Cyber Security Workshop

Hochschule
Albstadt-Sigmaringen

Albstadt-Sigmaringen University

Cyber Security Workshop

Protect your Data! - Cyber Security

Tobias Scheible

Über Tobias Scheible

Studium Kommunikations- und Softwaretechnik, Fachrichtung Kommunikationstechnik,
Hochschule Albstadt-Sigmaringen

2009 bis 2012: Softwareingenieur im Bereich Web Development,
Gute Aussicht Kommunikations GmbH

Seit 2012: Wissenschaftlicher Mitarbeiter | Bachelor IT Security & Master Digitale Forensik,
Hochschule Albstadt-Sigmaringen

Schwerpunkte

Internettechnologien, Web-Programmierung, Cloud Computing und Web Applications Security

Mail | Profil | Xing | Twitter | Facebook | Slideshare

Agenda

- IT-Sicherheit
  - Sicherheitsvorfälle
  - Hacking mit Google
- Passwortsicherheit
  - Sicherheit von Passwörtern
  - Passwortlisten und Tools
- Sicher im Web
  - Browser Fingerprinting
  - Firefox absichern
- Hardware Tools
  - Störsender
  - Keylogger

IT-Sicherheit

000000000

?

Quelle: heise.de

00000000

Launch-Code für die in den USA stationierten Atomraketen

(1962 bis 1977)

Quelle: heise.de

Atom-Raketen: Steuerungstechnik aus den 70ern

Quelle: zeit.de

Quelle: chip.de

Social Engineering - Gefälschte E-Mail

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

Aktion der Groupe Mutuel

Quelle: youtube.com

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

Quelle: heise.de

„Sozial-Ingenieure hacken Menschen.“

Freitag, 12. Februar 2016 | Service | Abo | Shop | Newsletter | Login | Registrieren | Suchbegriff, WKN, ISIN

Wirtschafts Woche

UNTERNEHMEN FINANZEN POLITIK ERFOLG TECHNOLOGIE

Trends Management Gründer Beruf Jobsuche Campus & MBA Karriere Jobturbo

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

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.

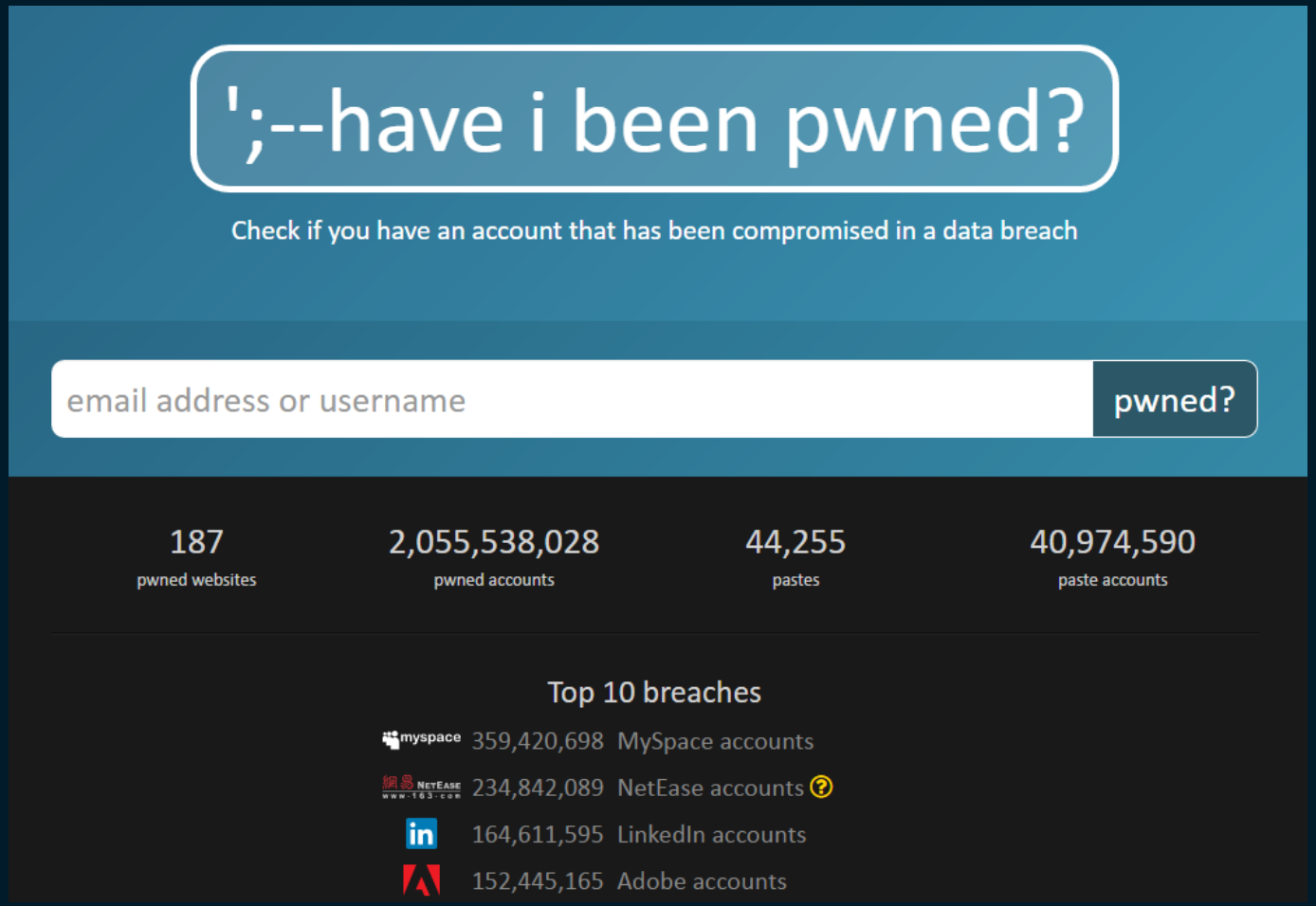
Bild: dpa

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

Quelle: wiwo.de

PRAXIS Passwort geleakt?



Quelle: haveibeenpwned.com

Angriff auf den Fernsehsender TV5

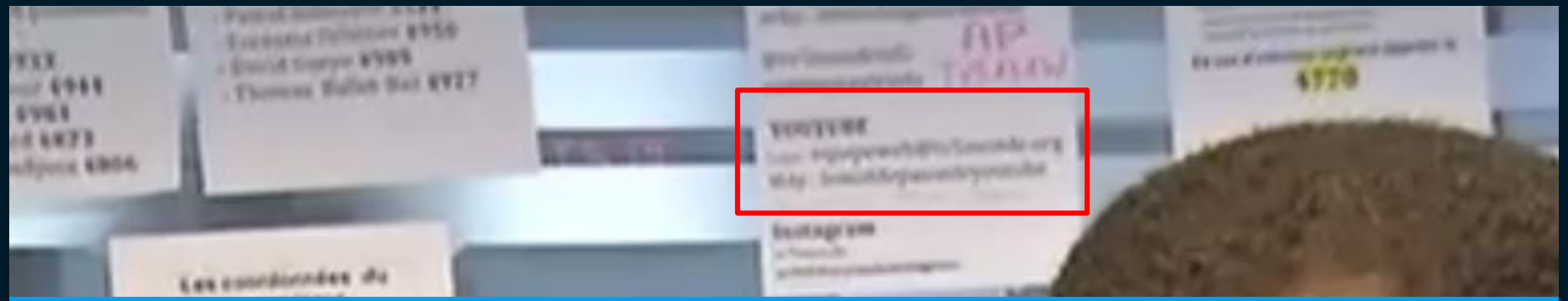
- Umfangreicher Angriff auf den französischen Sender TV5Monde
  - Alle Kanäle des Fernsehunternehmens TV5Monde gingen offline
  - Die Website verbreitete kurzfristig islamistische Drohungen
  - Auf der Facebook-Seite wurden ebenfalls Drohungen verbreitet
- Spekulationen über öffentlich einsehbare Passwörter

Quelle: heise.de

Angriff auf den Fernsehsender TV5

Quelle: heise.de

Angriff auf den Fernsehsender TV5



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

Quelle: heise.de

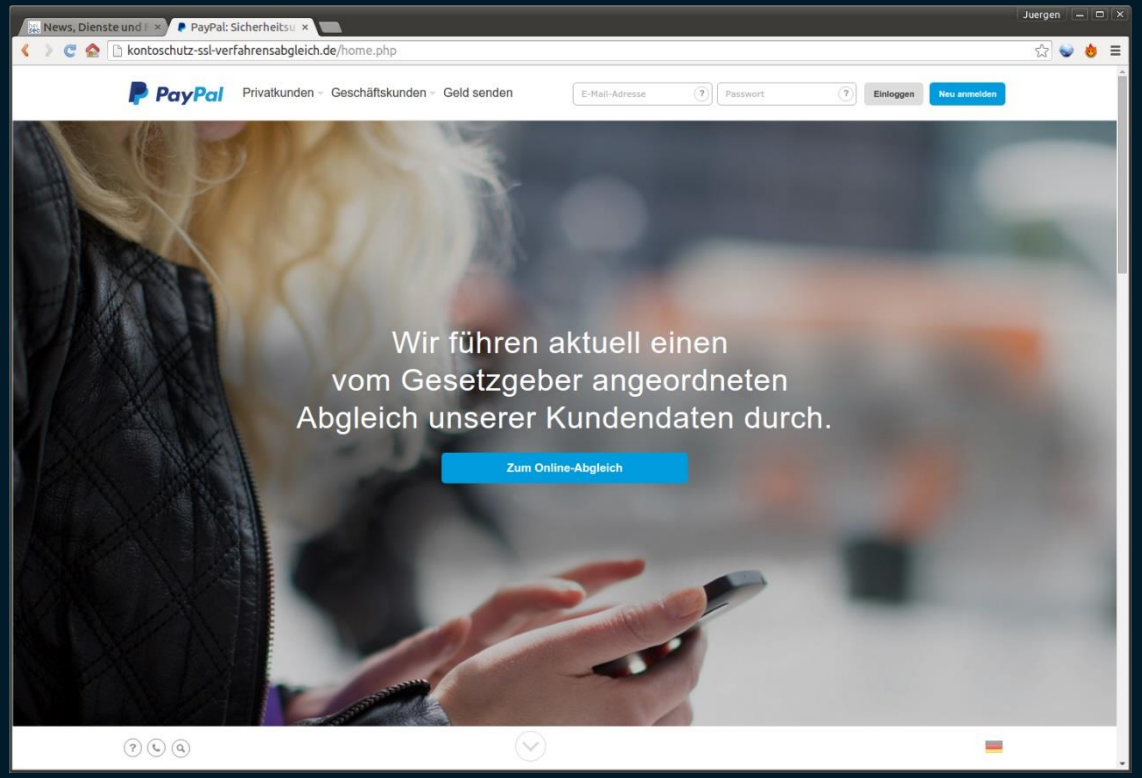
Passwort für Raketen-Warnsystem

- Passwort für Raketen-Warnsystem stand wohl monatelang im Internet
- Klassiker – Post-it Zettel auf Monitor
- Passwort: warningpoint2

Quelle: vice.com

Phisher verwenden Geo-Blocking

- "Sorry. Diese Phishing Website ist in deinem Land nicht verfügbar."
- Malware-Filterlisten (Crawler) häufig USA-zentriert
- Wenn eine deutsche Phishing-Website aus dem Ausland aufgerufen wird, werden harmlose Inhalte dargestellt



Quelle: heise.de

Bad E-Cigarette

- Ende 2014 machte eine Geschichte (ungeprüft) über einen mit Malware infizierten PC die Runde
- Nach Überprüfung aller Angriffsvektoren fand man heraus, dass über ein E-Zigaretten USB-Ladegerät Malware eingeschleust wurde

Quelle: reddit.com

Zugriff auf Geldautomaten

- 11/2015: Kommandozeilen-Zugriff auf Geldautomat während eines Updates (http://www.heise.de/security/meldung/Kommandozeilen-Zugriff-Sicherheitsluecke-in-Geldautomaten-der-Sparkasse-2867559.html)
- 10/2015: Angriff auf Geldautomaten via USB-Stick (http://www.berlin.de/polizei/polizeimeldungen/pressemitteilung.386807.php)
- 12/2014: Kriminelle verschafften sich über Spionage-Software Zugriff auf Geldautomaten und manipulierten die Geldausgabe so, dass die Scheinausgabefächer falsche Werte erhielten (http://www.heise.de/security/meldung/Anunak-So-geht-Bankraub-im-21-Jahrhundert-2505940.html)

