Hochschule
Albstadt-Sigmaringen

Albstadt-Sigmaringen University

Medientag
Live Hacking

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

Cyber Security

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

Quelle: pics-for-fun.com

Quelle: de.pinterest.com

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

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

Angriff auf den Fernsehsender TV5

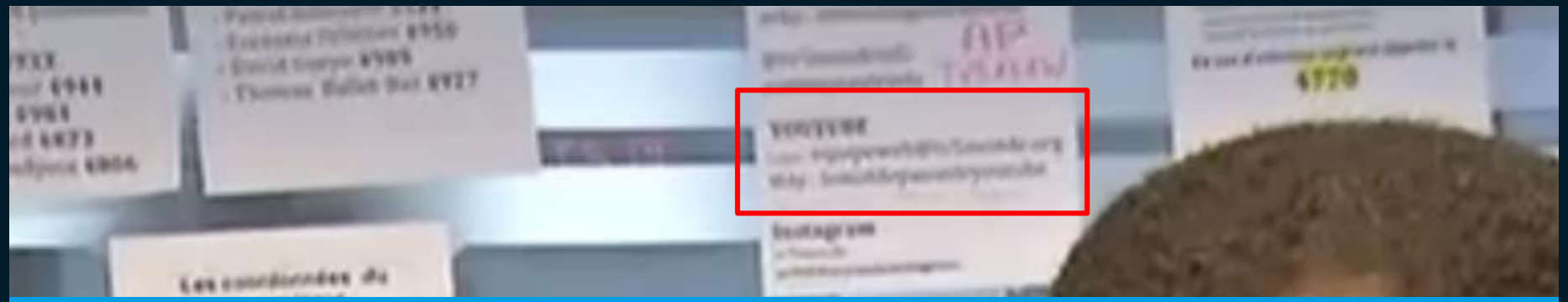
- Umfangreicher Angriff auf den französischen Sender TV5Monde
- Alle Kanäle des Fernsehunternehmens TV5Monde gingen offline
- Die Website verbreitete kurzfristig islamistische Drohungen
- Auf der Facebook-Seite wurden ebenfalls Drohungen verbreitet
- Spekulationen über öffentlich einsehbare Passwörter

