CCVOSSEL

We know IT.

CCVOSSEL
We know IT.

Lassen Sie sich nicht erpressen!

Proaktiver Cyber-Security Schutz im Jahr 2017

CCVOSSEL
We know IT.

Aktuelle Sicherheitslage

Aktuelle Sicherheitslage

Cyberangriffe Weltweit

CCVOSSEL
We know IT.

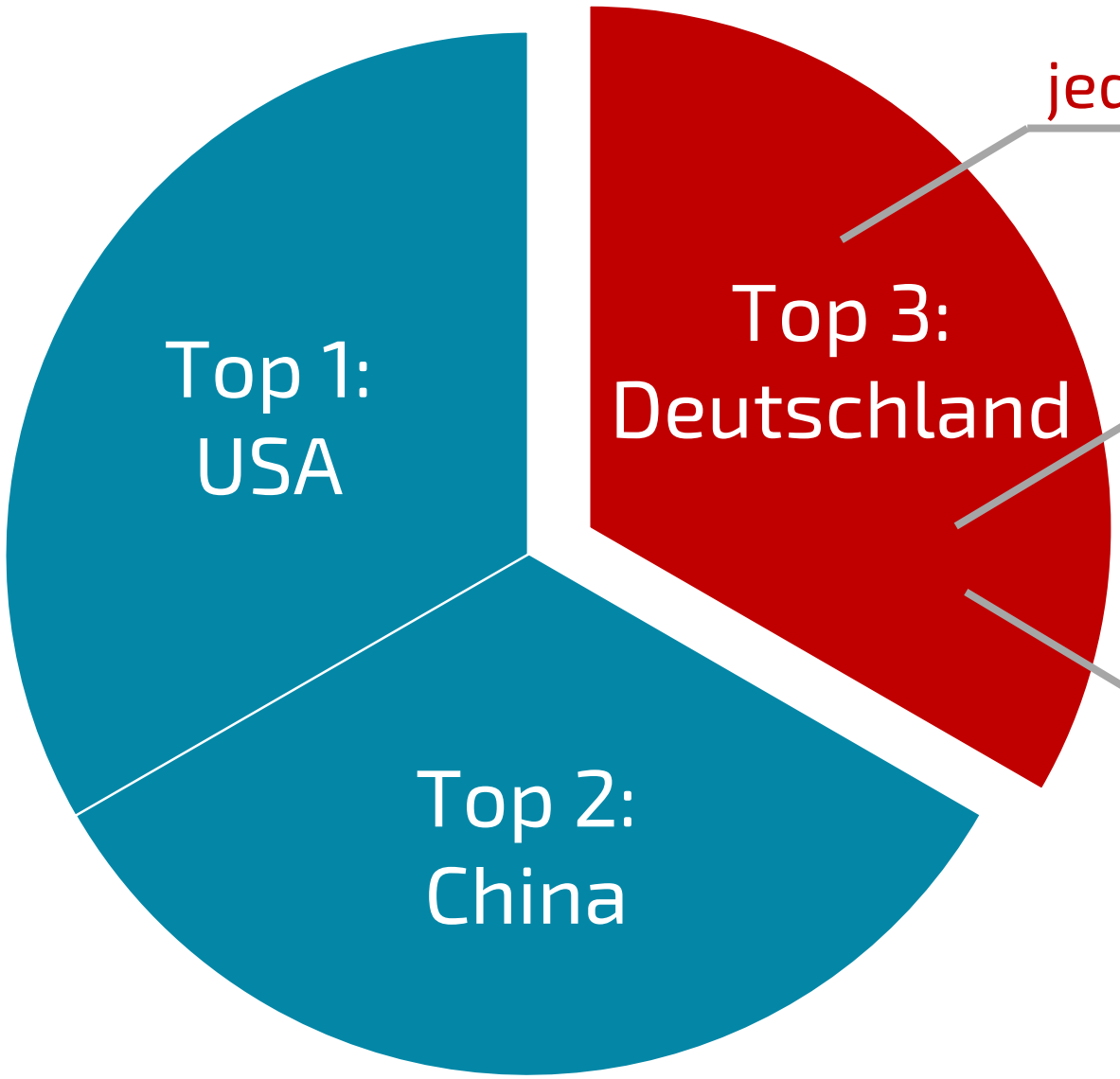
Aktuelle Sicherheitslage

Unvorstellbar viele Angriffspunkte

Aktuelle Sicherheitslage

CCVOSSEL
We know IT.

Top 3 Länder mit infizierten Rechnern



jede **40.** Website ist infiziert

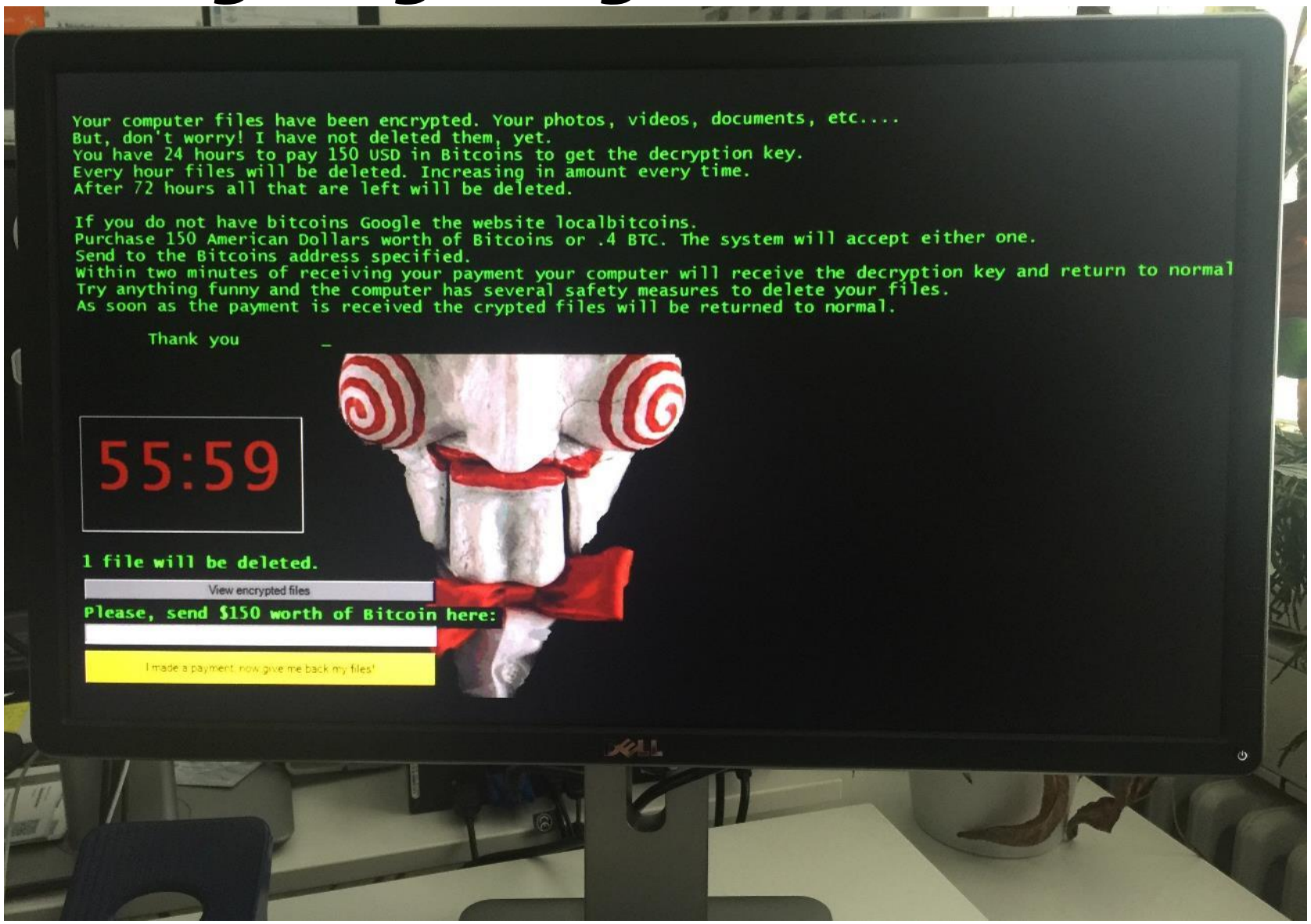
durchschnittliche Dauer bis zur Erkennung: **140 Tage**