Quelle: heise.de

Hacking mit Google

- Anweisungen zum Formulieren von Suchanfragen:

Operator	Purpose	Mixes with Other Operators?	Can be used Alone?	Web	Images	Groups	News
intitle	Search page Title	yes	yes	yes	yes	yes	yes
allintitle	Search page title	no	yes	yes	yes	yes	yes
inurl	Search URL	yes	yes	yes	yes	not really	like intitle
allinurl	Search URL	no	yes	yes	yes	yes	like intitle
filetype	specific files	yes	no	yes	yes	no	not really
allintext	Search text of page only	not really	yes	yes	yes	yes	yes
site	Search specific site	yes	yes	yes	yes	no	not really
link	Search for links to pages	no	yes	yes	no	no	not really
inanchor	Search link anchor text	yes	yes	yes	yes	not really	yes
numrange	Locate number	yes	yes	yes	no	no	not really
daterange	Search in data range	yes	no	yes	not really	not really	not really
author	Group author search	yes	yes	no	no	yes	not really
group	Group name search	not really	yes	no	no	yes	not really
insubject	Group subject search	yes	yes	like intitle	like intitle	yes	like intitle
msgid	Group msgid search	no	yes	not really	not really	yes	not really

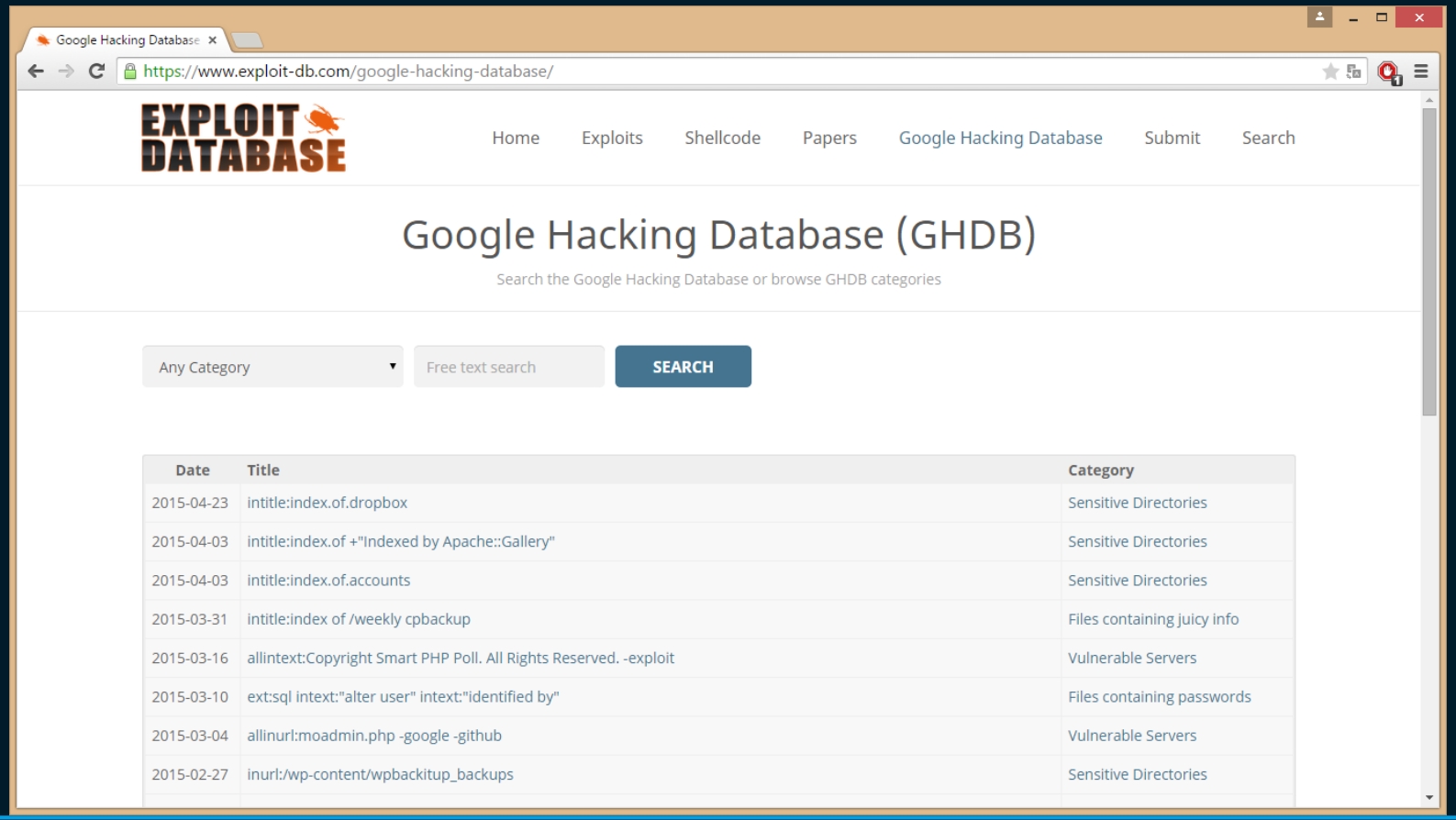
Quelle: wikipedia.org

PRAXIS Hacking mit Google

- Beispiel Suchanfragen nach Webcams:
  - inurl:"viewerframe?mode=motion"
  - intitle:"snc-rz30 home"
  - intitle:"WJ-NT104 Main"
  - inurl:LvAppl intitle:liveapplet
  - intitle:"Live View / - AXIS"
  - inurl:indexFrame.shtml

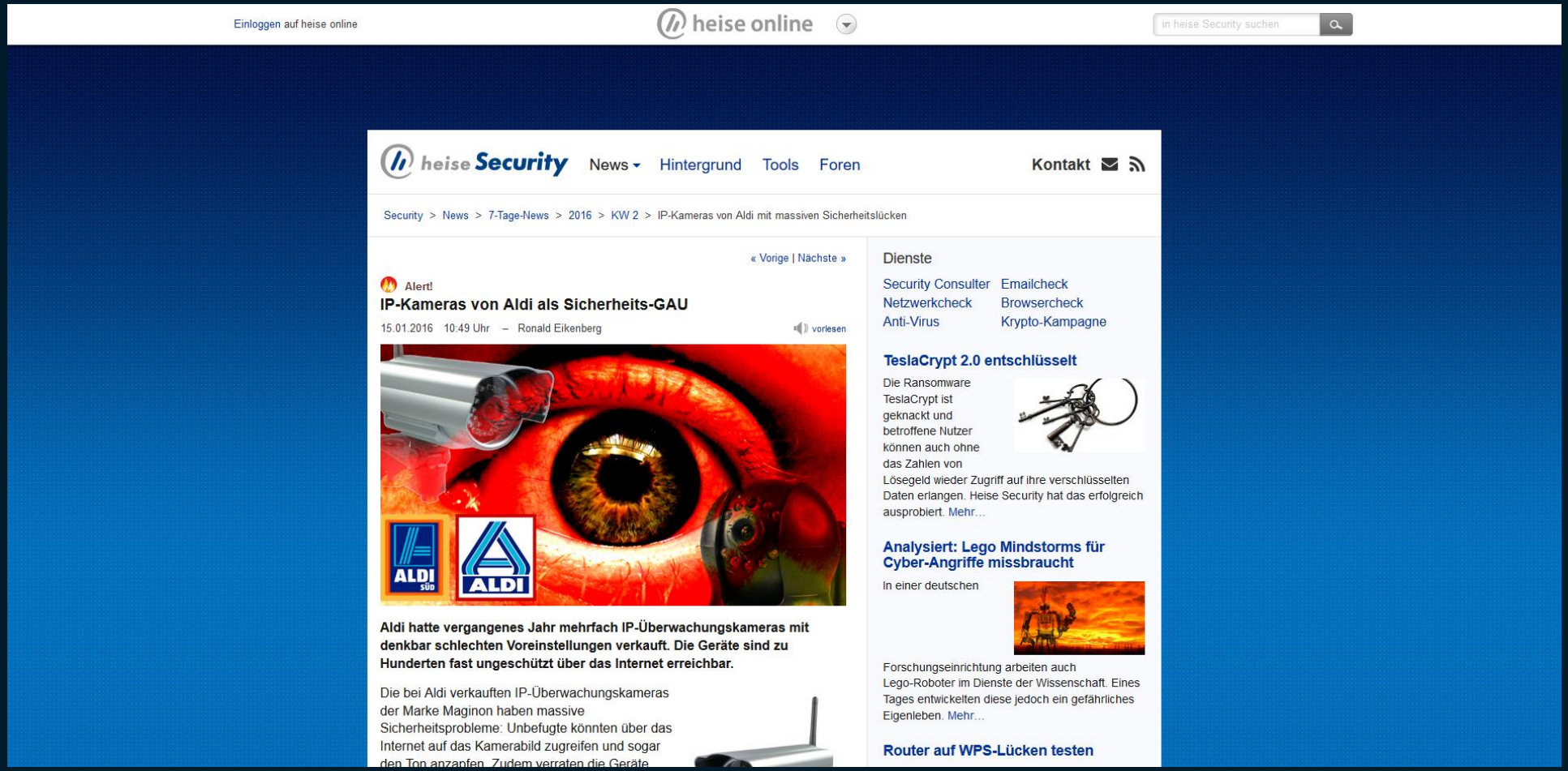
PRAXIS Hacking mit Google

- Datenbank mit vorformulierten Suchanfragen



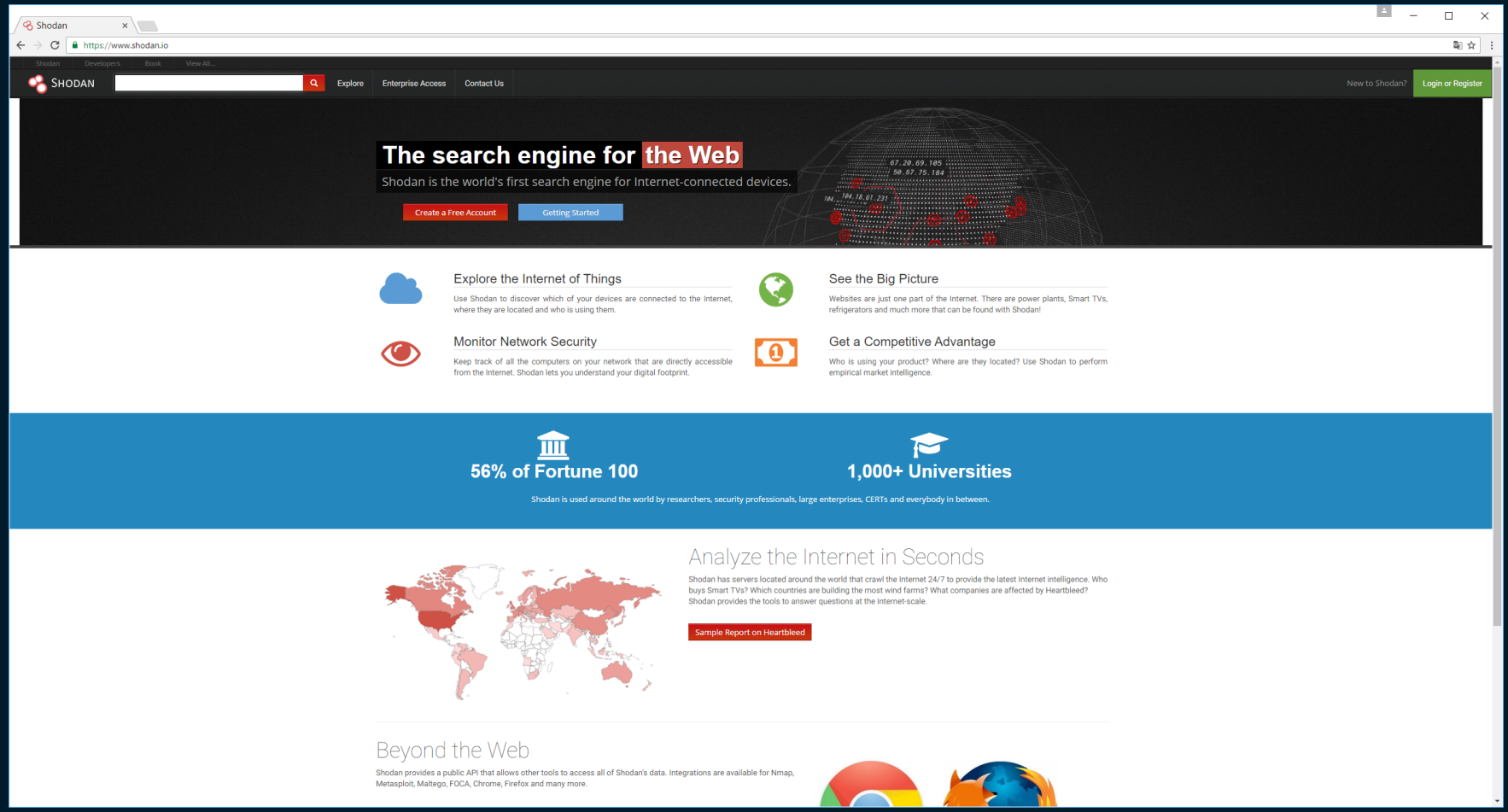
Quelle: wexploit-db.com

Bug or Feature?