Quelle: heise.de

Angriff auf den Fernsehsender TV5

Quelle: heise.de

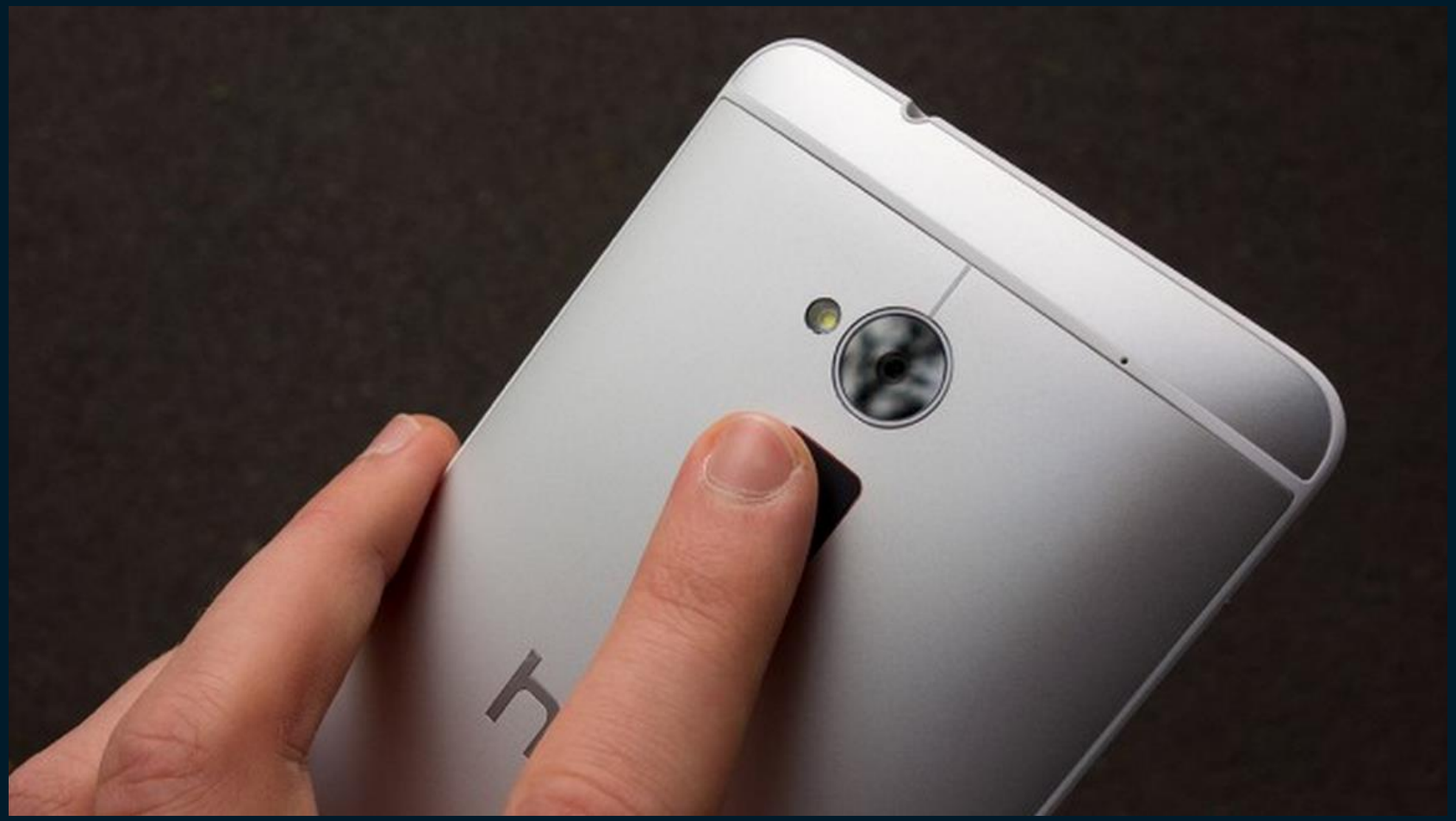
Angriff auf den Fernsehsender TV5



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

Quelle: heise.de

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

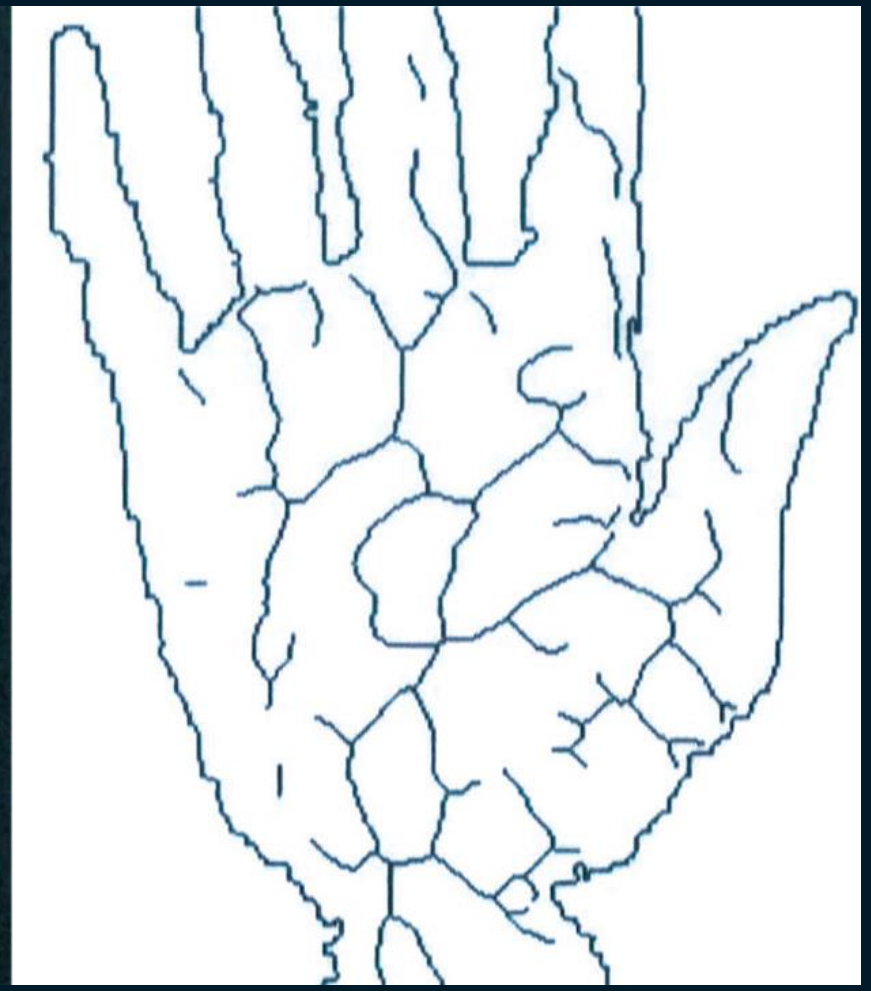
Fingerabdruck von Ursula von der Leyen

Quelle: heise.de

Venen-Scanner

Quelle: futerzone.at

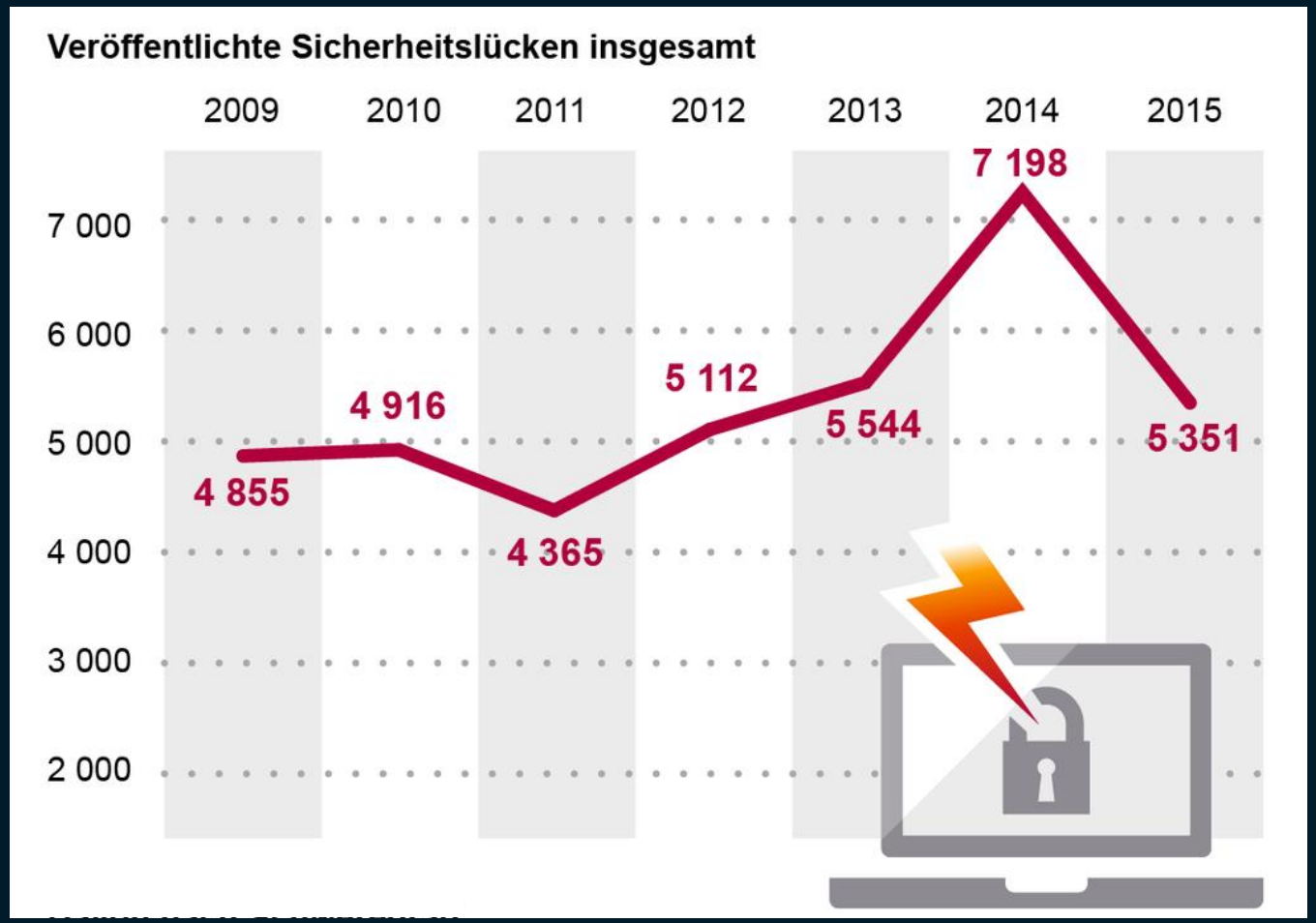
Venen-Scanner



Quelle: futerzone.at

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

Cyber Security Statistiken



Quelle: hpi.de

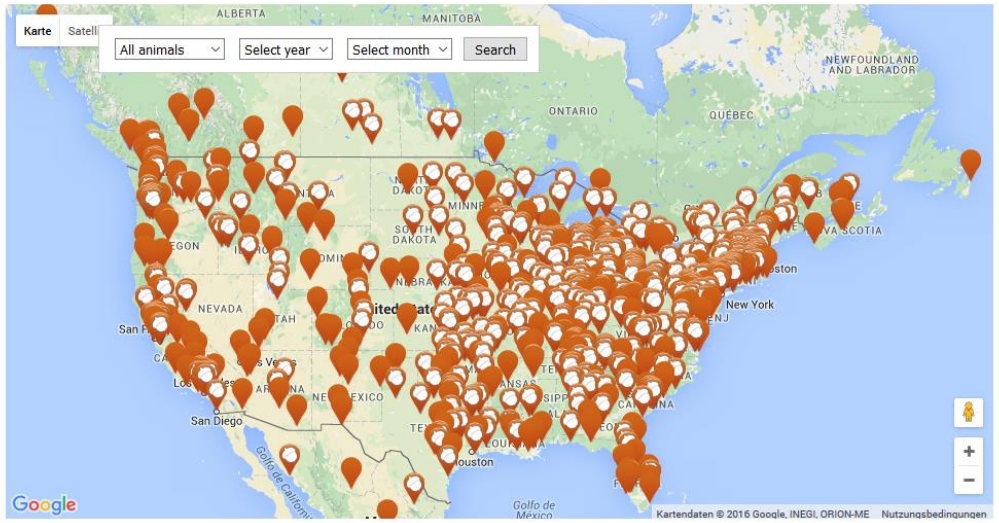
Größtes Sicherheitsrisiko?

Quelle: wikipedia.org

Größtes Sicherheitsrisiko?

Cyber Squirrel 1

Disrupting at the highest levels, its #CyberWar4Ever!



TOTAL SUCCESSFUL CYBER WAR OPS AS OF 2016.02.03 - 1139

Agent	Success
Squirrel	671
Bird	255
Racoon	54
Snake	48

ABOUT THIS MAP

This map lists all unclassified Cyber Squirrel Operations that have been released to the public that we have been able to confirm. There are many more executed ops than displayed on this map however, those ops remain classified.

Confirmation for all ops has been perserved by the Internet Archive's WayBack Machine whenever possible.

MOST RECENT UNCLASSIFIED OPS

Tweets may be blocked by your Ad blocker

More Tweets by @CyberSquirrel1

Quelle: cybersquirrel1.com

Größtes Sicherheitsrisiko?

Cyber Squirrel 1

Disrupting at the highest levels, its #CyberWar4Ever!

TOTAL SUCCESSFUL CYBER WAR OPS AS OF 2016.02.03 - 1139

Agent	Success
Squirrel	671
Bird	255
Racoon	54
Snake	48

ABOUT THIS MAP

