



Thorsten Strufe
Chair for Privacy and Security

The connected world – at lack of security

Industrial Security in der Automatisierungspraxis
Kooperationsveranstaltung TeleTrusT / Cluster Mechatronik &
Automation

(mit Dank an Dr. Stefan Köpsell)

Augsburg, 04.10.2018

Kurzer Überblick

Wer wir sind und was uns antreibt

Schnelleinführung in die IT Sicherheit

Vernetzung und deren Caveats

Einige Gedanken zur „Connected World“
- mit Beispielen, live und in Farbe!

(Dieser Vortrag war für 60‘ vorbereitet :-))

190 Years of Success

- 1828 Founded as engineering school
- 1890 „Royal Saxon Technical College“
- 1945 Largely destroyed
- 1946 Reopened as „TH Dresden“
- 1961 Technical University
- 1990 Full, comprehensive university
- 2012 University of Excellence

Facts and Figures

- Germany's only comprehensive TU
- Students: 33.506
 - International: 4.739 from 125 nations
 - Fresh-men: 7.808
- 122 Study programmes in 18 faculties
- > 8.200 employees
- Overall budget: 528.5 mio €
 - 257.7 mio € in third-party funding
- 3 (+2) Excellence clusters

Exzellenz 2018



PHYSICS
OF LIFE

- Health sciences, bio medicine/eng., CS
- *“to investigate the fundamental issues in cell and developmental biology”*
- understand the underlying biological processes of life as complex physical phenomena

Stephan Grill



CeTI

Centre for Tactile Internet
with Human-in-the-Loop

- Networking, CS, psychology & med.
- *„to democratize skills and promote equitiy through technology“*
- expediting the efficient cooperation between human and machine

Frank Fitzek, Shu-Chen Li, Thorsten Strufe



ct.qmat

- Smart materials and structures
- *„to pioneer materials with tailor-made functions in all areas of modern technology“*
- placing emphasis on quantum mechanisms on the atomic scale

Matthias Vojta, with Uni Würzburg

Facts and Figures

- Institute of Automatic Computing
1956
- Founding of the Faculty in 1969
- 26 (+3) Professors, 6 Institutes
- 1.764 students (+ ~350 PhD
students)
- ~300 graduates annually
- Over 200 ongoing research projects
- > 10mio€ third-party research funds
- 29 spin-offs since 2000

Key Research Areas

- Software technology for CPS & mobile
systems
- Cloud Computing and Internet security
- Big Data and knowledge extraction
- Human-computer interaction & visual
comp.
- Formal analysis of artificial systems
- Modeling & simulating natural systems

Kurzer Überblick

Wer wir eigentlich sind und was uns antreibt

Schnelleinführung in die IT Sicherheit

Vernetzung und deren Caveats

Einige Gedanken zur „Connected World“
- mit Live-Beispielen

„Sicherheit“: Safety vs. Security



(Funktions-)Sicherheit (*safety*)

Ziel: Schutz vor Schäden durch Fehlfunktionen

- technisches Versagen; Alterung, Stromausfall, Schmutz
 - menschliches Versagen; Dummheit, mangelnde Ausbildung, Fahrlässigkeit
 - höhere Gewalt; Feuer, Blitzschlag, Erdbeben
- Fehlerminimierung: Zuverlässigkeit, Testen

(IT-)Sicherheit (*security*)

Ziel: Schutz vor Schäden durch **zielgerichtete Angriffe** auf IT-Systeme

- Social-Engineering, Erpressung, Wirtschaftsspionage, Überwachung...
 - Terrorismus, Vandalismus
- Schutz eines IT-Systems, seiner Daten und Benutzer

Sicherheitsziele in Anwendungsdomänen

Internet/Telefonie-Anbieter:

- Schutz der Privatsphäre der Kunden
- Einschränkung des Zugriffs zu administrativen Funktionen
- Sicherung gegen Unterbrechungen