Quelle: heise.de

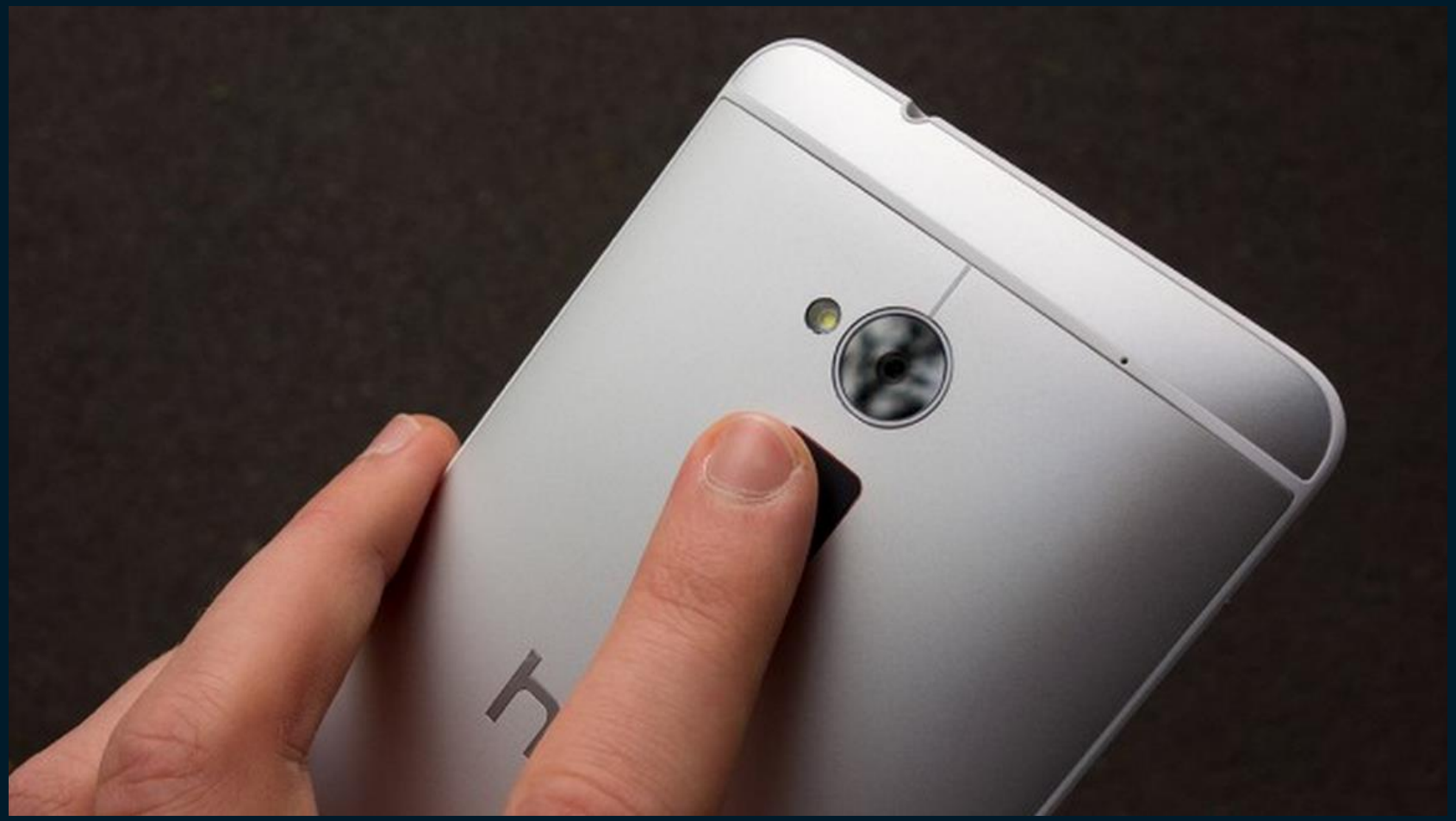
Suchmaschine für das Internet der Dinge



Quelle: shodan.io

Passwortsicherheit

Fingerabdruckscanner



Quelle: imore.com

Fingerabdruckscanner

Quelle: rolf-fensterbau.de

Fingerabdruckscanner

Quelle: telegraph.co.uk

Probleme mit Fingerabdruckscannern

- Einmal verlorener Abdruck kann nicht ersetzt werden
- Nur „10“ Möglichkeiten stehen zur Verfügung
- Größere Verbreitung sorgt für häufigere Diebstähle
- Komplexe Lösung nicht immer die sicherste

Quelle: clker.com

Ursula von der Leyen

Quelle: n24.de

Fingerabdruck von Ursula von der Leyen

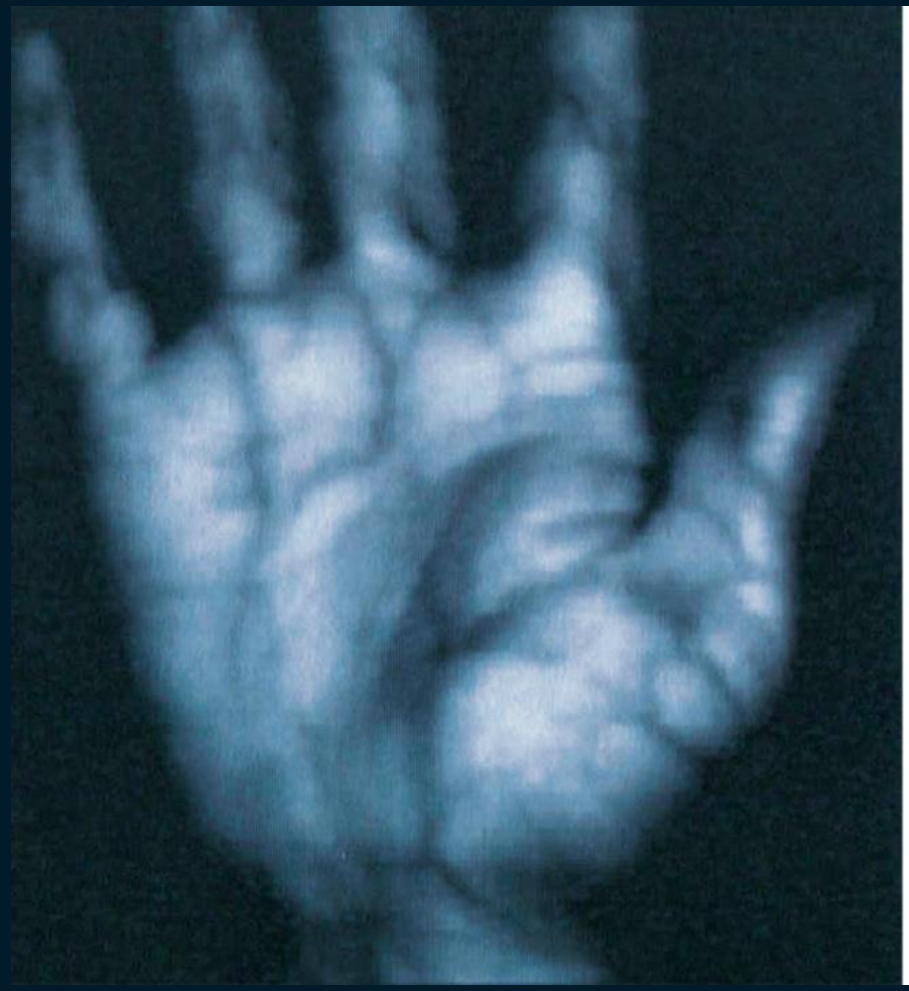
guten Tag, mein Name ist
Dr. von der Leyen

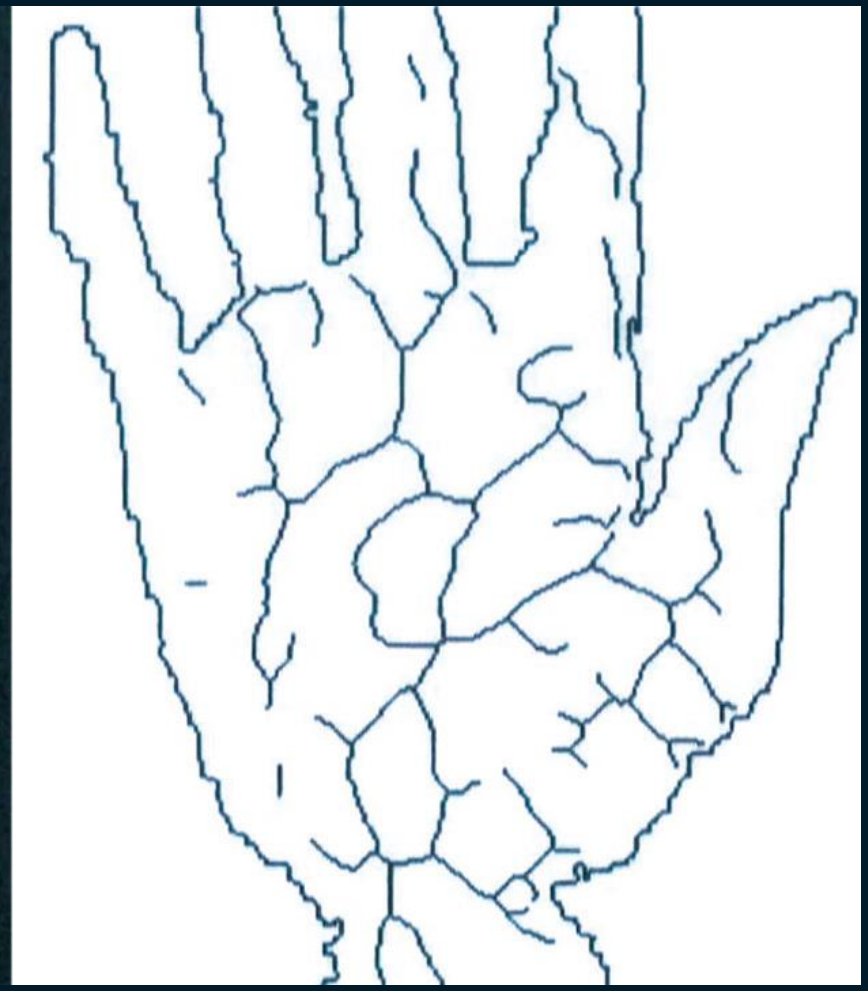
Quelle: heise.de

Venen-Scanner

Quelle: futerzone.at

Venen-Scanner





Quelle: futerzone.at

Quelle: http://futurezone.at/science/biometrie-venen-scanner-schlaegt-iris-messung/24.597.953