This map lists all unclassified Cyber Squirrel Operations that have been released to the public that we have been able to confirm. There are many more executed ops than displayed on this map however, those ops remain classified.

Confirmation for all ops has been perserved by the Internet Archive's WayBack Machine whenever possible.

MOST RECENT UNCLASSIFIED OPS

Tweets may be blocked by your Ad blocker

More Tweets by @CyberSquirrel1

Quelle: cybersquirrel1.com

Sicher im Netz

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.

Quelle: heise.de

PRAXIS Geteilte Fotos

- Fotos, die mit dem iPhone, Android Smartphone oder mit einer Digitalkamera gemacht, 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

- Öffnen Sie den zur Verfügung gestellten Portable Browser Firefox und rufen Sie die Seite http://mybrowserinfo.com

- Installieren Sie die genannten AddOns.
  - Random Agent Spoofer
  - uBlock Origin

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

Quelle: heise.de

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

Passwortsicherheit

Passwortsicherheit

Quelle: youtube.com

Passwortsicherheit

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

Top 100 Adobe Passwords with Count

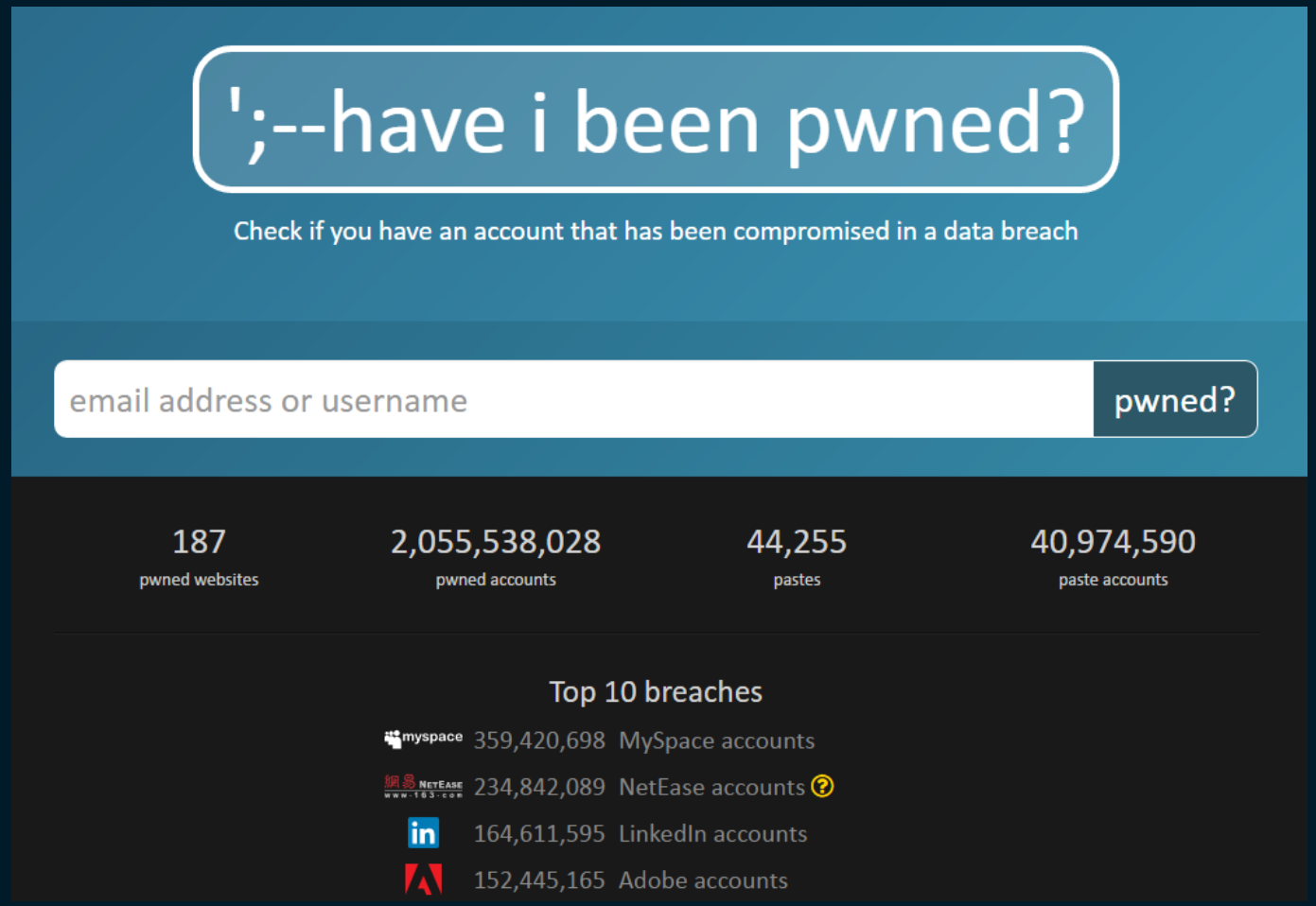
We do not (yet) have the keys Adobe used to encrypt the passwords of 130,324,429 users affected by their most recent breach. However, thanks to Adobe choosing symmetric key encryption over hashing, selecting ECB mode, and using the same key for every password, combined with a large number of known plaintexts 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	xz6PIeGzp6g=	aaaaaa

Quelle: stricture-group.com

PRAXIS Passwort geleakt?