51% der Unternehmen sind Opfer von Cyber-Crime

Quelle: Microsoft, Stand 03/2017

Aktuelle Sicherheitslage

Schlagartig steigende Zahl von Ransomware



Quelle: Foto eines Testrechners mit der Ransomware „Jigsaw“ der CCVOSSEL GmbH

Privatpersonen

150$ - 10.000$

Unternehmen

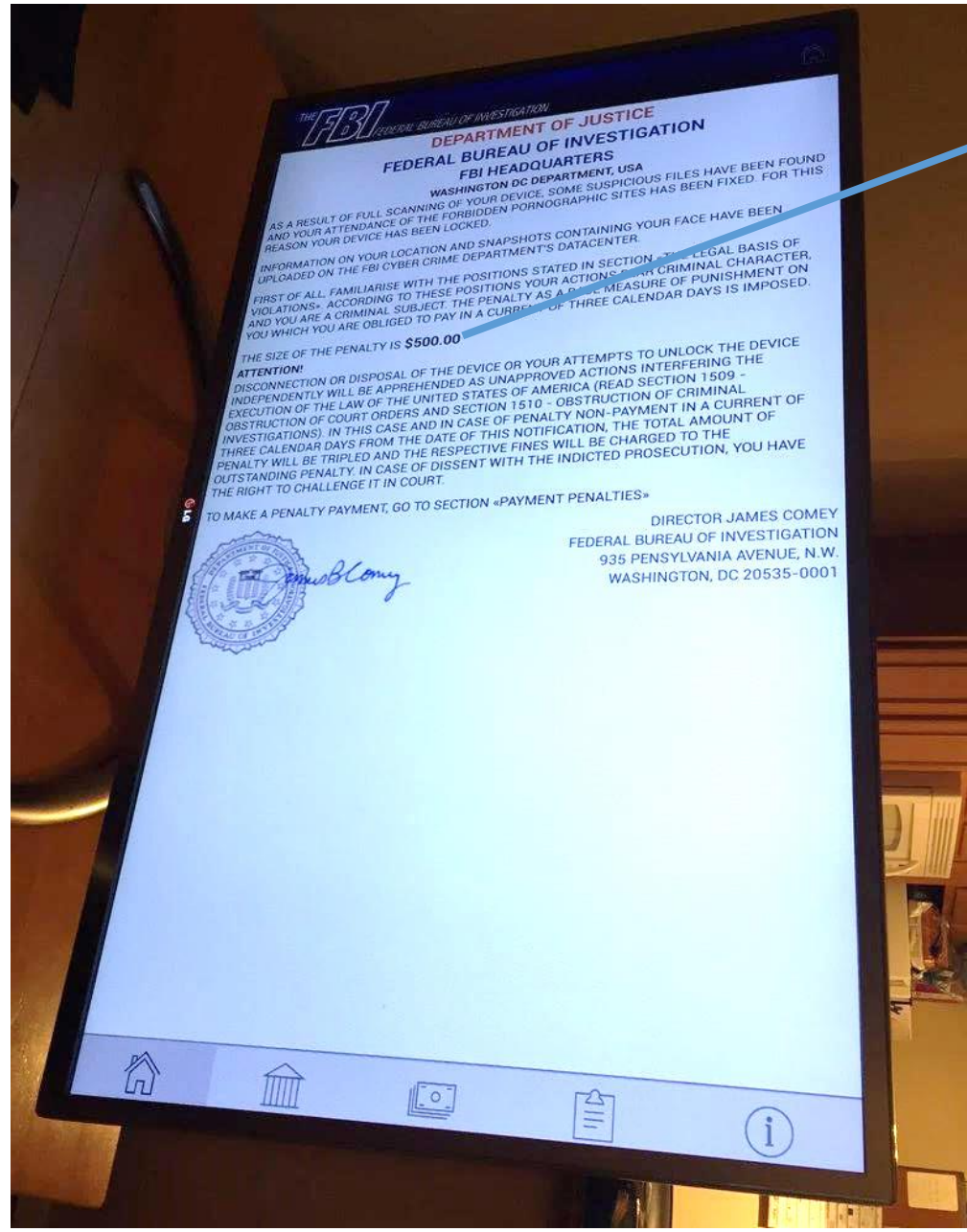
>50%:
10.000$ - 50.000$

70% der Opfer bezahlen!

Aktuelle Sicherheitslage

Quiz?

Ramsomware



Quelle: Darren Cauthon Twitter Blog, 25.12.2016

Aktuelle Sicherheitslage

Jegliche Websites im Visier

Quellen: Original-Screenshots der Webseiten im März 2017 (URLs im jeweiligen Screenshot ersichtlich)

Aktuelle Sicherheitslage

Angriffe auf Websites

CCVOSSEL
We know IT.

zone-h
unrestricted information

Home News Events Archive Archive Onhold Notify Stats Register Login search...