Firmen und Forschungseinrichtungen

- Schutz der Privatsphäre der Mitarbeiter
- Vertraulichkeit von Forschungsergebnissen (NDA!)
- Authentizität von Nachrichten und Dokumenten (Verträge, Zeugnisse)
- Sicherstellung des Betriebs

Alle Teilnehmer:

- Verhinderung des Eindringens durch außenstehende Hacker

Sicherheitsziele werden auch als **security objectives** bezeichnet

Etwas formaler: Ziele der IT Sicherheit



Vertraulichkeit (Confidentiality)

- Übertragene und gespeicherte Daten dürfen nur legitimierten Empfängern zugänglich sein
- Vertraulichkeit der Identität wird als Anonymität bezeichnet

Integrität (Integrity)

- Veränderungen an Daten müssen detektiert werden
- (Bedarf der Identifikation des Absenders!)

Verfügbarkeit (Availability)

- Informationen und Dienste sollen berechtigten Nutzern in angemessener Frist zugänglich sein

Zurechenbarkeit (Accountability)

- Die verantwortliche Partei für eine Operation soll identifizierbar sein

Kontrollierter Zugriff (Controlled Access)

- Nur autorisierte Parteien sollen in der Lage sein, auf Dienste oder Informationen zuzugreifen

Kurzer Überblick

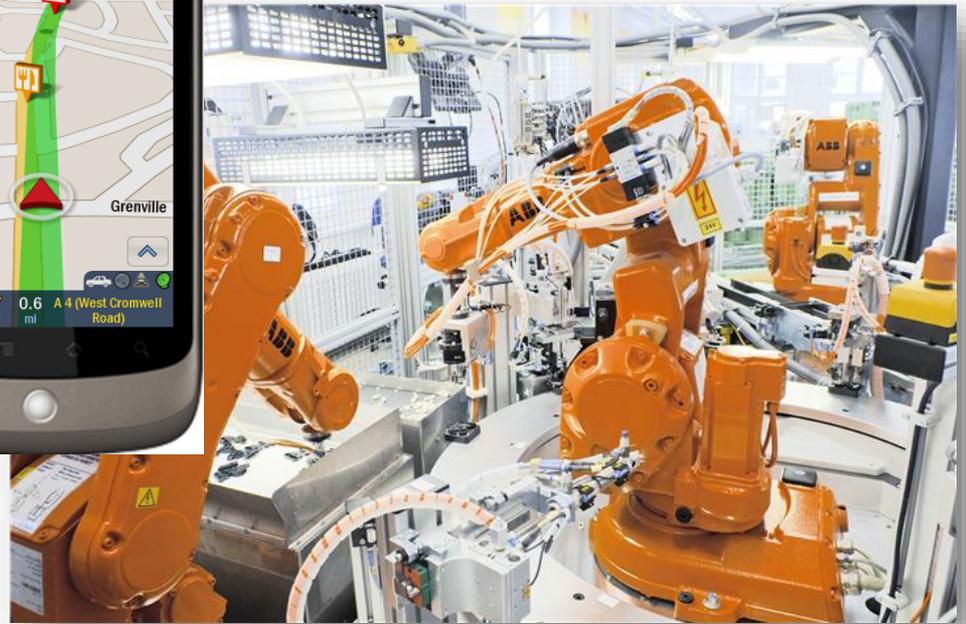
Wer wir eigentlich sind und was uns antreibt