Quelle: https://haveibeenpwned.com/

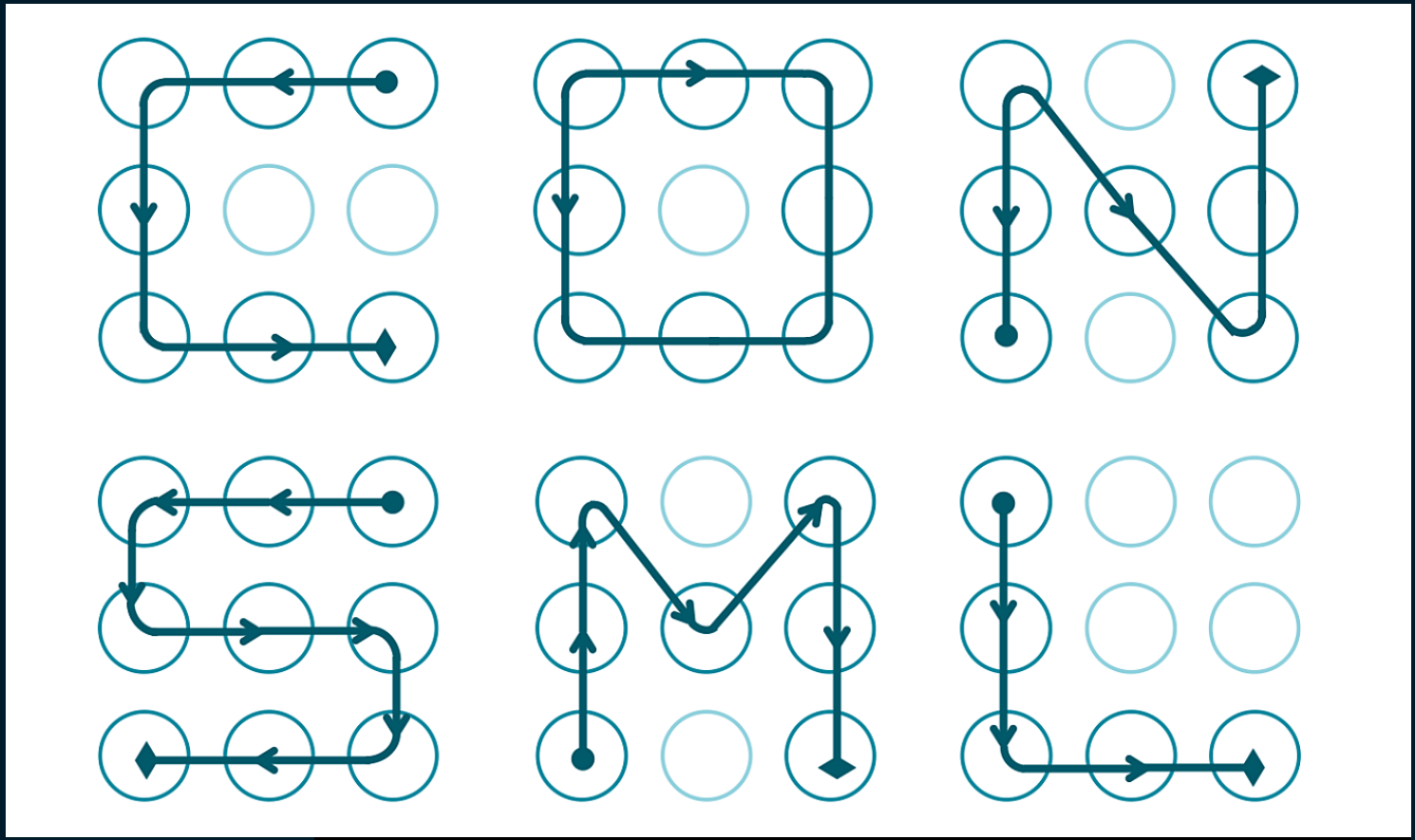
Bad Passwords – Bad Lock Patterns

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

Quelle: http://technic-al.com/advice/internet/how-bad-is-your-password/

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
- Muster von links → rechts; oben → unten werden häufig verwendet



Quelle: http://arstechnica.com/security/2015/08/new-data-uncovers-the-surprising-predictability-of-android-lock-patterns/

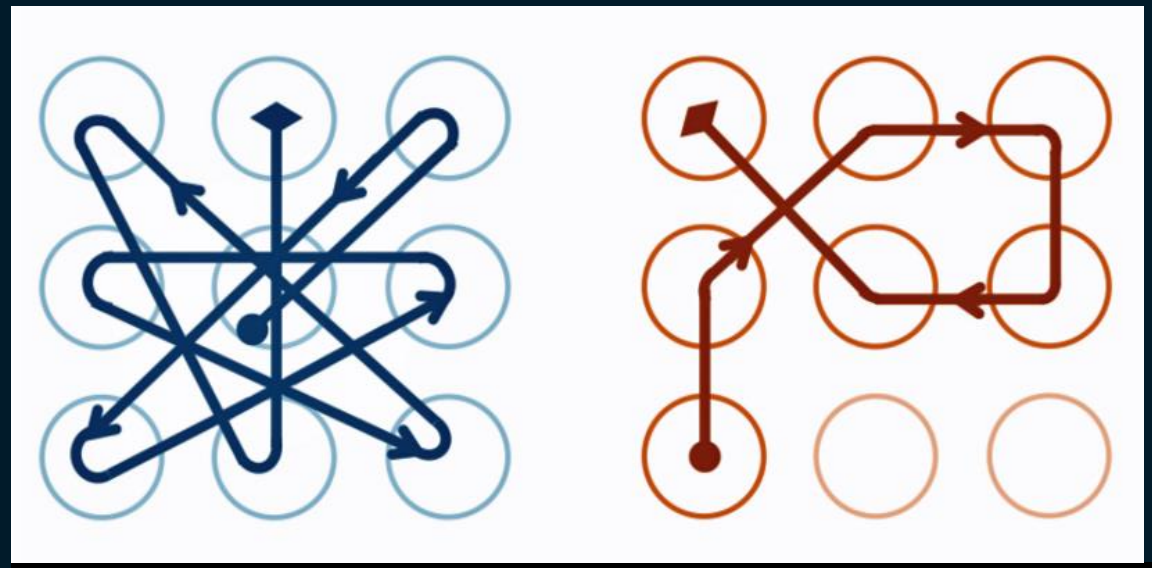
Lock Patterns vs. PINs-Kombinationsmöglichkeiten