Passwortsicherheit

Quelle: youtube.com

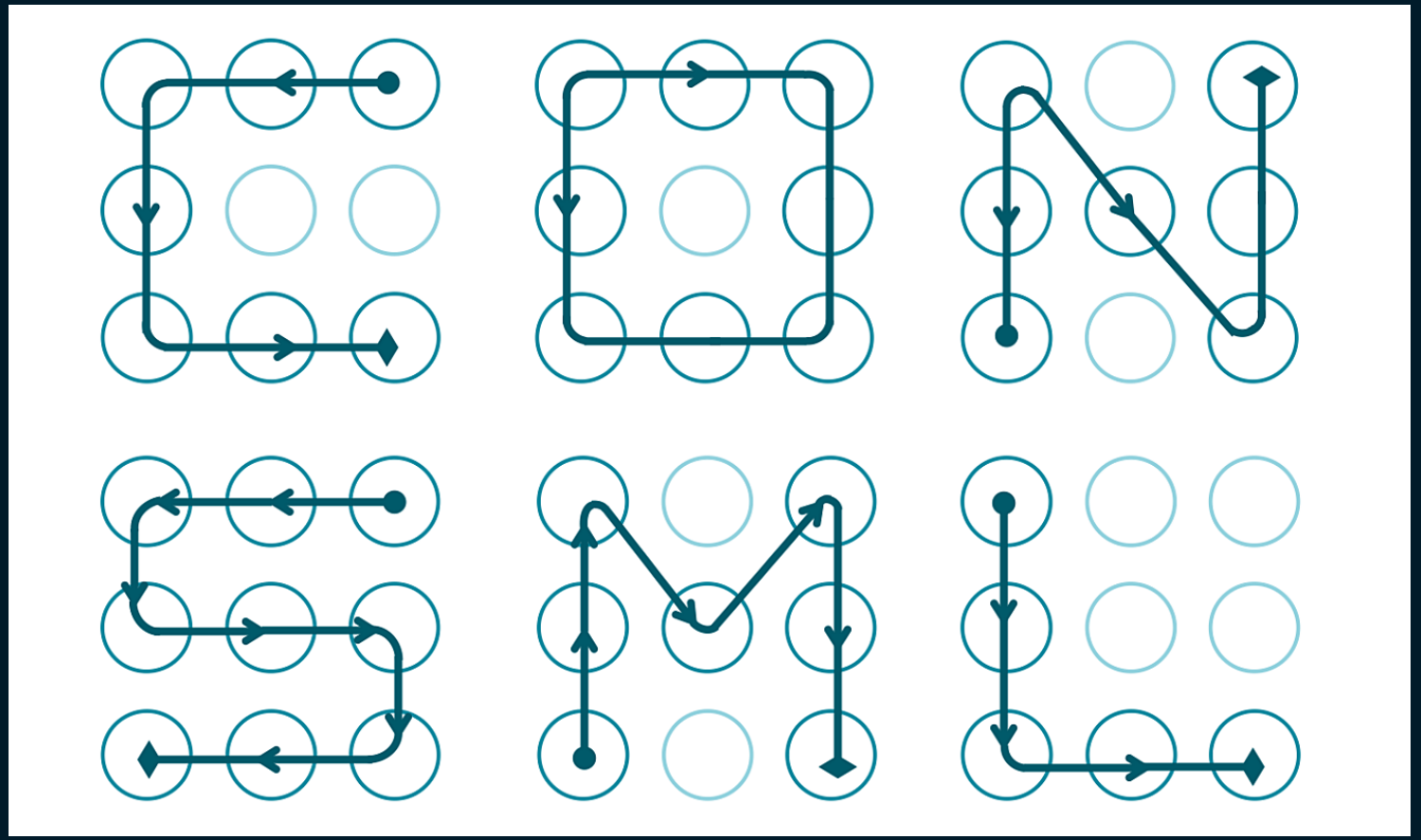
Bad Passwords – Bad Lock Patterns

- Jeder kennt Toplisten mit schlechten Passwörtern:
  - 12345
  - password
  - qwerty
  - …
- Studie von Marte Løge analysierte über 4000 Android Entsperrmuster im Rahmen ihrer Master Thesis

Quelle: technic-al.com

Bad Lock Patterns

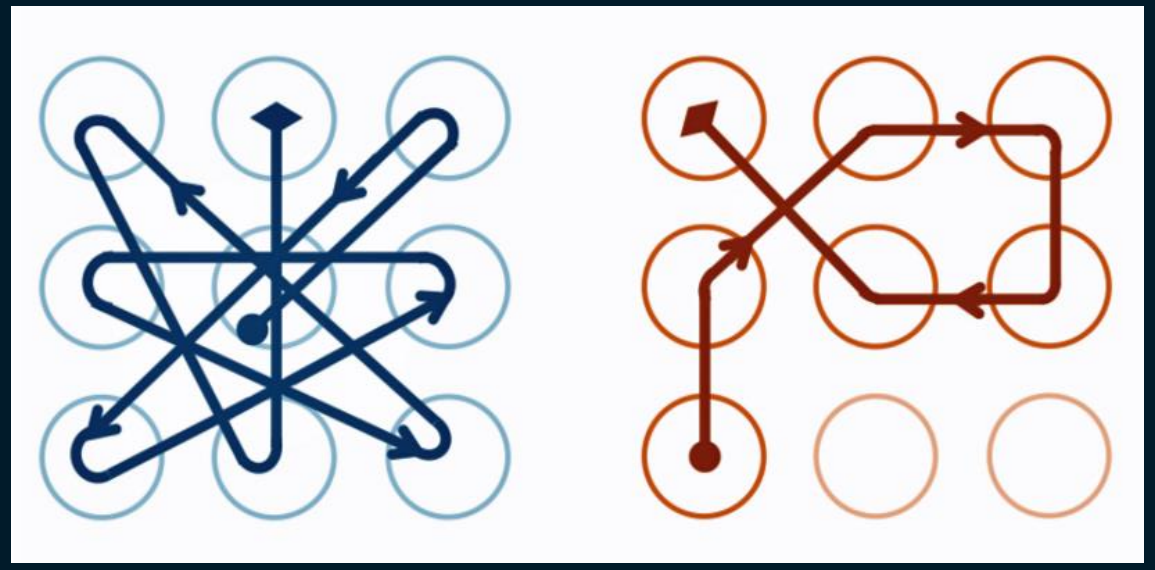
- 10 % aller Versuchspersonen nutzen ein Muster, das einem Buchstaben ähnelt
- 44 % starten oben links
- 77 % fangen in einer der vier Ecken an
- Durchschnittliche Anzahl von fünf verwendeten Knoten (~9000 Kombinationsmöglichkeiten)
- Muster von links → rechts; oben → unten werden häufig verwendet



Quelle: arstechnica.com

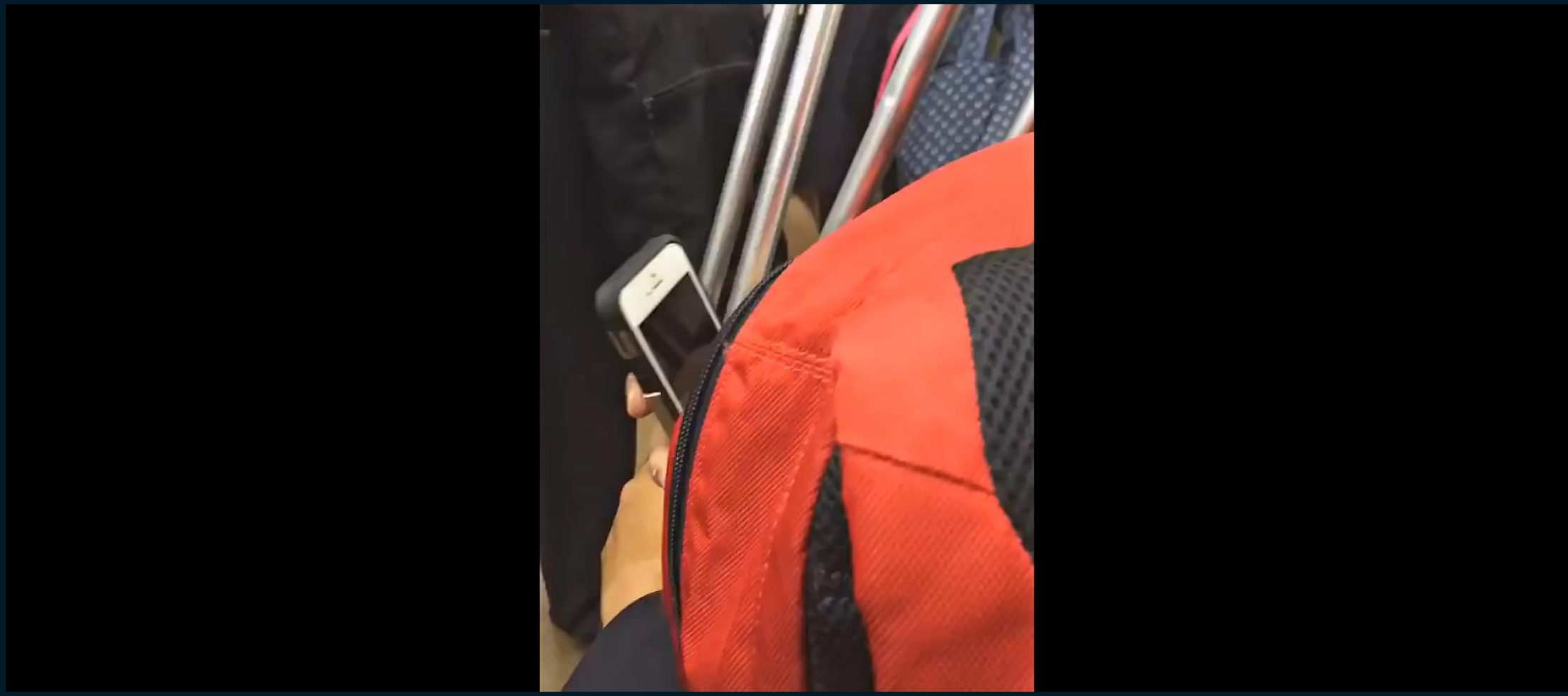
Bad Lock Patterns - Gegenmaßnahmen

- Komplizierte Muster verwenden
- Allerdings sind weitere mögliche Angriffsvektoren vorhanden:
  - Brute Force z. B. via Teensy + USB OTG Kabel
    - Selbst bei Beachtung der Penalty (i. d. R. 30 Sekunden) meist in einem vertretbaren Zeitraum knackbar 😊
  - Angriffe über ADB (Android Debug Bridge)
- PINs verwenden