[ENABLE FILTERS]

Total notifications: **1,871** of which **578** single ip and **1,293** mass defacements

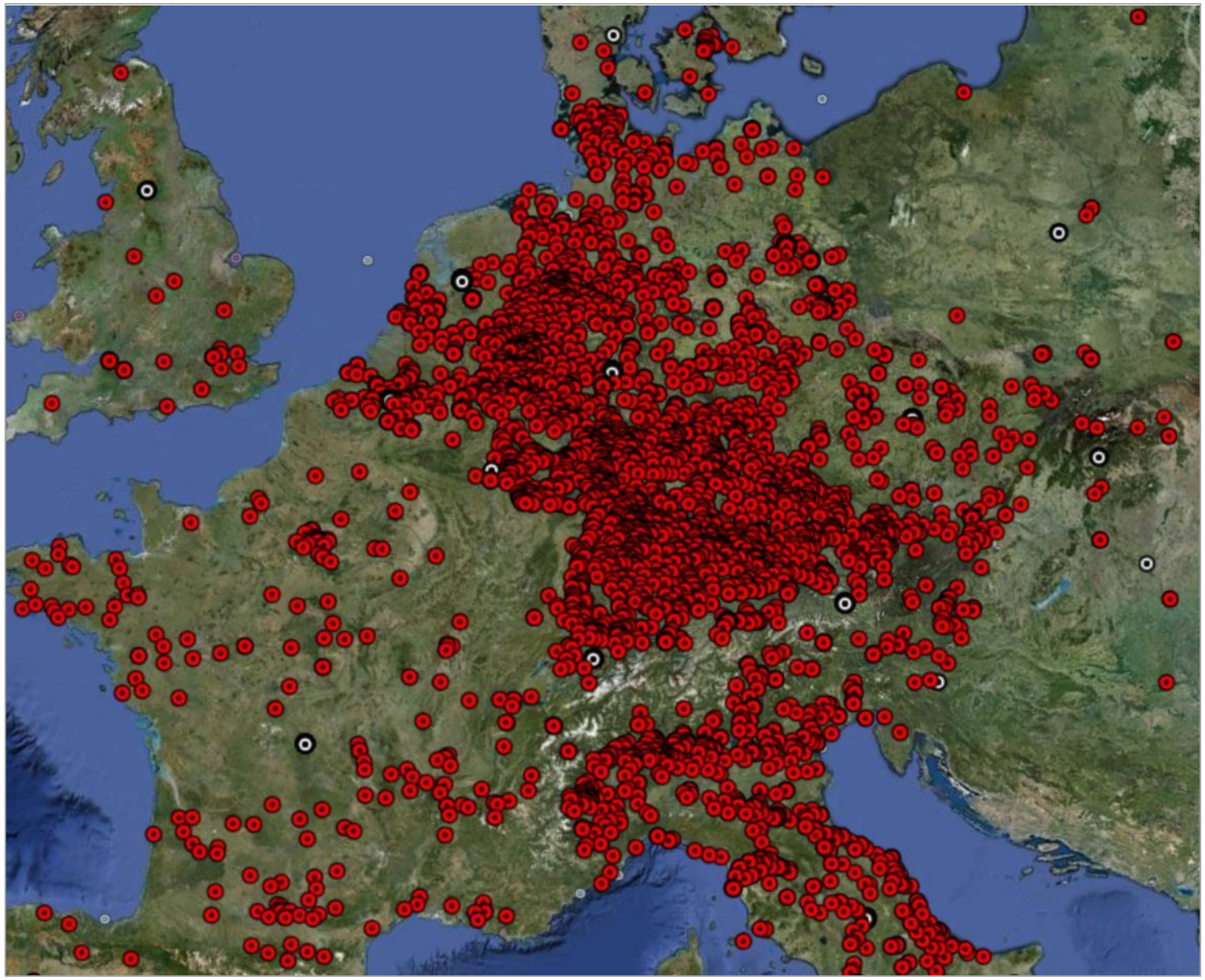
Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

Time	Notifier	H	M	R	L	★	Domain	OS	View
20:03	TeaM_CC	H					www.arandacommunications.com	Linux	mirror
20:03	m1ndburn3d	H					www.cvq.edu.mx	Linux	mirror
19:54	ByQuark	H					oftalmologiasos.com.ve	Linux	mirror
19:54	Mafia Hacking Team		M				dsp.co.ir/AllContents/	Unknown	mirror
19:54	Mafia Hacking Team		M				delta-logistics.com.vn/images/...	Win 2003	mirror
19:53	BD GREY HAT HACKERS	H					speakfortheunborn.com	Unknown	mirror
19:53	BD GREY HAT HACKERS	H					esrh.org	Linux	mirror
19:52	./UnIX		M				indianmovies.com/aceh-boys.html	FreeBSD	mirror
19:52	./UnIX		M				www.countrywidegroup.net/aceh-...	Win 2008	mirror
19:52	./UnIX	H	M				www.childreninnaturensw.com.au	Unknown	mirror

Aktuelle Sicherheitslage

CCVOSSEL
We know IT.

Öffentlich erreichbare Industriesteueranlagen in Europa



ICS Systeme online in Europa lt. https://cyberarms.files.wordpress.com/2013/03/scada-systems-europe.png (Stand 2013)

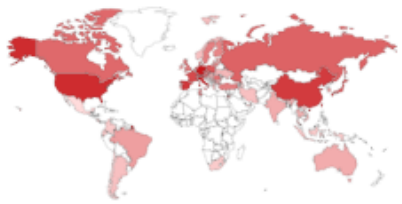
Aktuelle Sicherheitslage

Suchmaschine mal anders - Shodan

SHODAN

simatic

TOP COUNTRIES



Taiwan, Prov...	194
Germany	174
Italy	130
United States	120
Spain	99

Total results: 1,561

80.14.173.141

LStLambert-656-1-123-141.w80-14.abo.wanadoo.fr

Orange

Added on 2017-03-07 20:32:06 GMT

France

Details

ics

```
Copyright: Original Siemens Equipment
PLC name: SIMATIC 300
Module type: CPU 315-2 DP
Unknown (129): Boot Loader                A
Module: 6ES7 315-2AH14-0AB0  v.0.4
Basic Firmware: v.3.3.2
Module name: CPU 315-2 DP
Serial number of module: S C-C4UR95612012
Plant identification:
Basic Hardware: 6ES7 3...
```

Quelle: https://www.shodan.io

Aktuelle Sicherheitslage

IoT-Geräte unsicher, ein Beispiel:

EASY HOME®

WIFI Steckerset

- Bestehend aus WIFI Adapter und Funkadapter
- Für innen oder außen

Produkt Info

je Set 19,99*

Quelle: Auszug aus Prospekt von Aldi-Süd, https://www.aldi-sued.de, Angebot vom 17.09.2016

