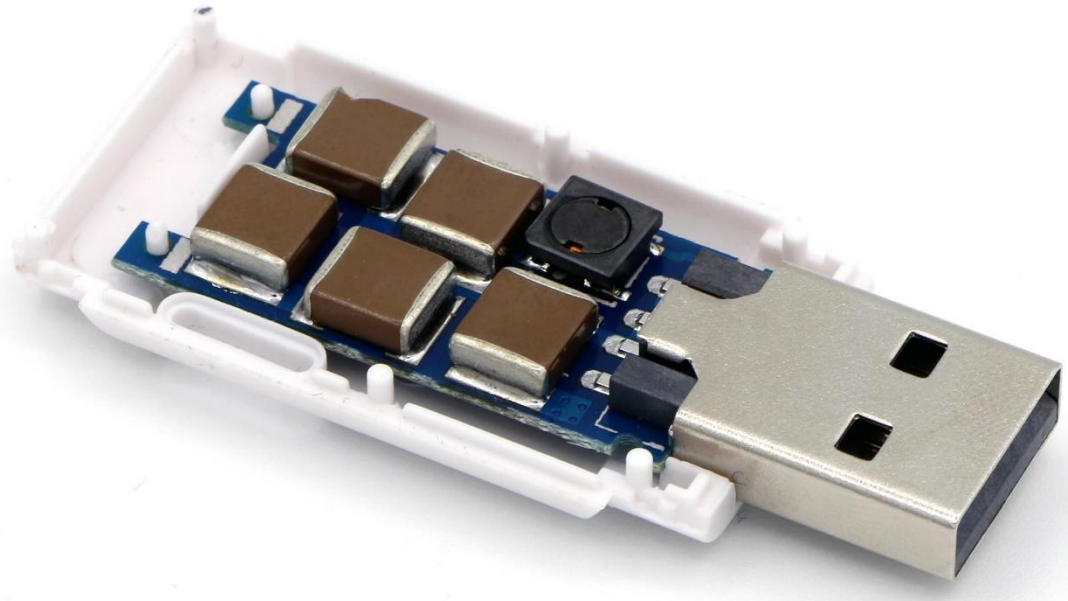
Social Engineering

Passwortsicherheit

Hacking Hardware
- Gadgets
- Logger
- USB
- Funk
- Netzwerk

USB – BadUSB (USBNinja)