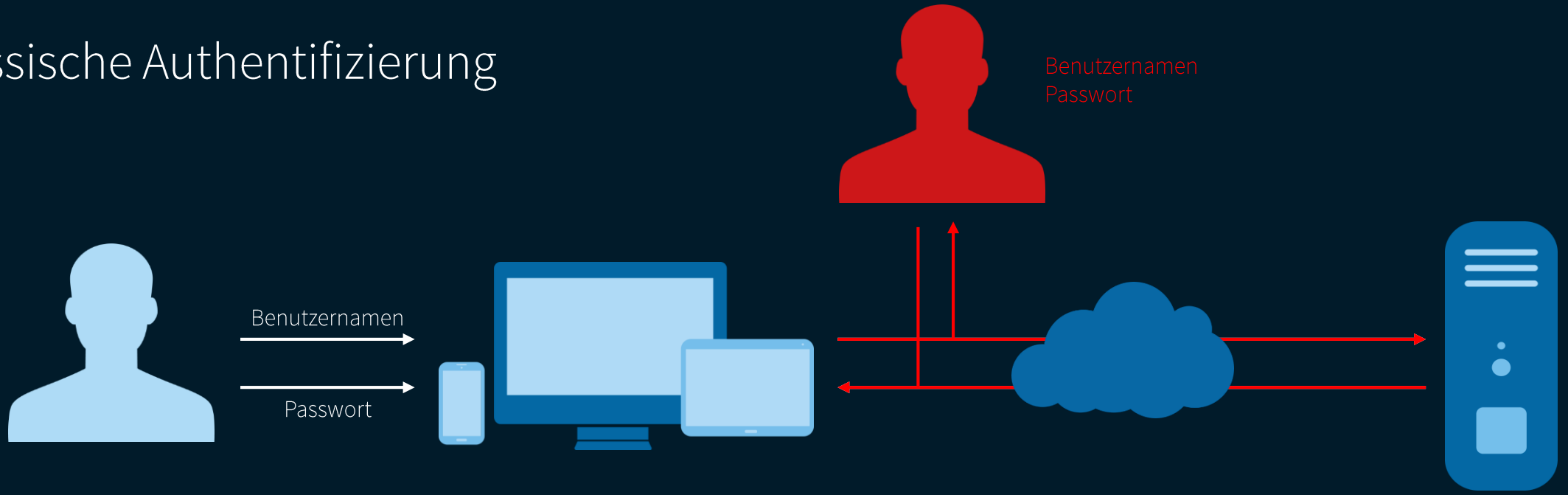
Quelle: arstechnica.com

Bad Lock Patterns - Gegenmaßnahmen



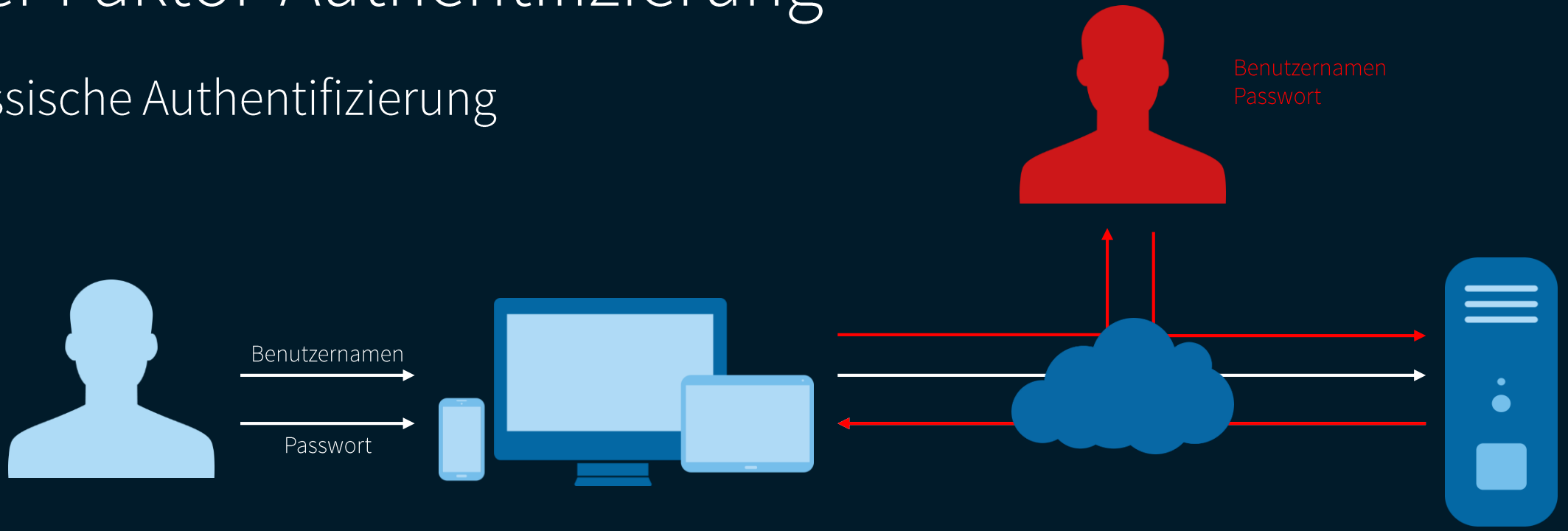
Zwei-Faktor-Authentifizierung

- Klassische Authentifizierung



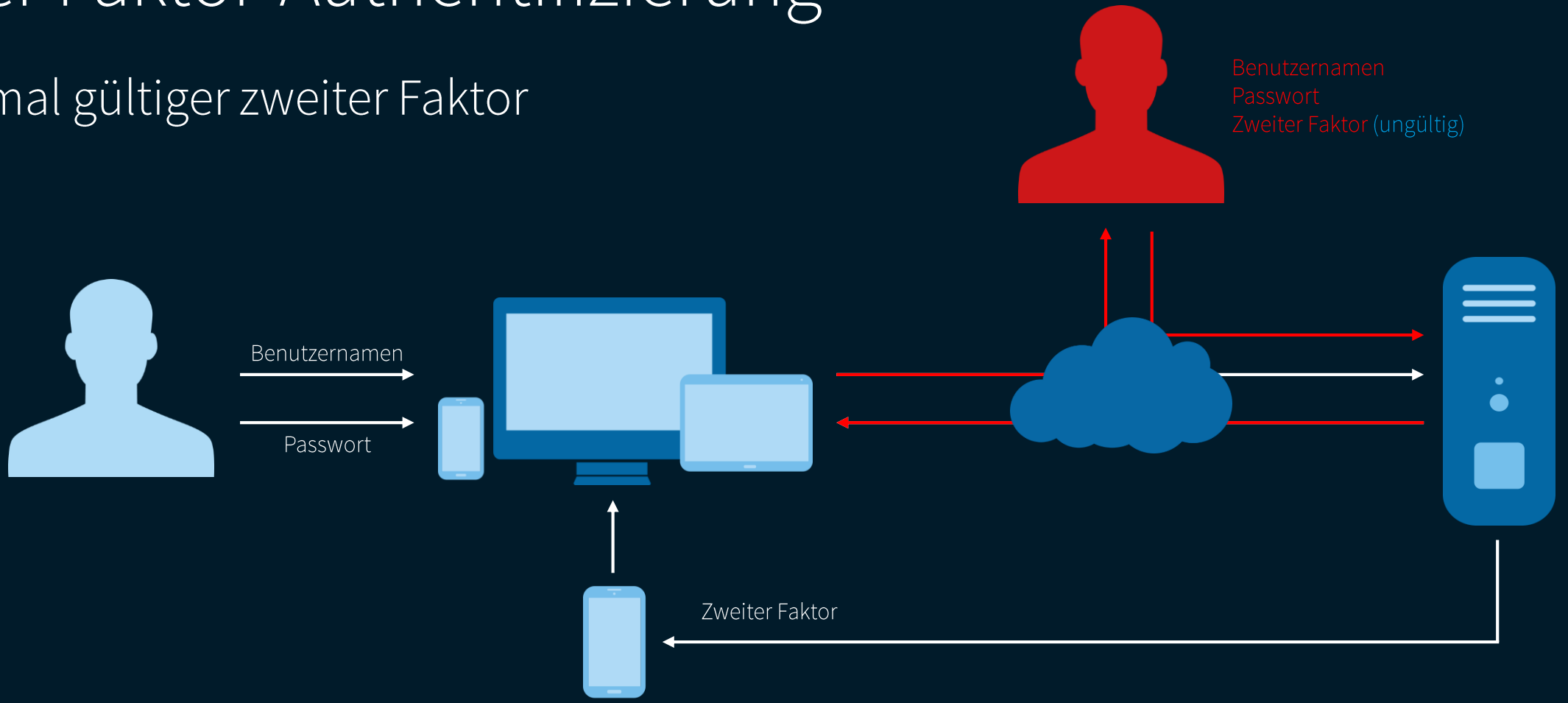
Zwei-Faktor-Authentifizierung

- Klassische Authentifizierung



Zwei-Faktor-Authentifizierung

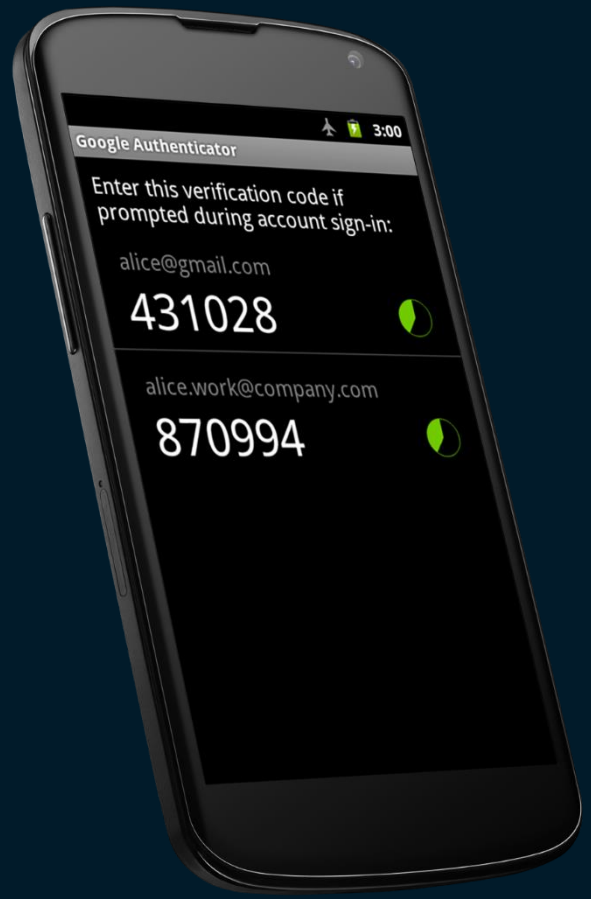
- Einmal gültiger zweiter Faktor



Zwei-Faktor-Authentifizierung

- Mittelbare Zwei-Faktor-Authentifizierung
  - Manuelle Eingabe eines zweiten Faktors
- Halbautomatische Zwei-Faktor-Authentifizierung
  - Keine Dateneingabe mehr notwendig – z.B. NFC-Karte
- Vollautomatische Zwei-Faktor-Authentifizierung
  - Authentifizierung mit dem Smartphone per Bluetooth
- Universelle Zwei-Faktor-Authentifizierung
  - Über Herstellergrenzen hinweg – z.B. FIDO-Allianz

Zwei-Faktor-Authentifizierung



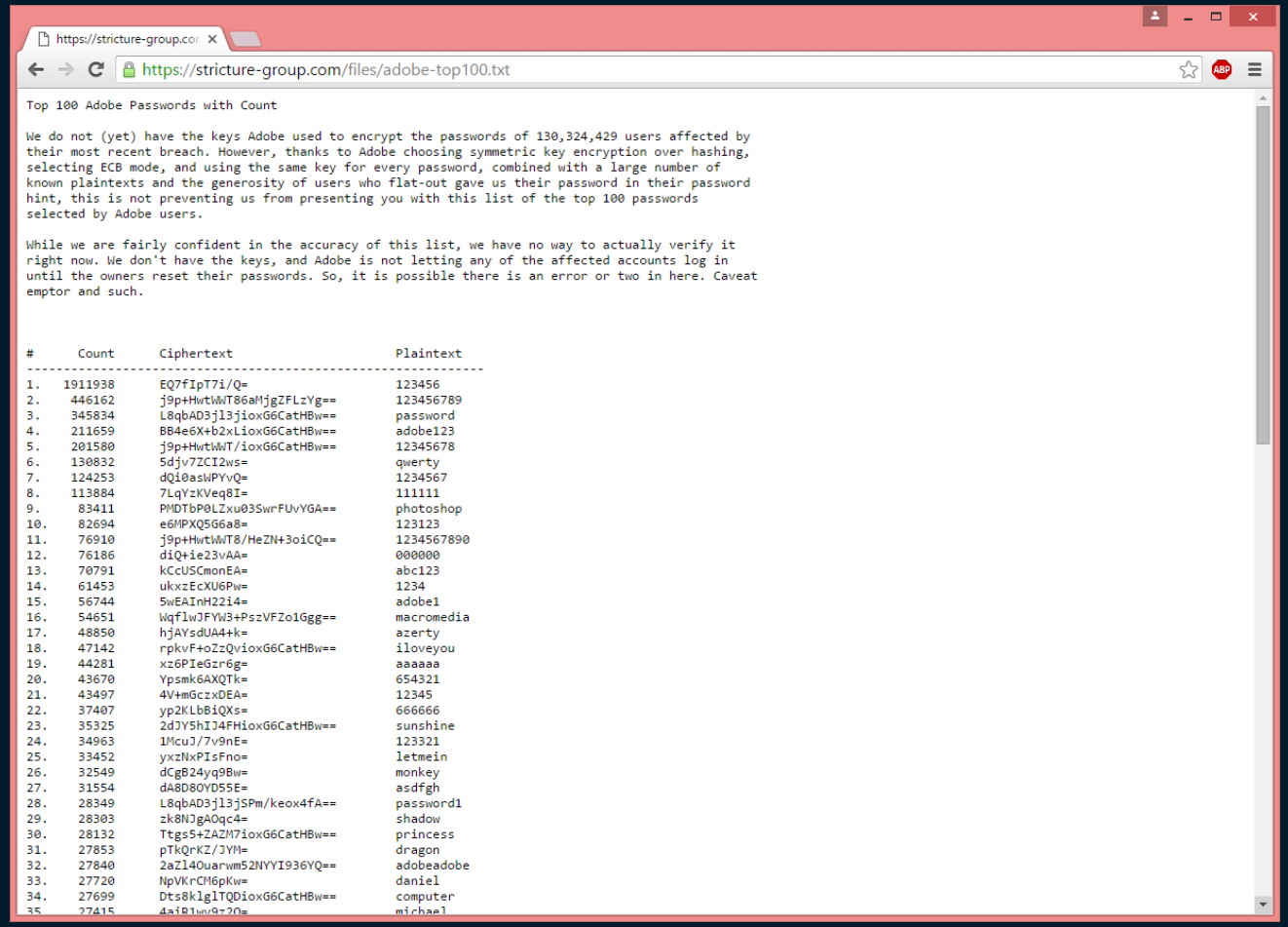
Quelle: mockuphone.com

Quelle: linuxveda.com

Hashfunktionen

- Abbildung einer großen Eingabemenge auf eine kleinere Zielmenge
- Einwegfunktion auf Basis mathematischer Algorithmen
- Verwendung:
  - Speicherung von Passwörtern
  - Validierung von größeren Datenmengen
- Beispiele (MD5):
  - test
    098f6bcd4621d373cade4e832627b4f6
  - Es gibt keine Sicherheit, nur verschiedene Grade der Unsicherheit.
    648374430dca4feb98efbba184bb8c97