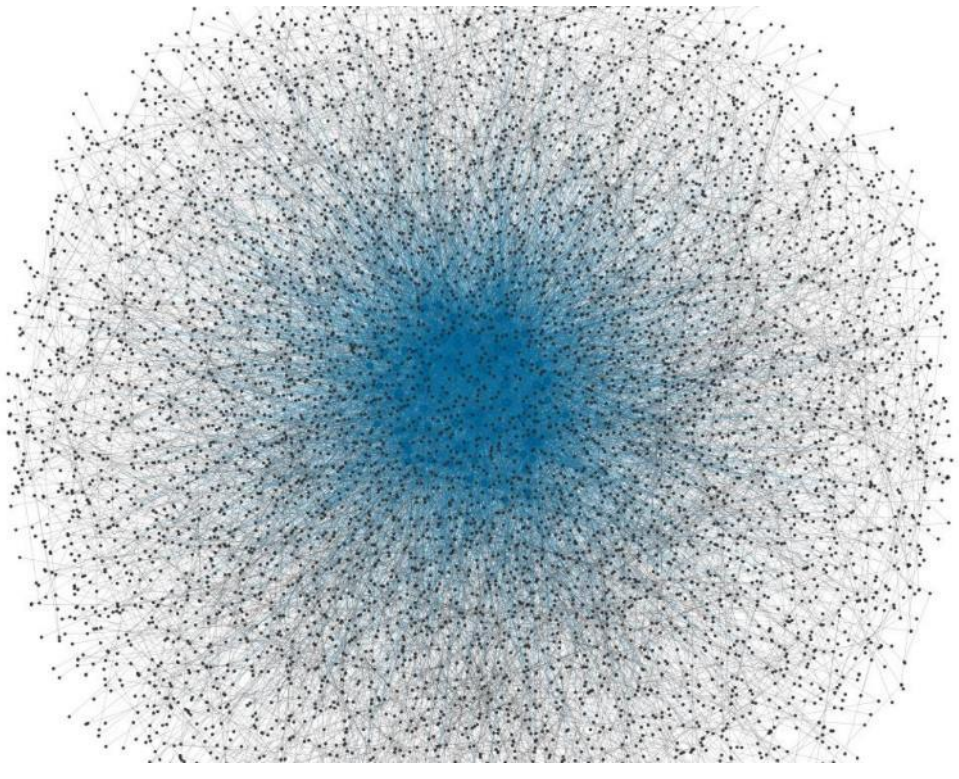
Quelle: Rainer W. Gerling, Max-Planck-Gesellschaft, DFN-Konferenz 02/2017
Zugriff auf Port 80 des Easy Home Gerätes,
Username: admin Passwort: admin

Aktuelle Sicherheitslage

Riesige Botnetze

Aufbau und Geschäftsmodell

- Ausführung beliebiger Schadprogramme gesteuert vom Bot-Master
- Zeitweise Vermietung als Geschäftsmodell

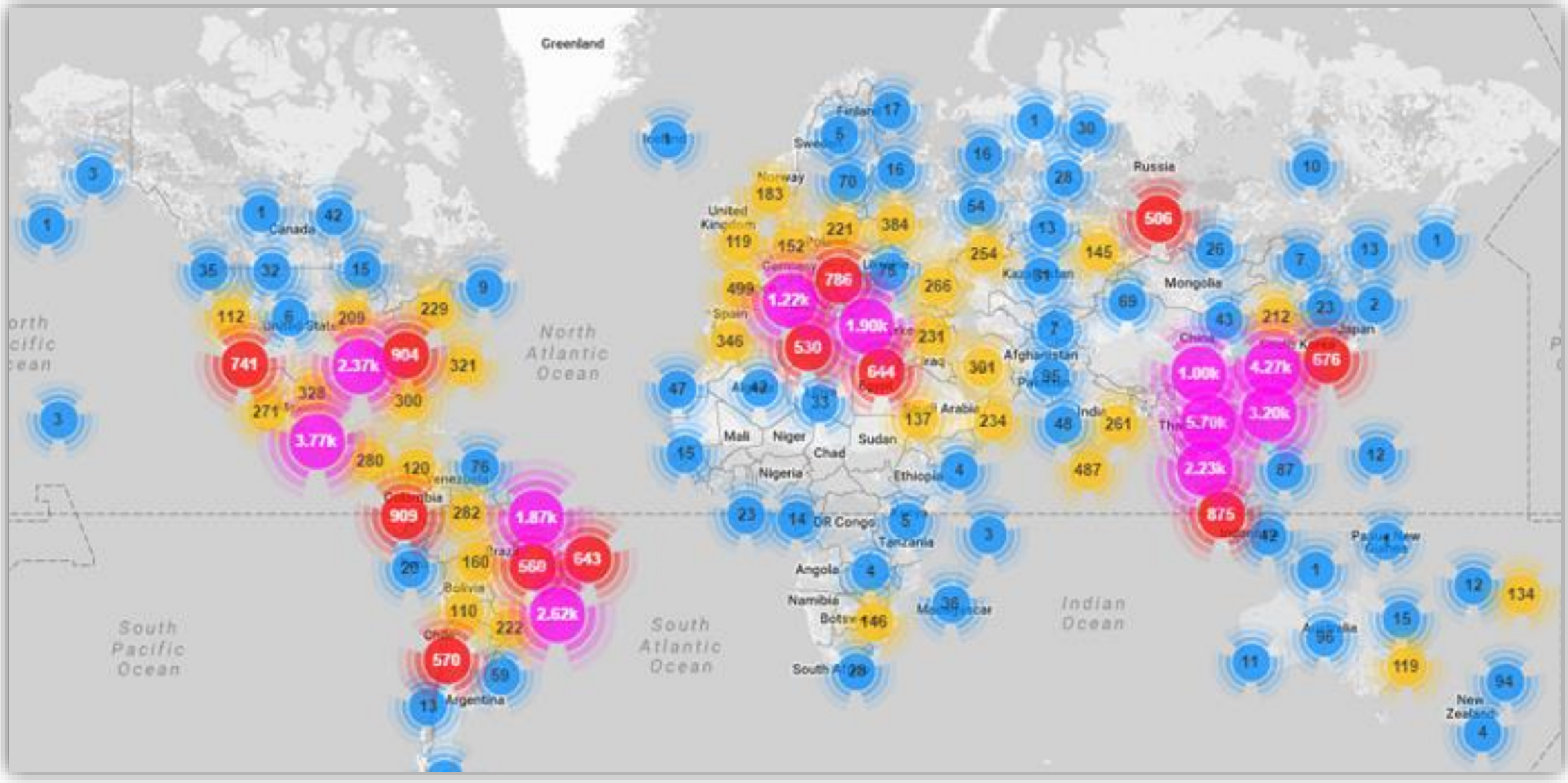


Einsatz

- SPAM-Versendung
- DDoS
- Klickbetrug
- Bitcoin-Mining
- Ransomware-Verteilung
- Filesharing
- Keylogging (z.B. Credentials, Kontodaten, Kreditkarten etc.)
- Proxy-Hosts (Verschleierung)

Aktuelle Sicherheitslage

IoT - Botnetz Mirai



Quelle Incapsula, https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

Aktuelle Sicherheitslage

IoT - Botnetz Mirai

Viele Bots davon sind:

- Überwachungskameras (CCTV)
- Router
- Digital Video Recorder

DDoS mit 500Gbps-1000Gbps:

- Twitter
- Netflix
- Airbnb
- GitHub
- Internetinfrastruktur von Liberia
- DSL-Router der deutschen Telekom
- …

Aktuelle Sicherheitslage

Warum so viele Angriffe?