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

Unter Android: Fünf Versuche möglich, dann 30 Sekunden Penalty
Das bedeutet: Ein 5-stelliges Wischmuster lässt sich in ~ 12 Stunden knacken (ein 4- oder 5-stelliges in ~15 Stunden) / Ein 4-stelliger Pin ist in ~17 Stunden knackbar

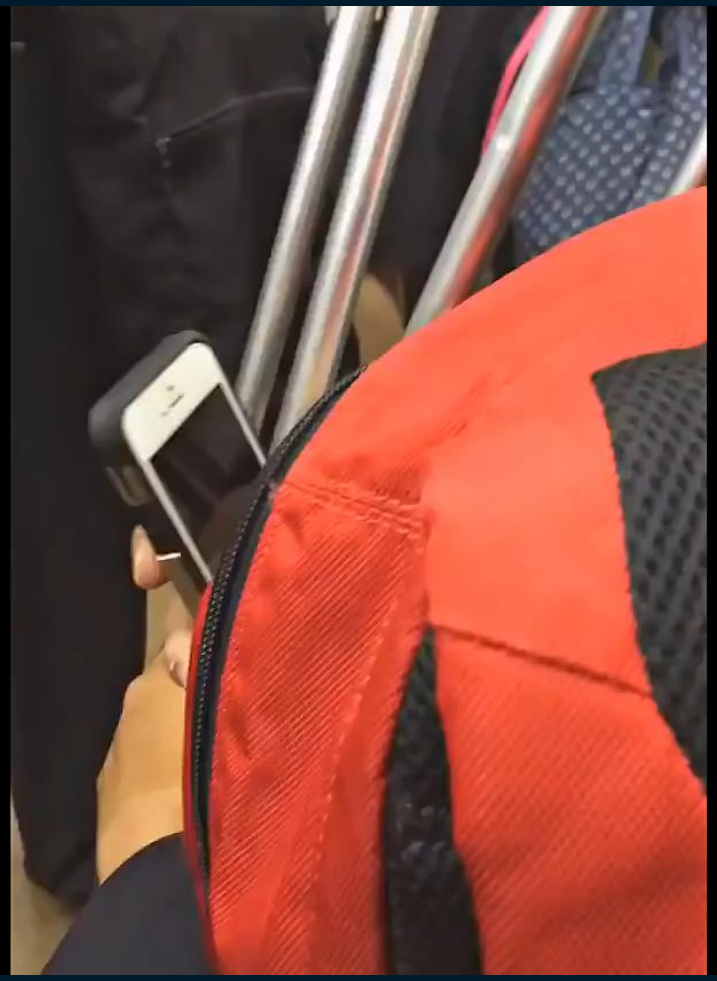
Bad Lock Patterns - Gegenmaßnahmen

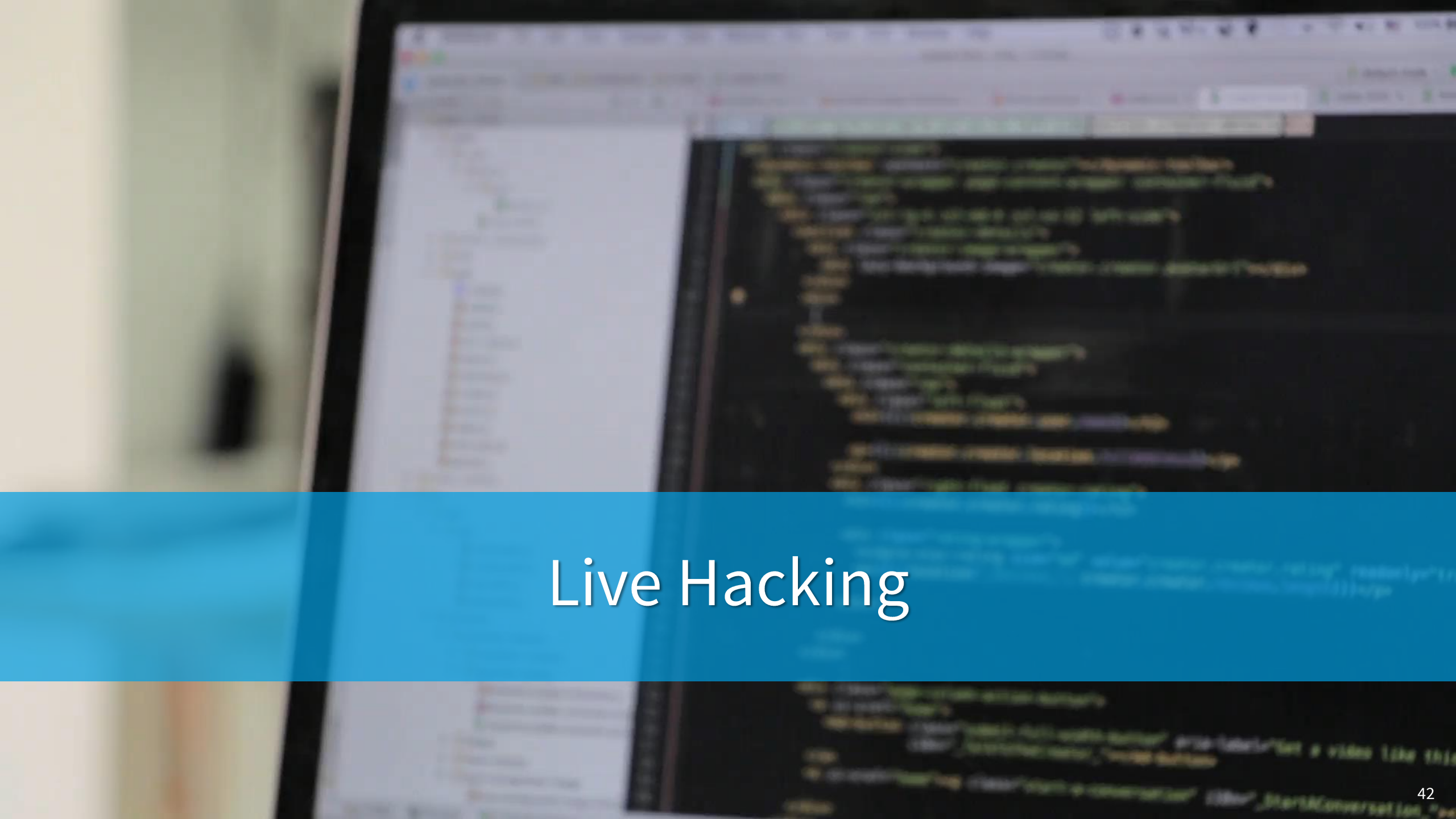
- Komplizierte Muster verwenden
- Allerdings sind weitere mögliche Angriffsvektoren vorhanden:
  - Angriffe über ADB (Android Debug Bridge)
- Lange PINs verwenden