Hashfunktionen



https://stricture-group.com/files/adobe-top100.txt

Top 100 Adobe Passwords with Count

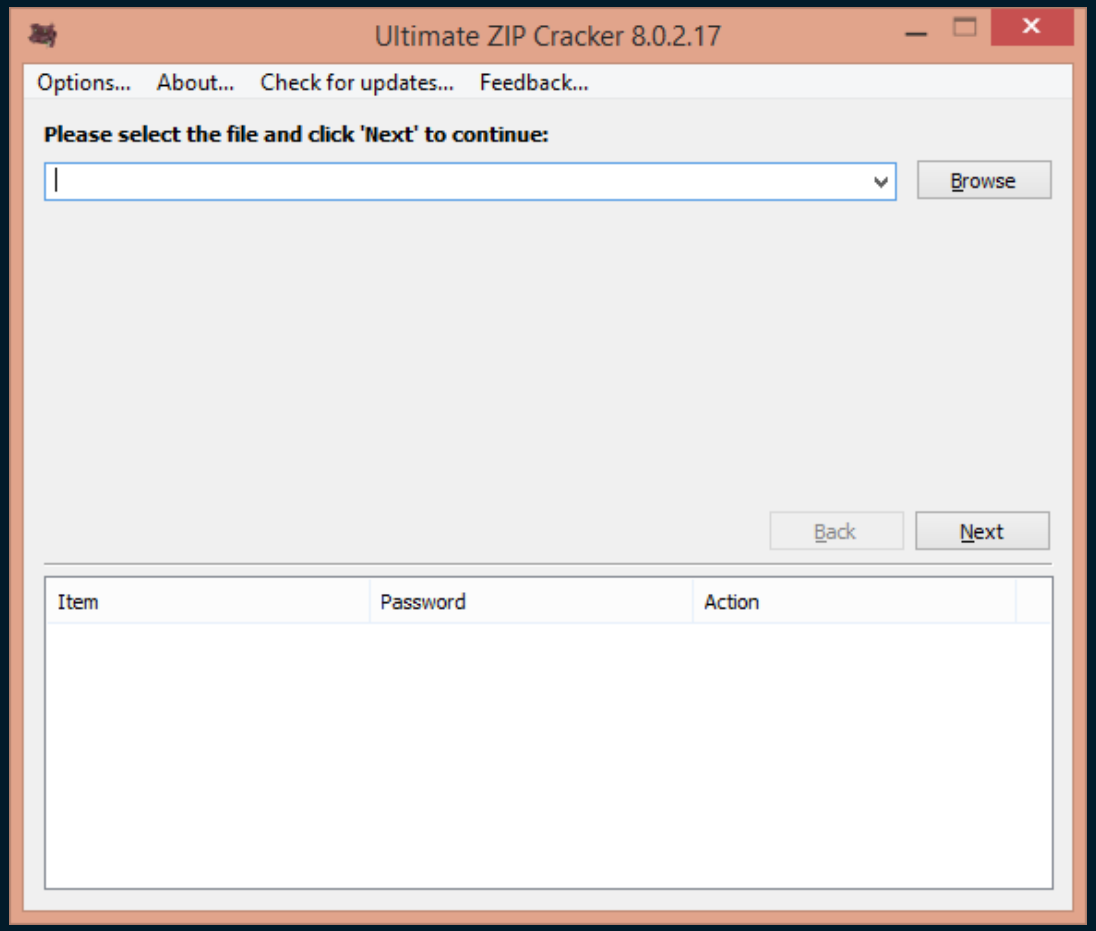
We do not (yet) have the keys Adobe used to encrypt the passwords of 130,324,429 users affected by their most recent breach. However, thanks to Adobe choosing symmetric key encryption over hashing, selecting ECB mode, and using the same key for every password, combined with a large number of known plaintexts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

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

#	Count	Ciphertext	Plaintext
1.	1911938	EQ7fIpT7i/Q=	123456
2.	446162	j9p+HwtWWT86aMjgZFLzYg==	123456789
3.	345834	L8qbAD3jl3jioxG6CatHBw==	password
4.	211659	BB4e6X+b2xLioxG6CatHBw==	adobe123
5.	201580	j9p+HwtWWT/ioxG6CatHBw==	12345678
6.	130832	5djv7ZCI2ws=	qwerty
7.	124253	dQi0asWPYvQ=	1234567
8.	113884	7LqYzKVeq8I=	111111
9.	83411	PMDTbP0LZxu03SwrFUvYGA==	photoshop
10.	82694	e6MPXQ5G6a8=	123123
11.	76910	j9p+HwtWWT8/HeZN+3oiCQ==	1234567890
12.	76186	diQ+ie23vAA=	000000
13.	70791	kCcUSCmonEA=	abc123
14.	61453	ukxzEcXU6Pw=	1234
15.	56744	5wEAInH22i4=	adobe1
16.	54651	WqflwJFYW3+PszVFZo1Ggg==	macromedia
17.	48850	hjAYsdUA4+k=	azerty
18.	47142	rpkvF+oZzQvioxG6CatHBw==	iloveyou
19.	44281	xz6PIeGzr6g=	aaaaaa
20.	43670	Ypsmk6AXQTk=	654321
21.	43497	4V+mGczxDEA=	12345
22.	37407	yp2KLbBiQXs=	666666
23.	35325	2dJY5hIJ4FHioxG6CatHBw==	sunshine
24.	34963	1McuJ/7v9nE=	123321
25.	33452	yxzNxPIsFno=	letmein
26.	32549	dCgB24yq9Bw=	monkey
27.	31554	dA8D8OYD55E=	asdfgh
28.	28349	L8qbAD3jl3jSPm/keox4fA==	password1
29.	28303	zk8NJgAOqc4=	shadow
30.	28132	Ttgs5+ZAZM7ioxG6CatHBw==	princess
31.	27853	pTkQrKZ/JYM=	dragon
32.	27840	2aZl4Ouarwm52NYYI936YQ==	adobeadobe
33.	27720	NpVKrCM6pKw=	daniel
34.	27699	Dts8klglTQDioxG6CatHBw==	computer
35.	27415	4aiR1wv9z2Q=	michael

Quelle: stricture-group.com

PRAXIS Passwörter knacken



- Am Beispiel von ZIP-Dateien
- Knacken Sie die beiden Dateien:
  - http://cyber-security-lab.de/data/datei-ZipCrypto.zip
  - http://cyber-security-lab.de/data/datei-AES256.zip

Quelle: vdgsoftware.com

Quelle: pics-for-fun.com

Quelle: de.pinterest.com

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	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,	Id	7R
6	5=	mF	2n	XY	m:	f<	YH	mo	h4	7-
7	vT	ej	R:	+<	Vg	Nh	a9	6;	dJ	N{
8	d6	G7	p)	ek	pJ	mb	y2	e?	Jm	Rv

Passwortkarten

Link: sparkasse.de Passwort:

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,	Id	7R
6	5=	mF	2n	XY	m:	f<	YH	mo	h4	7-
7	vT	ej	R:	+<	Vg	Nh	a9	6;	dJ	N{
8	d6	G7	p)	ek	pJ	mb	y2	e?	Jm	Rv

Passwortkarten

Link: sparkasse.de Passwort: V=

Nr: 1 Kategorie: Online-Banking

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

Passwortkarten

Link: sparkasse.de Passwort: V=6<

Nr: 1 Kategorie: Online-Banking

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

Passwortkarten

Link: sparkasse.de Passwort: V=6<Bd

Nr: 1 Kategorie: Online-Banking

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

Passwortkarten

Link: sparkasse.de Passwort: V=6<BdG2

Nr: 1 Kategorie: Online-Banking

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

Passwortkarten

Link: sparkasse.de Passwort: V=6<BdG2W-

Nr: 1 Kategorie: Online-Banking

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

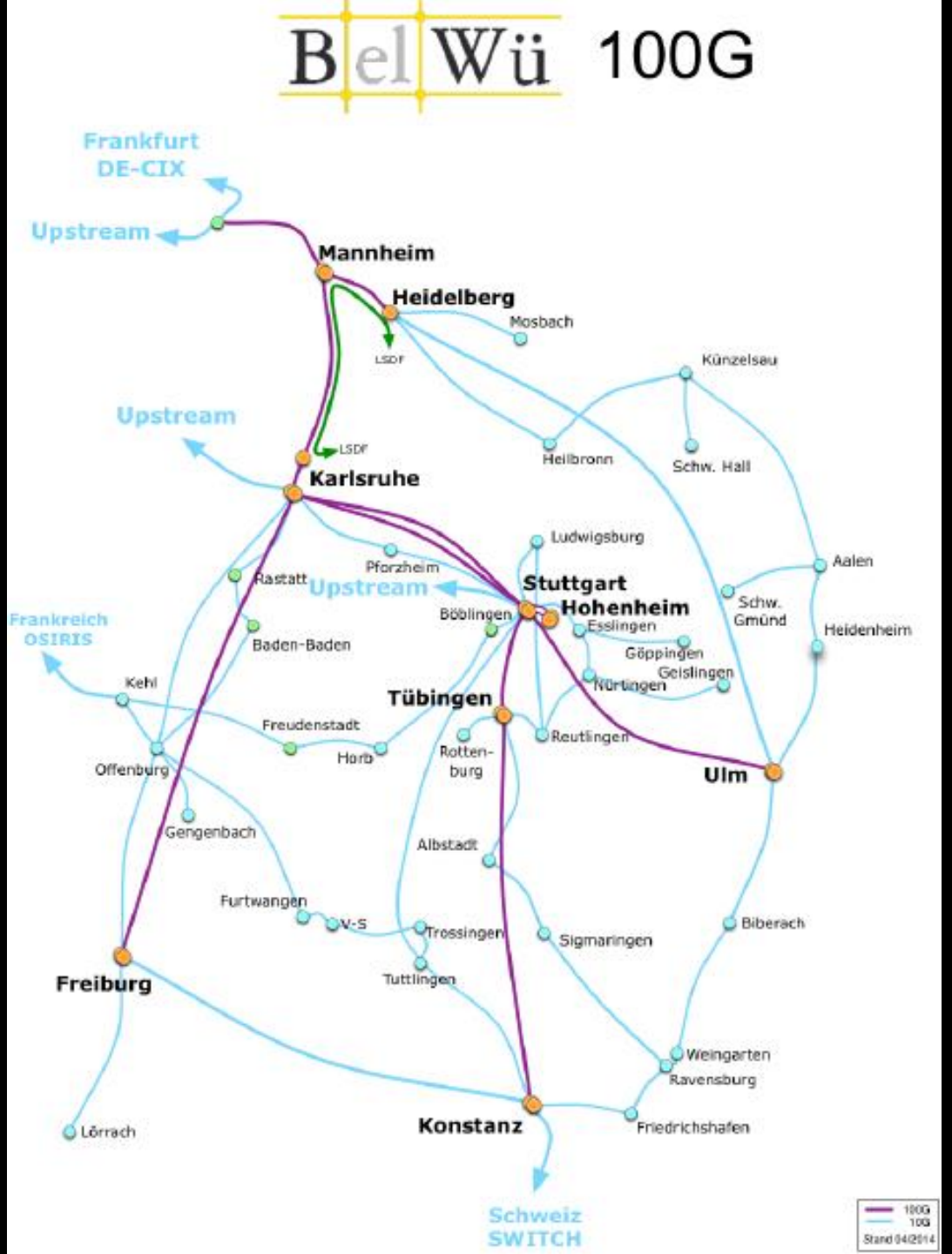
Sicher im Web

Neuartiger DDoS-Angriff

- Security-Journalist Brian Krebs war Ziel eines massiven DDoS-Angriffs
- Angriff mit bis zu 665 GBit pro Sekunde
- Botnetz bestand aus Routern, IP-Kameras und digitalen Videorekordern
- Internet of Things (IoT) Geräte