- **Hacking – das kann jeder**
- **Ein Job wie jeder andere**
- **Unzählige Angriffsziele**
- **Hoher Motivationsfaktor**
- **Bekanntheit**
- **Geld**

CCVOSSEL
We know IT.

Social Engineering

Social Engineering

Was ist das und wo findet es statt?

„[…] zwischenmenschliche Beeinflussungen mit dem Ziel, bei Personen bestimmte Verhaltensweisen hervorzurufen […]“

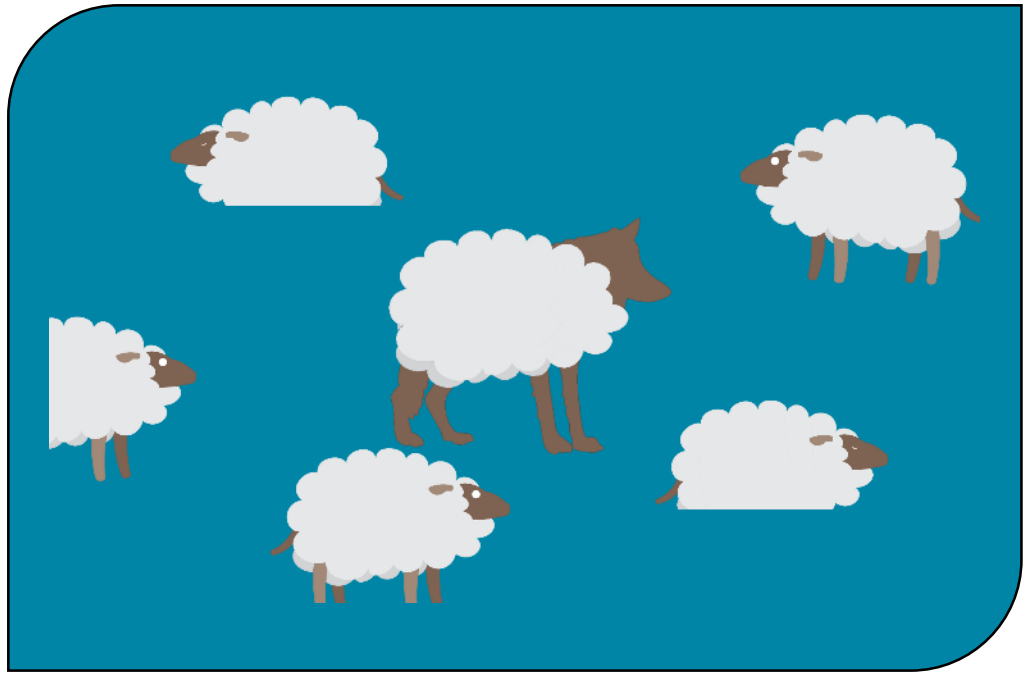
Quelle: https://de.wikipedia.org/wiki/Social_Engineering_(Sicherheit)

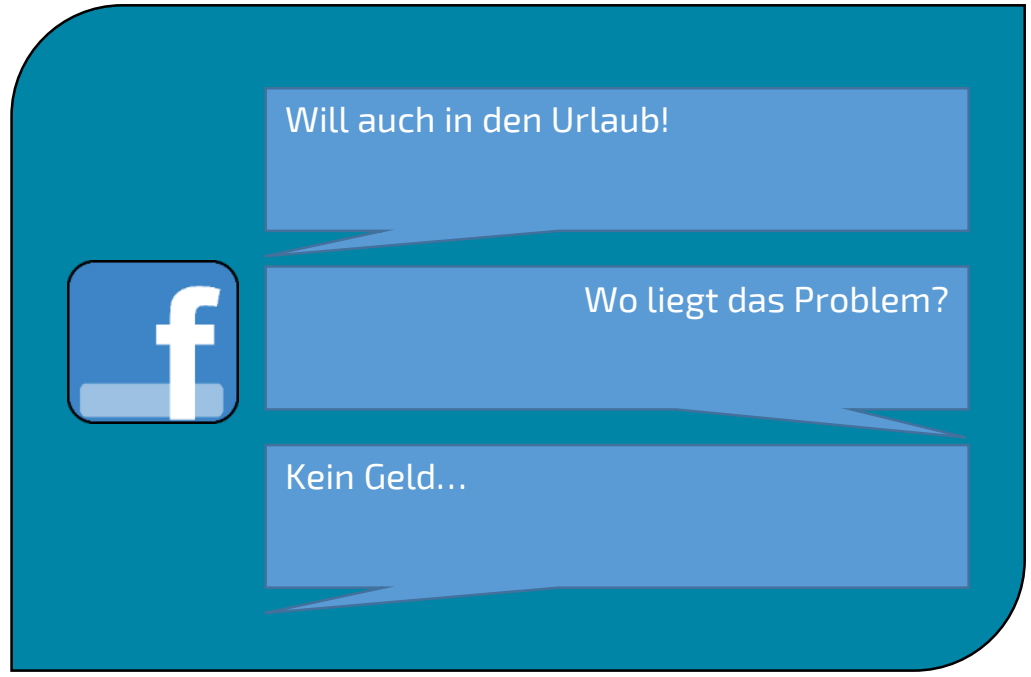
- Social-Media
- Foren
- Telefon
- Echte Welt!

Social Engineering

Information Gathering

CCVOSSEL
We know IT.





Social Engineering

Auch über WhatsApp & Co.

CCVOSSEL
We know IT.