Quelle: http://arstechnica.com/security/2015/08/new-data-uncovers-the-surprising-predictability-of-android-lock-patterns/

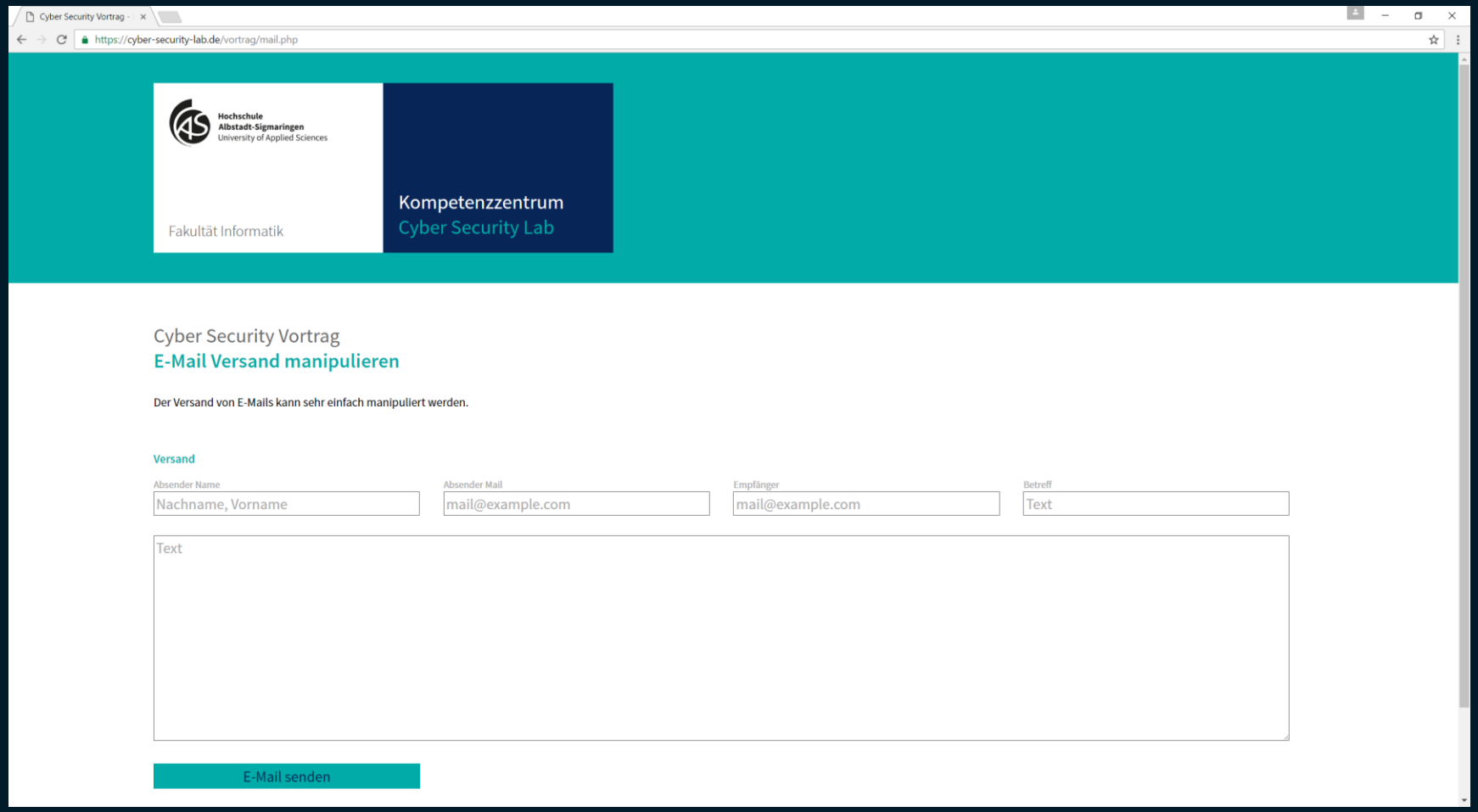
Bad Lock Patterns - Gegenmaßnahmen



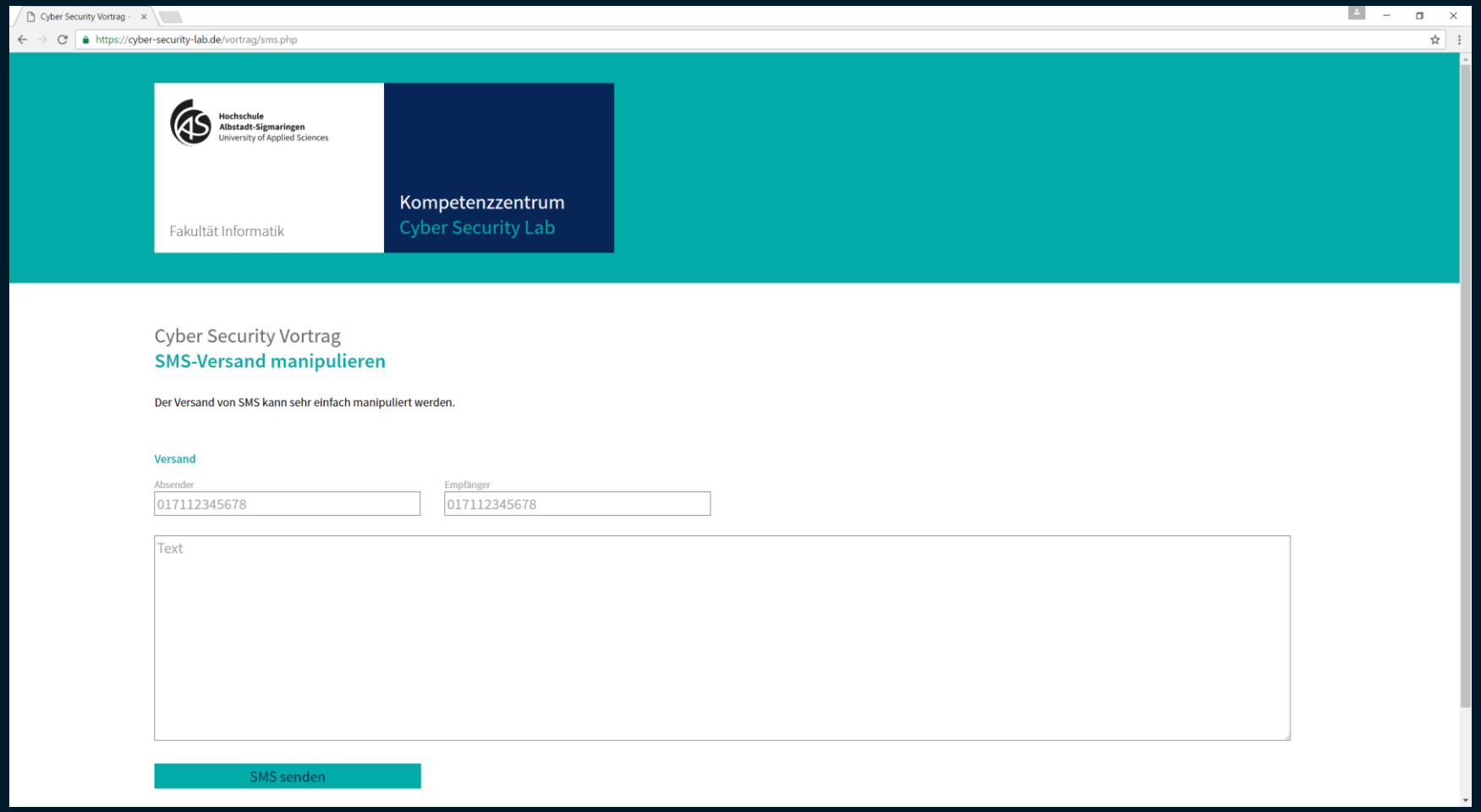


Live Hacking

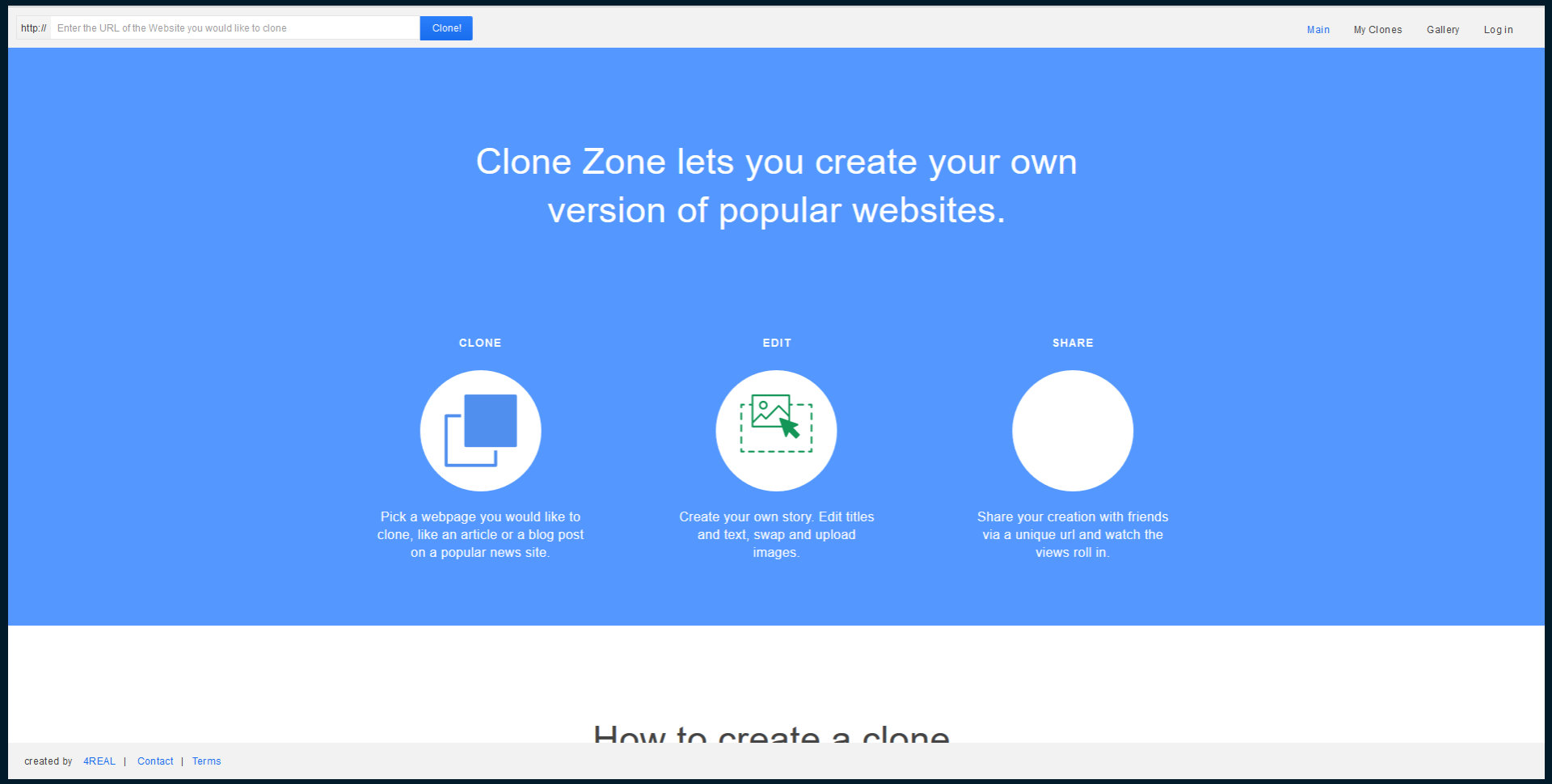
E-Mail-Versand manipulieren



SMS-Versand manipulieren



PRAXIS Website manipulieren