- Angriff auf OVH mit bis zu 1,1 Bit die Sekunde
- über eine Million infizierte Geräte

Quelle: heise.de

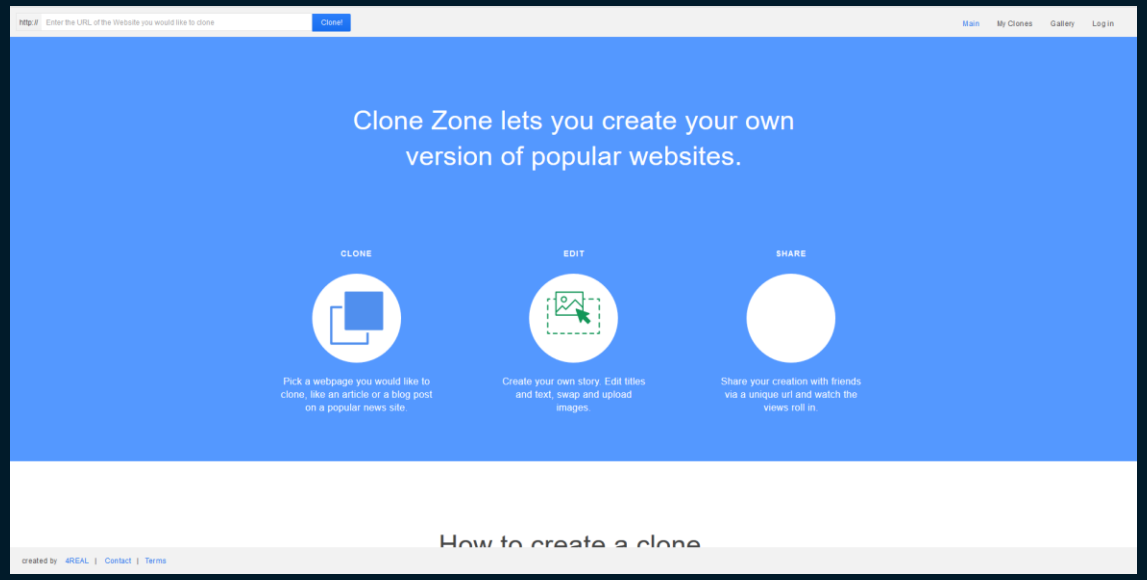

BelWü 100G
Frankfurt
DE-CIX
Upstream
Mannheim
Heidelberg
Mosbach
LSDF
Künzelsau
Upstream
LSDF
Heilbronn
Schw. Hall
Karlsruhe
Ludwigsburg
Pforzheim
Aalen
Rastatt
Upstream
Stuttgart
Hohenheim
Schw. Gmünd
Frankreich
OSIRIS
Böblingen
Esslingen
Heidenheim
Baden-Baden
Göppingen
Geislingen
Kehl
Nürtingen
Tübingen
Freudenstadt
Reutlingen
Rotten-
burg
Horb
Offenburg
Ulm
Gengenbach
Albstadt
Furtwangen
V-S
Trossingen
Sigmaringen
Biberach
Freiburg
Tuttlingen
Weingarten
Ravensburg
Lörrach
Konstanz
Friedrichshafen
Schweiz
SWITCH
100G
10G
Stand 04/2014

Cybercrime as a Service

Quelle: youtube.com

PRAXIS Websites manipulieren

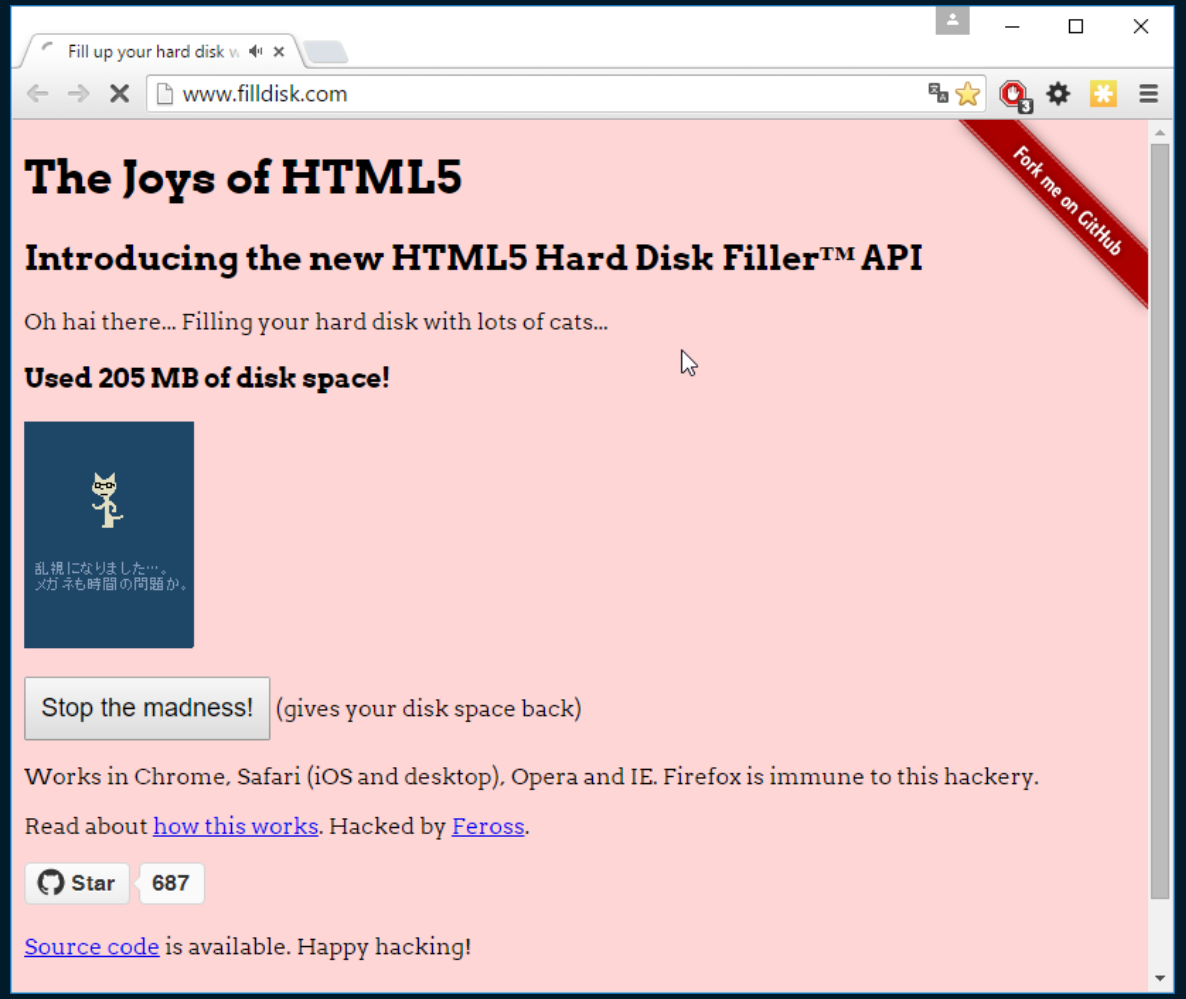
- Manipulation über Short-Link
  - Beispiel Short-Link: http://bit.ly/1E0kPOv
  - Anfällig bei der Verbreitung über soziale Netzwerke
  - Auf Smartphones spielt die URL eine untergeordnete Rolle



Quelle: tinyur1.co

PRAXIS HTML5 Hard Disk Filler

- Neue Webtechnologien führen zu weiteren Sicherheitsrisiken
- LocalStorage erlaubt bis zu 2.5, 5 oder 10 MB an Speicher pro Domain (von der Browserimplementierung abhängig)
- http://www.filldisk.com



PRAXIS Geteilte Fotos

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

http://metapicz.com

Quelle: heise.de

PRAXIS Browser sicherer machen

- Laden Sie den Portable Browser Firefox herunter und besuchen Sie die beiden Dienste https://amiunique.org und https://panopticlick.eff.org

- Konfigurieren Sie Firefox und installieren Sie die genannten Add-ons.
  - Anleitung: https://scheible.it/firefox-web-browser-security-tuning/

- Prüfen Sie, wie sich die genannten Websites bei aktiviertem / deaktiviertem Add-on unterschiedlich verhalten.

PRAXIS Ab ins Darknet

- Öffnen Sie den zur Verfügung gestellten TOR-Browser
- Surfen Sie auf eine Website und prüfen Sie, welche Verbindungsroute gewählt wurde
- Wechseln Sie ihre Identität
- Öffnen Sie die folgenden Hidden Services (Darknet-Websites):
  - http://3g2upl4pq6kufc4m.onion
  - http://vfqnd6mieccqyiit.onion

Quelle: heise.de

Hardware Tools

Keysweeper

Home | Video | Themen | Forum | English | DER SPIEGEL | SPIEGEL TV | Abo | Shop

SPIEGEL ONLINE NETZWELT

Politik | Wirtschaft | Panorama | Sport | Kultur | Netzwelt | Wissenschaft | Gesundheit | einestages | Karriere | Uni | Reise

Nachrichten > Netzwelt > Web > Internetkriminalität > Keysweeper: USB-Ladegerät schneidet Tastatureingaben mit

Keysweeper: Ladegerät schneidet Tastatureingaben mit

REUTERS

Anwender beim Tippen (Symbolbild): Ladegerät als Sicherheitsrisiko

Ein Sicherheitsforscher hat ein Ladegerät konzipiert, mit dem sich Eingaben auf kabellosen Tastaturen mitschneiden lassen. Auf Wunsch sendet es sogar Benachrichtungs-SMS an seinen Besitzer, wenn etwas Bestimmtes getippt wird.

Like 3m Follow @MailOnline DailyMail

Wednesday, Nov 4th 2015 10PM 8°C 1AM 7°C 5-Day Forecast

MailOnline Science & Tech

Home | News | U.S. | Sport | TV&Showbiz | Australia | Femail | Health | Science | Money | Video | Travel | Fashion Finder

Latest Headlines | Science | Pictures Login

The £6 'spy box' that tracks EVERYTHING you type: Hacker creates a USB charger that can steal banking details remotely

- KeySweeper device was created by security researcher Samy Kamkar
- The covert device looks, and works, like a typical USB wall charger
- It 'sniffs' and logs
- Device sends thes
- It can even alert a is typed, such as

Site Web Enter your search Search

Like Daily Mail | Follow @dailymailtech | Follow Daily Mail | +1 Daily Mail

heise Security News Hintergrund Tools Foren Kontakt

Security > News > 7-Tage-News > 2015 > KW 3 > USB-Ladegerät spioniert Funk-Tastaturen aus

« Vorige | Nächste »

USB-Ladegerät spioniert Funk-Tastaturen aus

14.01.2015 16:08 Uhr – Fabian A. Scherschel vorlesen

Dienste

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

Router auf WPS-Lücken testen

Viele WLAN-Router weisen die sogenannte PixieDust-Lücke auf, über die sich Angreifer ganz einfach Zugang zu Ihrem Netz verschaffen können. Kommen Sie denen zuvor und testen Sie Ihr eigenes Funknetz. Mehr…

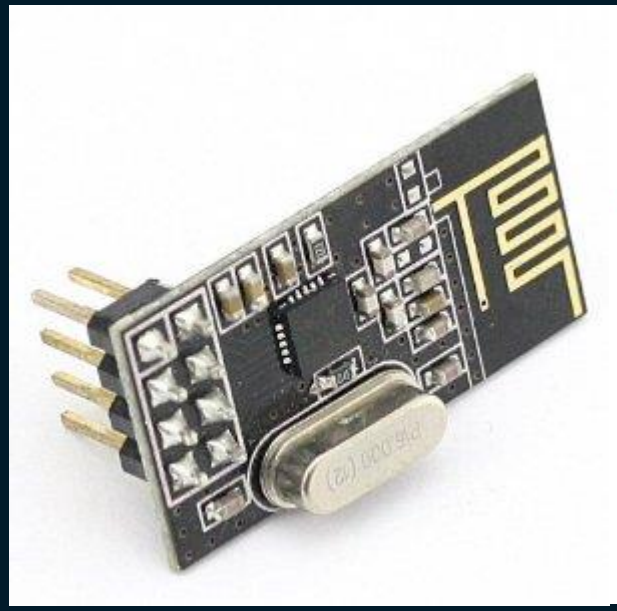
Analysiert: Google-Interna im Second-Hand-Shop