Quelle: http://www.pcwelt.de/news/WhatsApp-Vorsicht-bei-Gutscheinen-von-Rewe-und-Lidl-10103455.html

Social Engineering

CEO-Fraud *(Fraud = Betrug)*

Beim **CEO-Fraud** geben sich **Täter** - nach Sammlung jeglicher Art von Information über das anzugreifende Unternehmen - beispielsweise als **Geschäftsführer** (CEO) des Unternehmens aus und veranlassen einen Unternehmensmitarbeiter zum **Transfer eines größeren Geldbetrages ins Ausland.**

Quelle BKA, https://www.bka.de/SharedDocs/Downloads/DE/IhreSicherheit/CEOFraud.html

Quelle: Microsoft, Stand 03/2017

CCVOSSEL
We know IT.

Proaktiver Schutz

Proaktiver Schutz

Patchmanagement

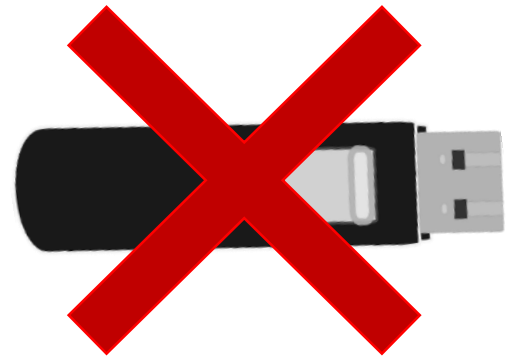
CCVOSSEL
We know IT.

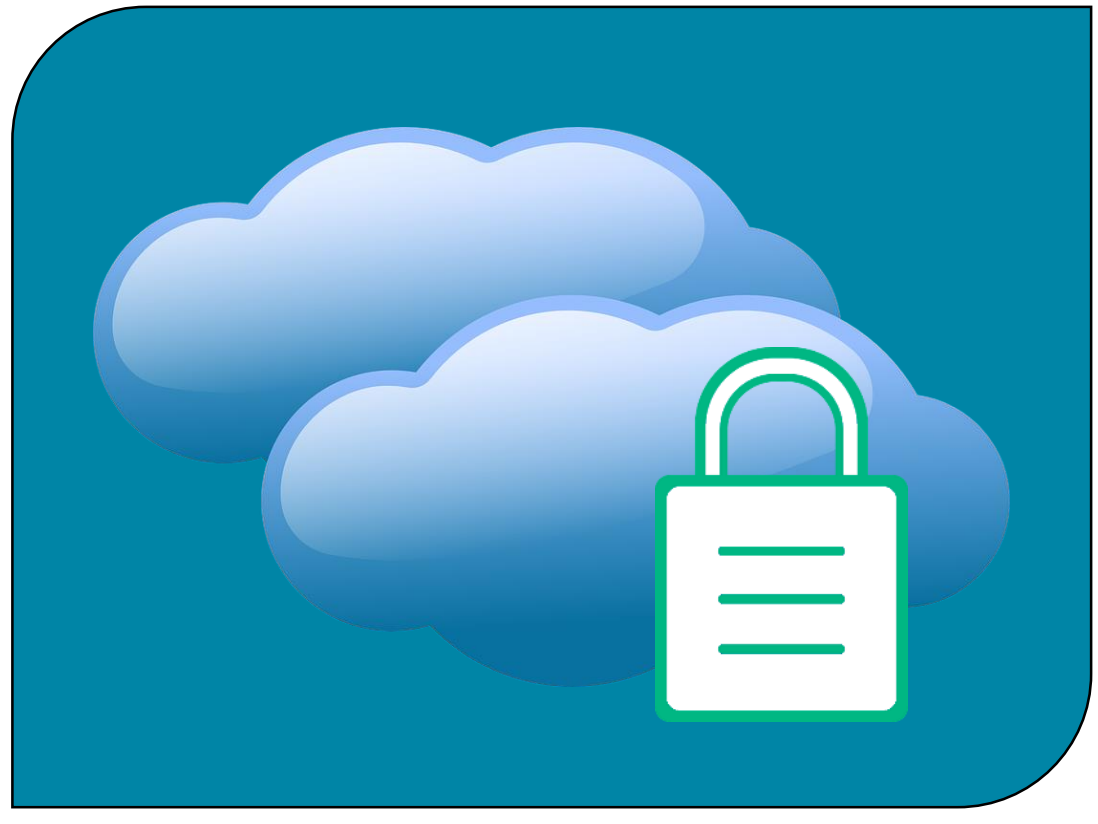
Kontinuierliches Update-Management

Proaktiver Schutz

Daten-Verschlüsselung

CCVOSSEL
We know IT.





Proaktiver Schutz

Systemhärtung

Härtung von Systemen, Beispiel Serverhärtung:

- Strenge **Kennwortrichtlinien**
- Deaktivierung von **unnötigen Diensten**
- Deaktivierung von **Abwärtskompatibilitäten**
  (z.B. LM, NTLMv1, SMBv1, unstrict RPC)
- Einschränkung von **Spezialrechten** (Privilegien) und **UAC**
- Aktivierung detaillierter **Protokollierung**
- Deaktivierung der **Datenaussendung** an Microsoft (Datenschutz)

…

Lösungsmöglichkeiten:

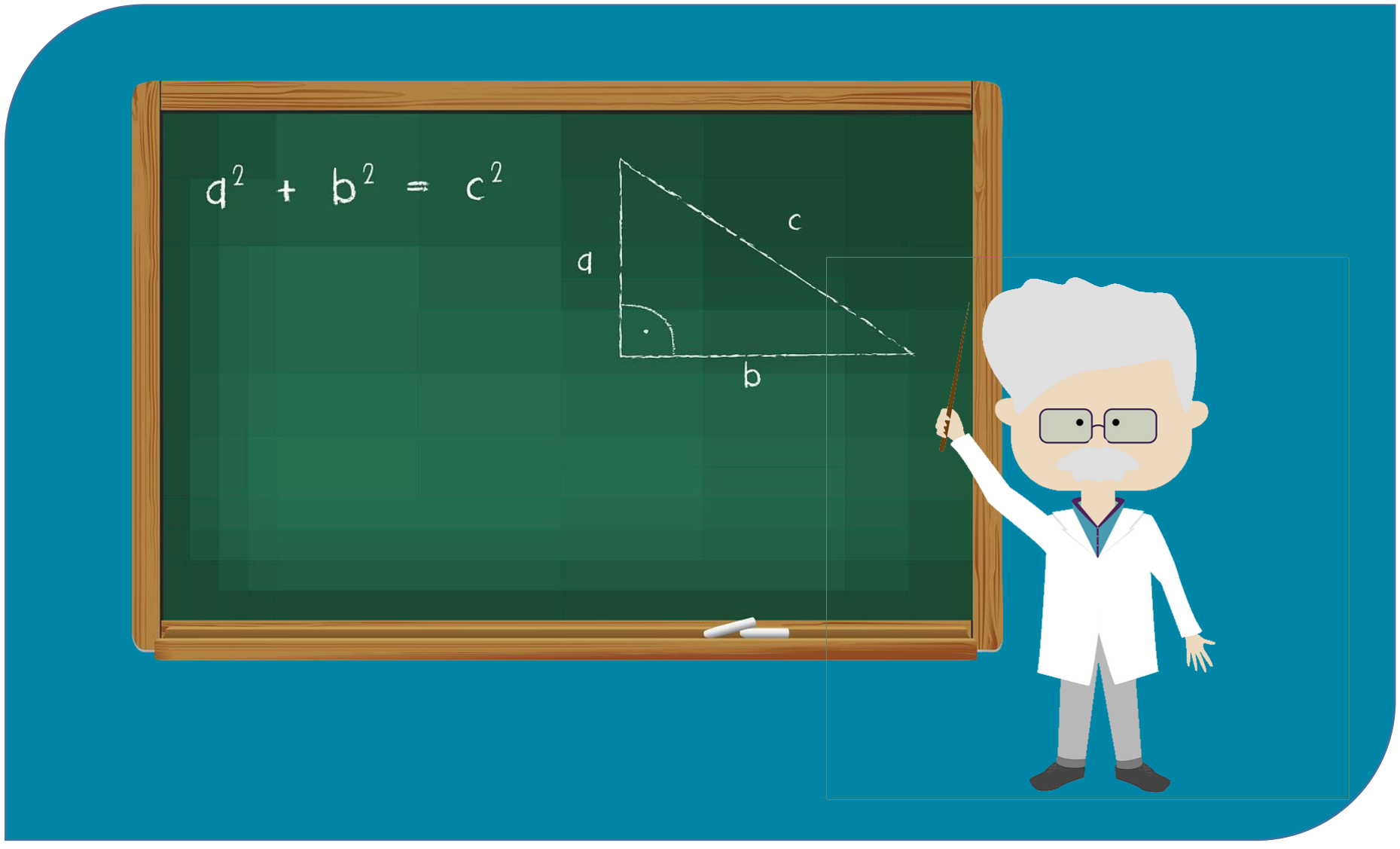
CCSHP
(Server Hardening Package)

CCDHP
(Database Hardening Package)

Proaktiver Schutz

Awareness-Schulungen

CCVOSSEL
We know IT.



Proaktiver Schutz

Awareness-Tools

CCVOSSEL
We know IT.

z.B. CCAWARE

Proaktiver Schutz

Kennwortsicherheit

Sichere Kennwörter

Mein Vater erklärt mir unser Sonnensystem → ***M***ein ***V***ater ***e***rklärte ***m***ir ***j***eden ***S***onntag ***u***nsere ***P***laneten

MVemjSuP → MV3mj$up → MV3mj$up!FB04

2-Faktor-Authentifizierung (2FA)

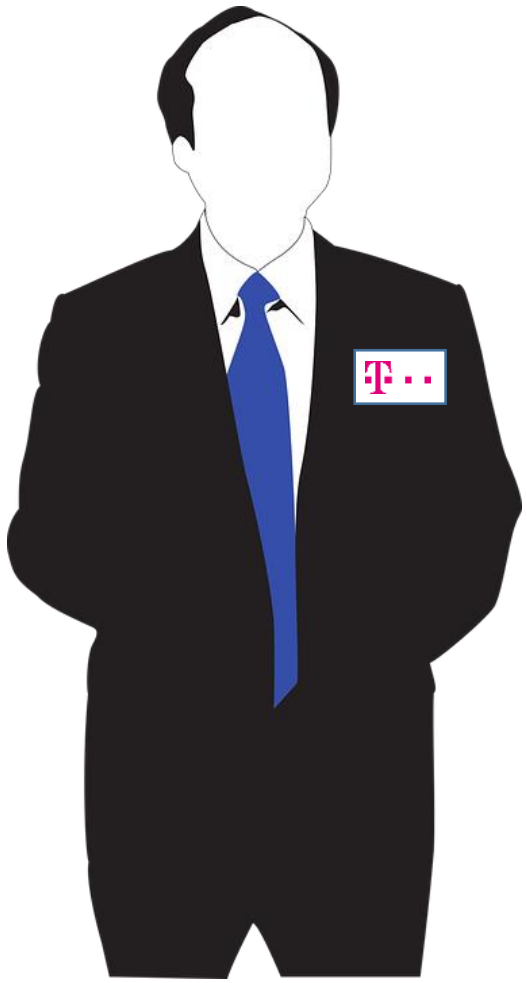
tokenbasierte Authentifizierung

tokenlose Authentifizierung

Proaktiver Schutz

Social Engineering Test

CCVOSSEL
We know IT.



- Phishing-Kampagne
- Telefon-Engineering
- Zutrittsversuche
- Diebstahlsimulation
- physischer Zugriff