Quelle: clonezone.link

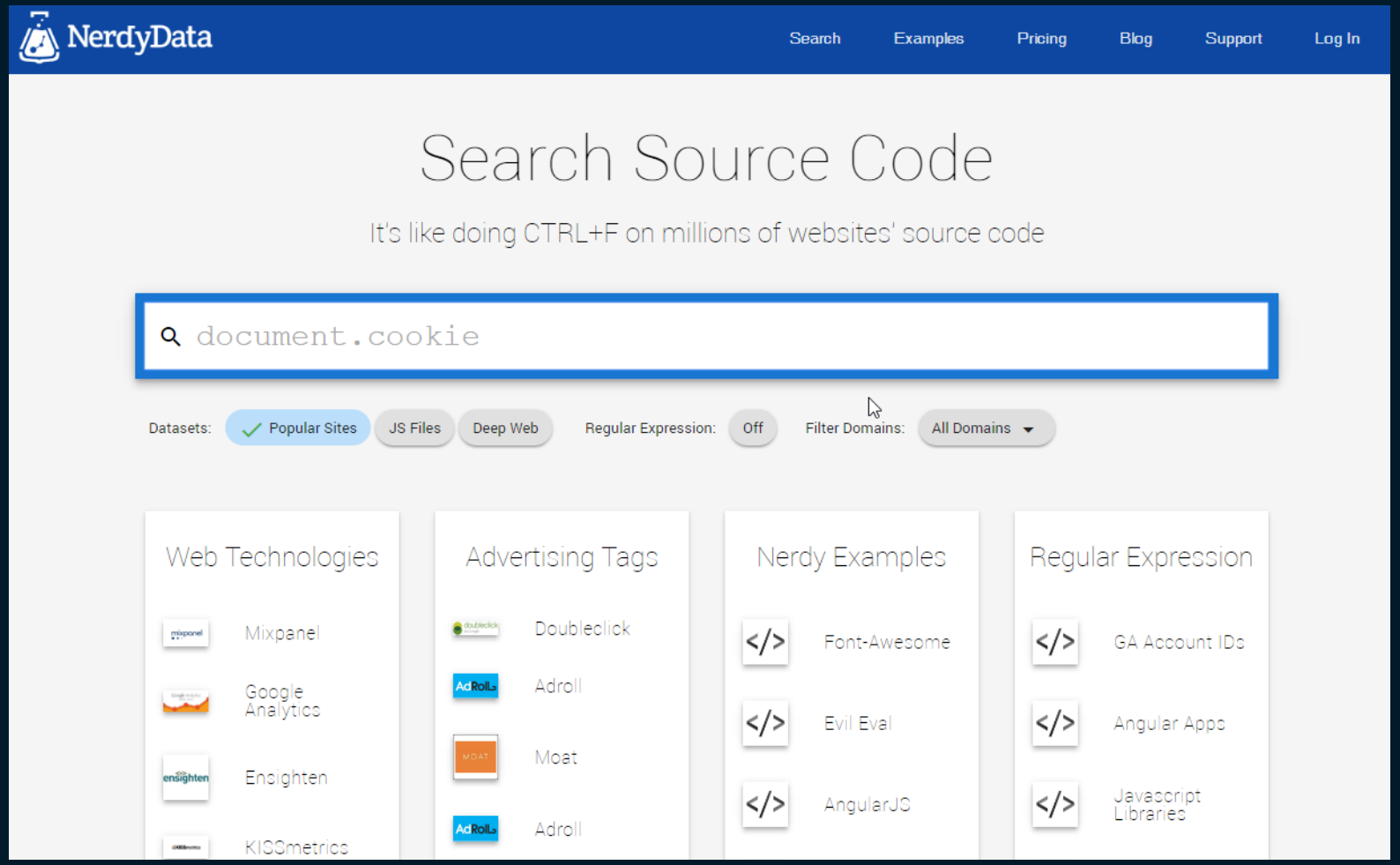
Google als Hacking-Tool

Quelle: google.de

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
- GHDB – the Google Hacking DataBase

Onlineshops manipulieren



Quelle: nerdydata.com

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 Consulter | 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…

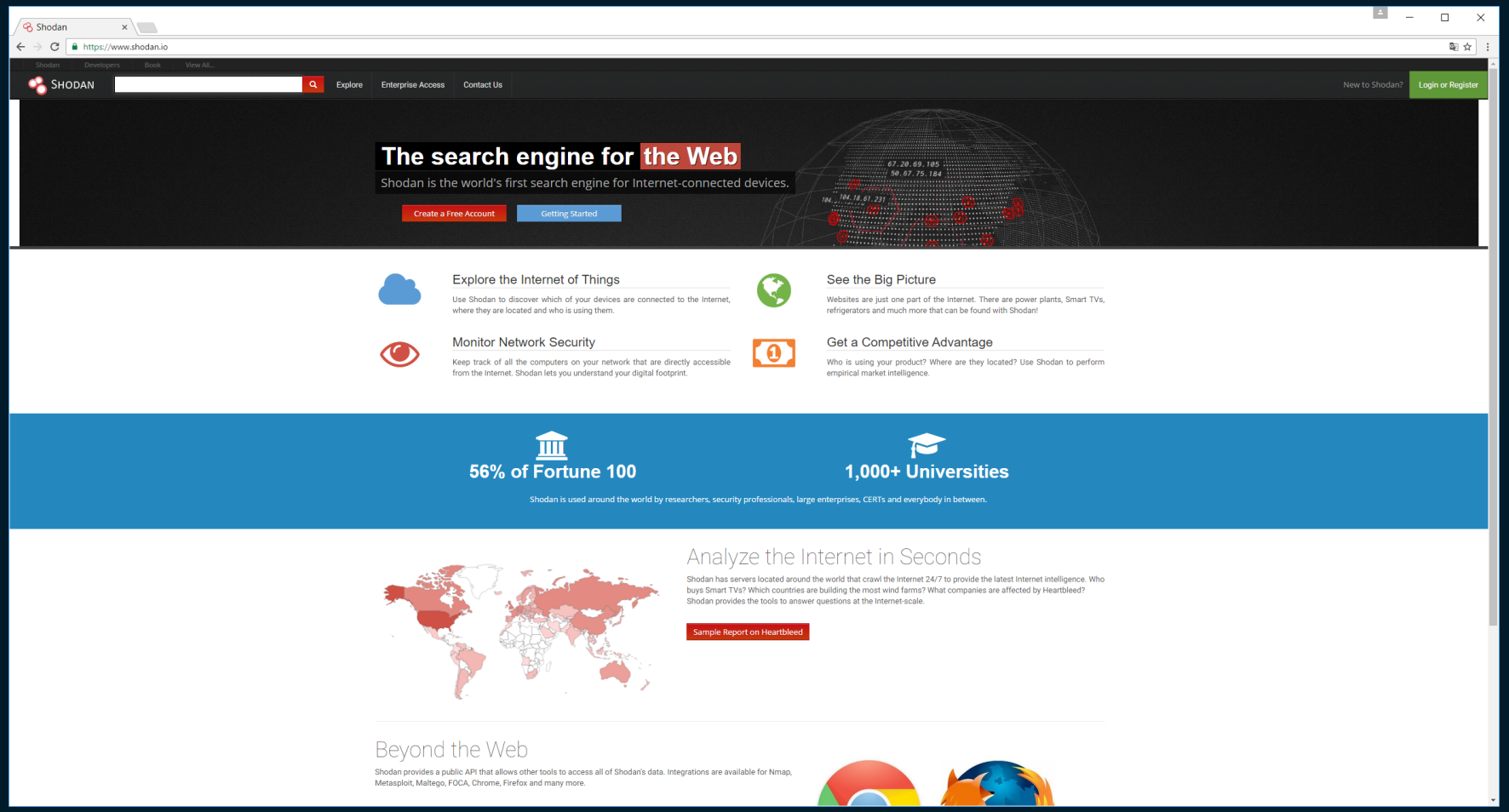
Analysiert: Lego Mindstorms für Cyber-Angriffe missbraucht

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

Quelle: heise.de

Suchmaschine für das Internet der Dinge



Quelle: shodan.io

PRAXIS Web Demo Plattform

- Öffnen Sie die Web Demo Plattform (Link auf dem PDF)
- Wir fangen mit den ersten Übungen an…

Vielen Dank

Präsentation online unter http://cyber-security-lab.de