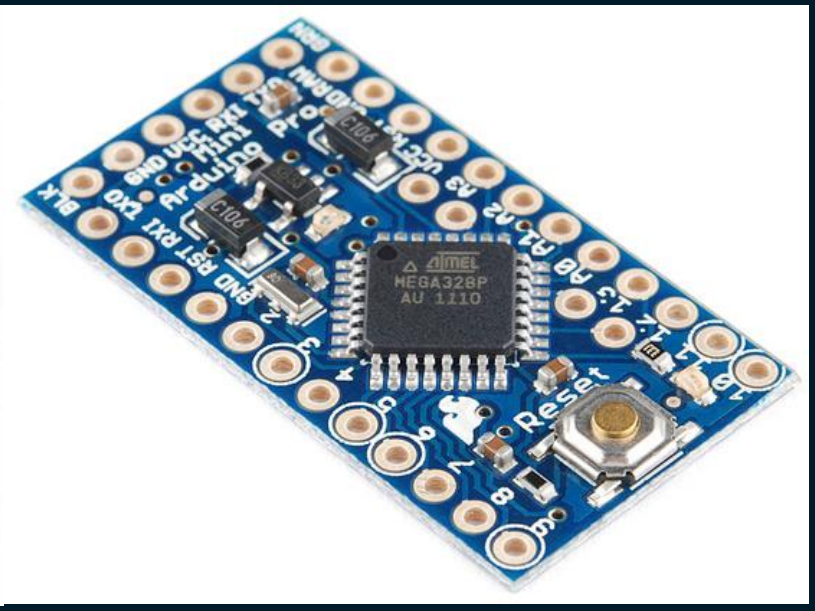
Ein in Deutschland gekaufter Gebraucht-

Keysweeper

- Das proprietäre und unverschlüsselte Protokoll eines Keyboards wurde per Reverse Engineering analysiert und „geknackt“
- Das Ergebnis basiert auf der Arbeit von Travis Goodspeed (goodfet.nrf), welche wiederum auf der Arbeit von Thorsten Schröder und Max Moser (KeyKeriki v2.0) basiert.
- Die Hardware besteht im Wesentlichen aus einem programmierbaren Mikrocontroller und dem 2,4 GHz Transceiver nRF24L01+
  - maniacbug‘s RF24-Bibliothek

Hardware





Quelle: miniinthebox.com

Quelle: sparkfun.com

Keysweeper Reverse Engineering für Anfänger

- Allgemeines Vorgehen:
  1. Gehäuse entfernen
  2. Funktion der Bauteile identifizieren
  3. Bauteil identifizieren
  4. Informationen zum Bauteil sammeln
  5. Blogs finden, die sich mit dem Bauteil/Protokoll/… beschäftigen

Keysweeper: Schwierigkeiten des Sniffings

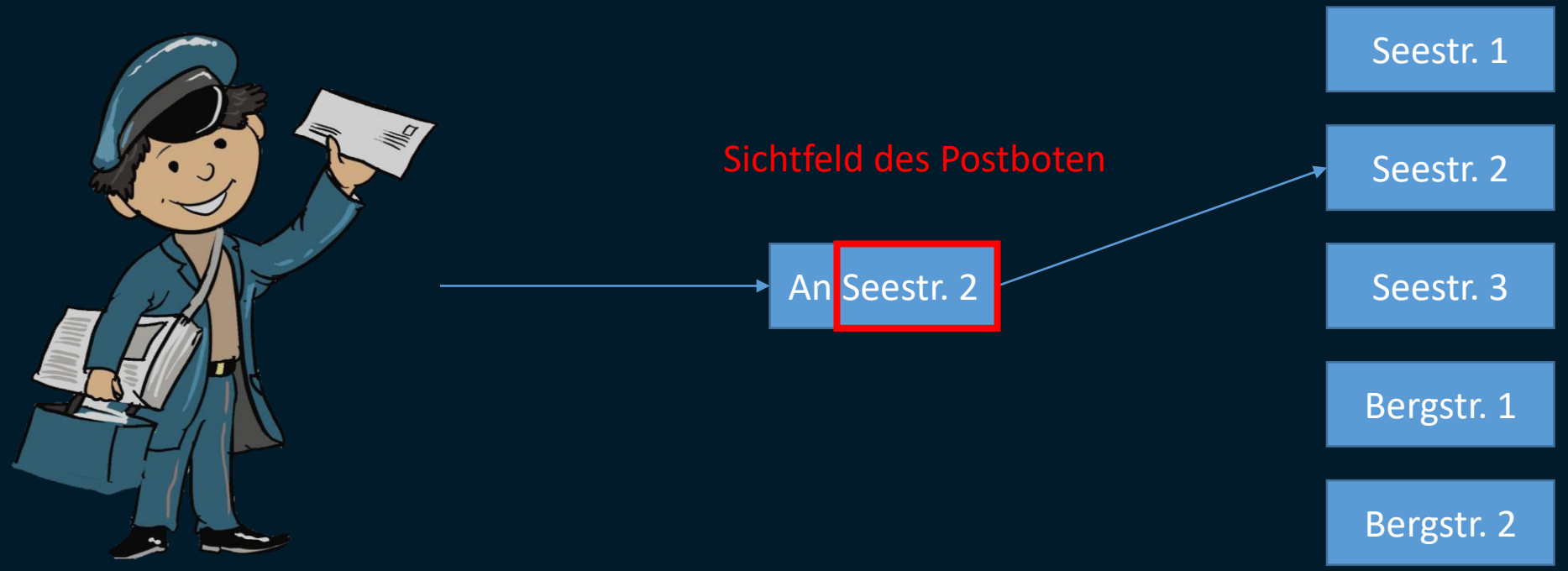
- Wir reden von 2,4 GHz, ABER es gibt mehrere Kanäle innerhalb der Frequenz
- Die Pakete werden gezielt versendet (MAC-Adressen)
- MAC-Adressen sind nicht bekannt
- Das Modul nRF24L01+ liefert nur Pakete, die gezielt an seine MAC-Adresse gesendet wurden

Keysweeper: Transceiver umfunktionieren

- Die MAC-Adresse wird entgegen dem Standard auf 2 Bytes verkürzt und auf die bekannte Preambel 0x00AA oder 0x0055 gesetzt, somit erhalte ich Pakete, die nicht für mich bestimmt sind.
- Die gesammelten Daten werden interpretiert und so die MAC-Adresse identifiziert

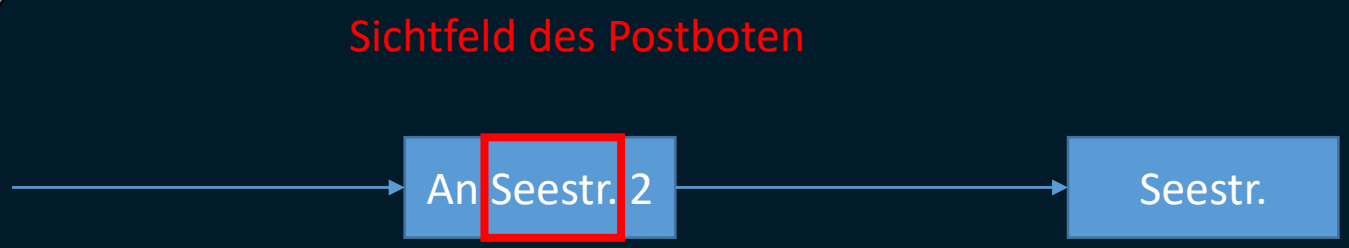
Keysweeper: Transceiver umfunktionieren

- Die MAC-Adresse wird entgegen dem Standard auf 2 Bytes verkürzt und auf die bekannte Preambel 0x00AA oder 0x0055 gesetzt, somit erhalte ich Pakete, die nicht für mich bestimmt sind.



Keysweeper: Transceiver umfunktionieren

- Die MAC-Adresse wird entgegen dem Standard auf 2 Bytes verkürzt und auf die bekannte Preambel 0x00AA oder 0x0055 gesetzt, somit erhalte ich Pakete, die nicht für mich bestimmt sind.



Keysweeper: Ablauf

- Von Frequenzbereich 2403 bis 2480 die MAC-Adresse 0x00AA und 0x0055 durchwechseln und schauen, ob man was „hört“
- Interpretation (Entschlüsselung) der Daten, wenn was Sinnvolles „reinkommt“

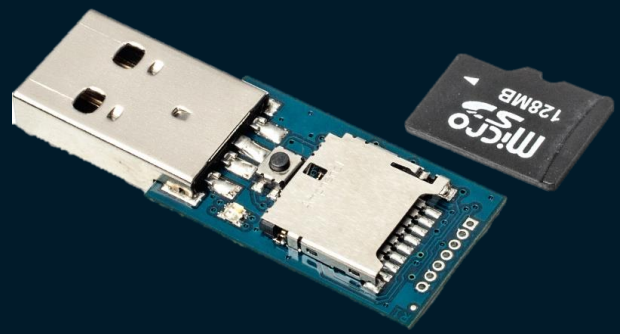
Keylogger

- Tastatureingabe mitprotokollieren
  - Eingaben vor dem Start des Betriebssystem werden erfasst
  - Nur wenige MB reichen für sehr lange Zeit
  - Daher sehr günstig herzustellen
- Moderne Varianten mit WLAN bzw. Funk

Quelle: amazon.com

Bad USB

- Sicherheitsrisiko:
  - Controller und Firmware in USB-Geräten
- Angriff:
  - HID (Maus, Tastatur, …) kann simuliert werden
  - Durch Eingaben können beliebige Aktionen in sehr kurzer Zeit durchgeführt werden



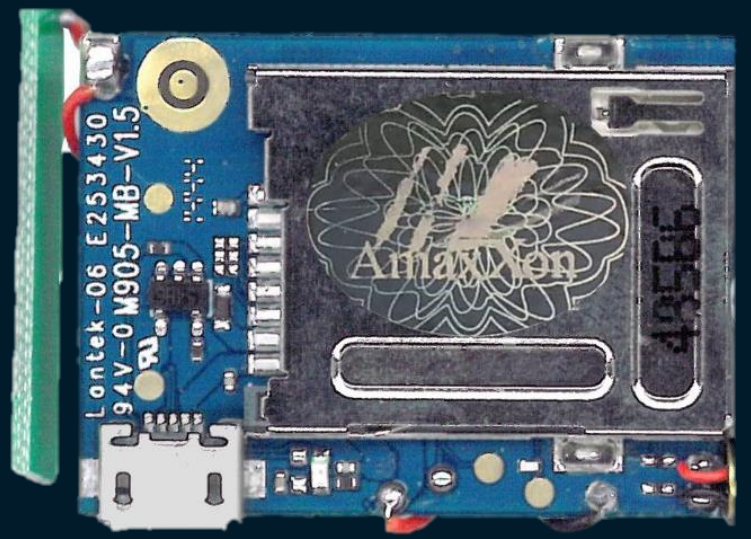
Quelle: coolcomponents.co.uk

Quelle: hachshop.com

Quelle: heise.de

GSM Wanzen

- Versteckte Überwachungselektronik
  - Sind frei verkäuflich
  - Kann in Geschenken versteckt sein
  - Kann in alltägliche Gegenstände versteckt sein
    - Computermäuse
    - Rauchmelder
    - Kugelschreiber
    - Feuerzeuge
    - …



Quelle: amazon.de

Störsender

- Unterbrechung von Funkverbindungen
  - Viele Frequenzen
    - GSM
    - UMTS
    - LTE
    - BlueTooth
    - GPS
    - …
  - Kann frei gekauft werden
  - Nutzung ist in Deutschland illegal

Quelle: pki-electronic.com

Quelle: shop-alarm.de

Vielen Dank

Präsentation online unter: https://scheible.it

Hochschule Albstadt-Sigmaringen

Fakultät Informatik

Bachelorstudiengänge
IT Security
Technische Informatik
Wirtschaftsinformatik

Masterstudiengänge
Business Analytics
Digitale Forensik
Systems Engineering
Data Science

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

Weitere Fakultäten

Business Science and Management
Betriebswirtschaft
Energiewirtschaft und Management

Engineering
Maschinenbau
Material and Process Engineering
Textil- und Bekleidungstechnologie
Wirtschaftsingenieurwesen

Life Sciences
Facility Management
Lebensmittel, Ernährung, Hygiene
Pharmatechnik