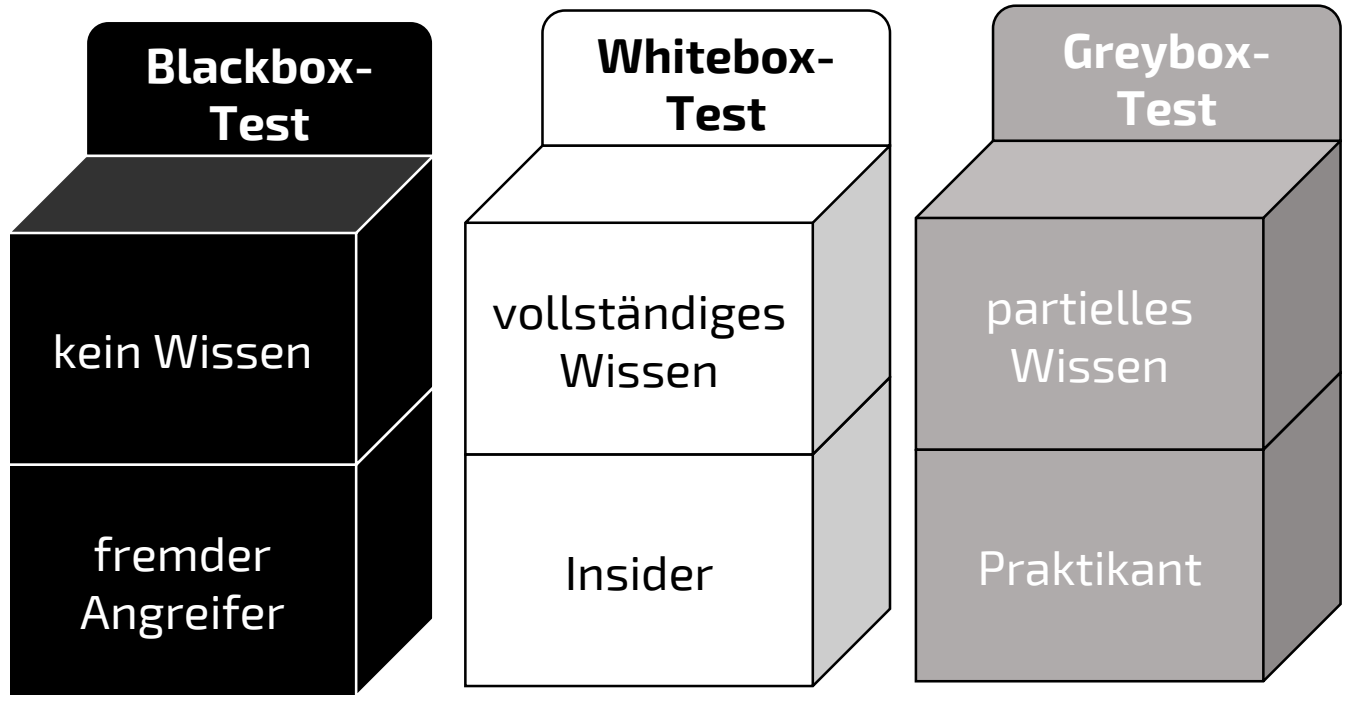
Proaktiver Schutz

Pentest

Was wird getestet?

- Infrastruktur-Penetrationstest
- Webanwendungs-Penetrationstest

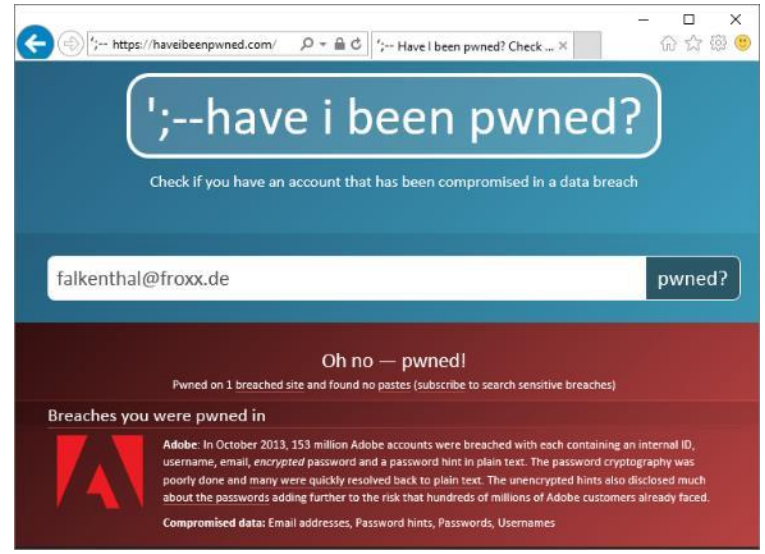
Wie wird getestet?



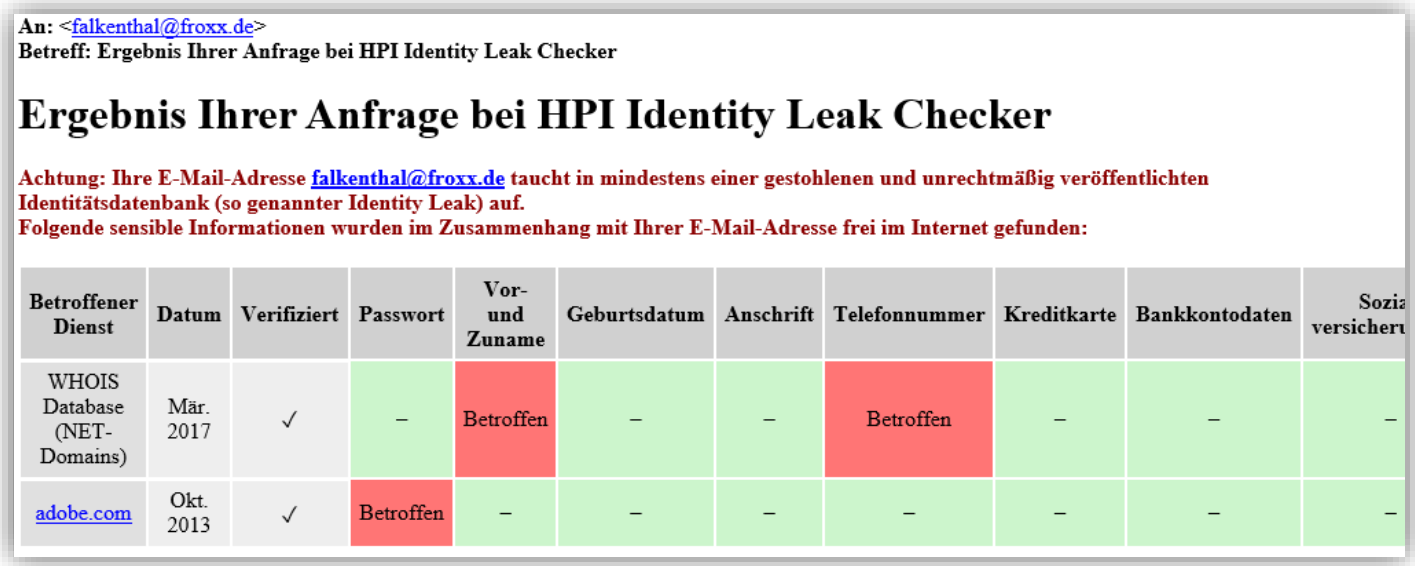
Proaktiver Schutz

Check yourself!

https://haveibeenpwned.com/



https://sec.hpi.uni-potsdam.de/leak-checker



An: <falkenthal@froxx.de>
Betreff: Ergebnis Ihrer Anfrage bei HPI Identity Leak Checker

Ergebnis Ihrer Anfrage bei HPI Identity Leak Checker

Achtung: Ihre E-Mail-Adresse falkenthal@froxx.de taucht in mindestens einer gestohlenen und unrechtmäßig veröffentlichten Identitätsdatenbank (so genannter Identity Leak) auf.
Folgende sensible Informationen wurden im Zusammenhang mit Ihrer E-Mail-Adresse frei im Internet gefunden:

Betroffener Dienst	Datum	Verifiziert	Passwort	Vor- und Zuname	Geburtsdatum	Anschrift	Telefonnummer	Kreditkarte	Bankkontodaten	Sozia versicheru
WHOIS Database (NET-Domains)	Mär. 2017	✓	–	Betroffen	–	–	Betroffen	–	–	–
adobe.com	Okt. 2013	✓	Betroffen	–	–	–	–	–	–	–

CCVOSSEL
We know IT.

Vielen Dank für Ihre Aufmerksamkeit!

Q & A

CCVOSSEL

We know IT.