USB - USBKill



IT Sicherheit und Digitale Forensik

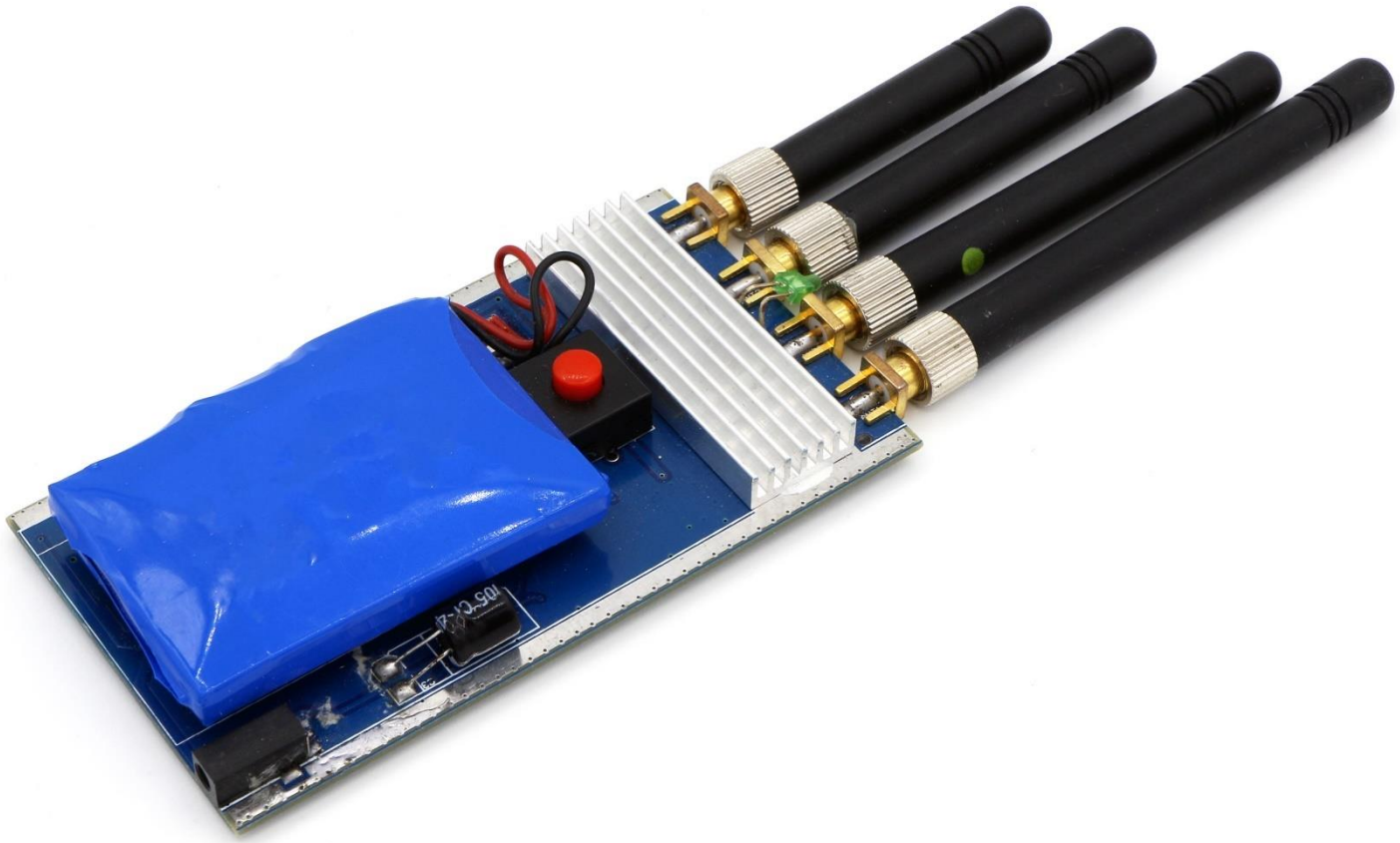
Cyber Security

Social Engineering

Passwortsicherheit

Hacking Hardware
- Gadgets
- Logger
- USB
- Funk
- Netzwerk

Funk - Störsender



Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Fakultät Informatik

IT Sicherheit und Digitale Forensik

Cyber Security

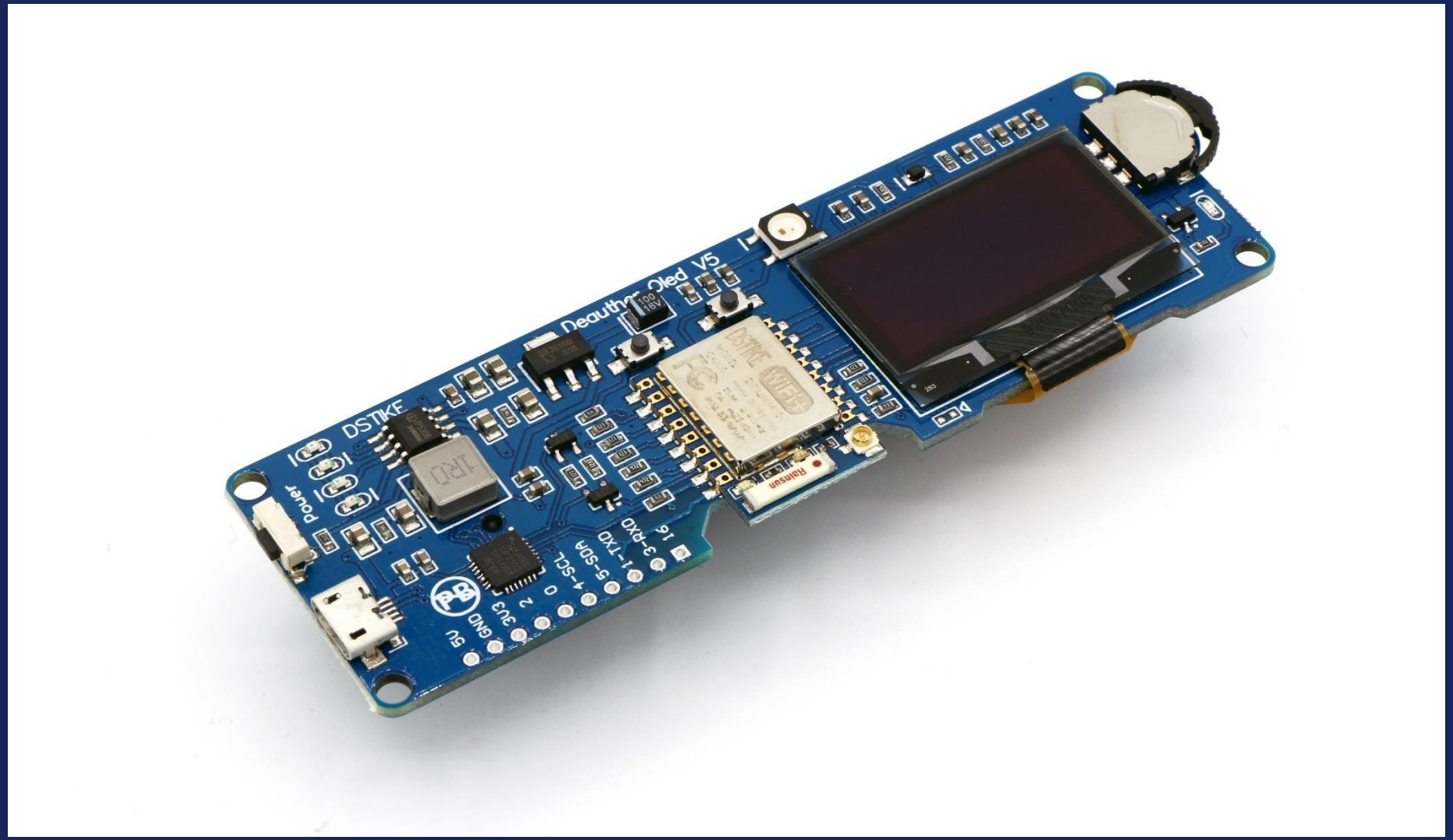
Social Engineering

Passwortsicherheit

Hacking Hardware
- Gadgets
- Logger
- USB
- Funk
- Netzwerk

Funk - Software Defined Radio

Netzwerk – WiFi Deauther



Netzwerk - Packet-Squirrel

Vielen Dank für Ihre Aufmerksamkeit

Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Fakultät Informatik

IT Sicherheit und Digitale Forensik

Prof. Holger Morgenstern
Tobias Scheible, M.Eng.

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=5M9k7wfiWiI, 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=opRMrEfAIiI, 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/symfobrute/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