Schnelleinführung in die IT Sicherheit

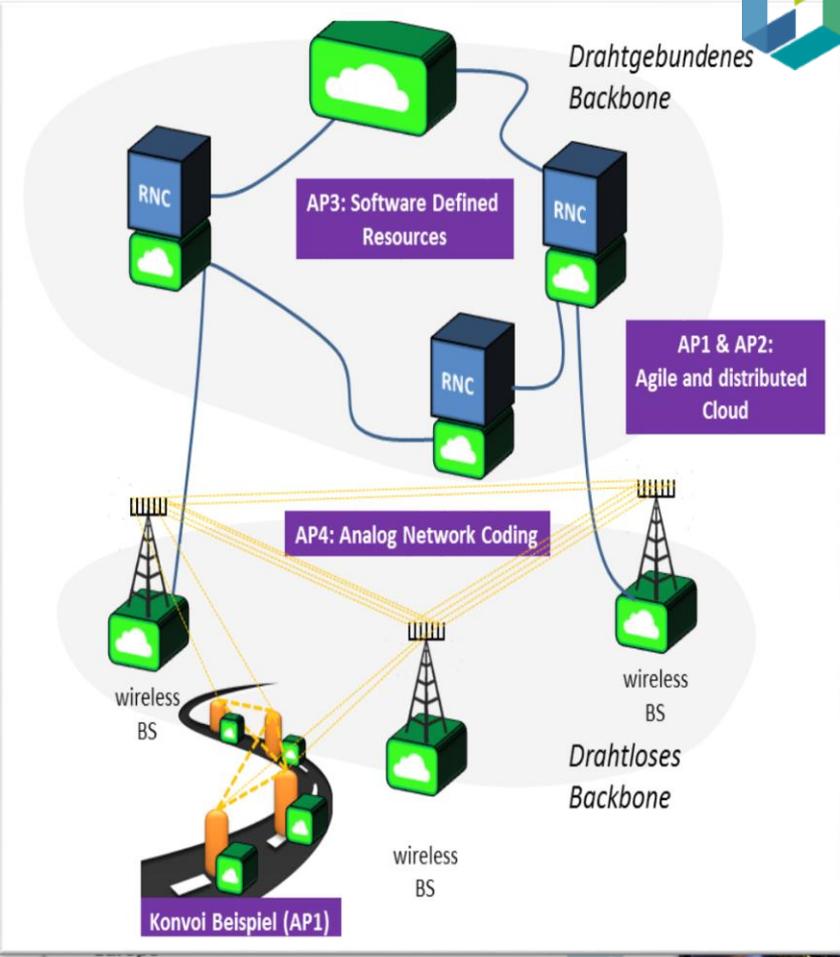
Vernetzung und deren Caveats

Einige Gedanken zur „Connected World“
- mit Live-Beispielen

Networked Applications over Time



„Cloud“ Deployment over Time

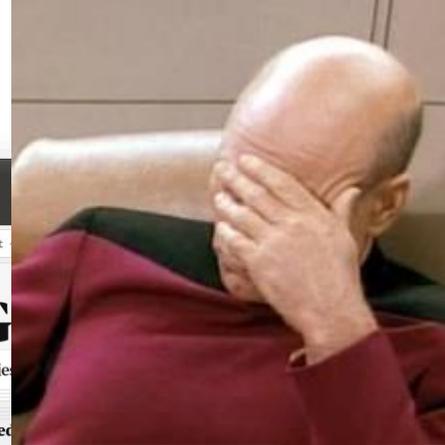


days a week. Find out more about our data center locations,



- Hamina, Finland
- St Ghislain, Belgium
- Dublin, Ireland
- Eemshaven, Netherlands

Data: „Datenreichtum“



Yahoo says all three billion accounts hacked in 2013 data theft

Jonathan Stempel, Jim Finkle



Facebook's week of shame: the Cambridge Analytica fallout | Technology | The Guardian - Mozilla Firefox

Facebook's week of shame: the Cambridge Analytica fallout

Support The Guardian | News | Opinion | Sport | Culture | Lifestyle | More

World UK Science Cities Global development Football Tech Business Environment Obituaries

The Cambridge Analytica Files Facebook

Facebook's week of shame: the Cambridge Analytica fallout

Mark Zuckerberg kept his silence - then did little to assuage the anger in a week that laid bare the worst of Silicon Valley



▲ \$60bn was wiped off Facebook's market capitalisation in wake of Zuckerberg's silence over data breach. Photograph: Justin Sullivan/Getty Images

Tim Adams
@TimAdamsWrites
Sat 24 Mar 2018 21:11 GMT

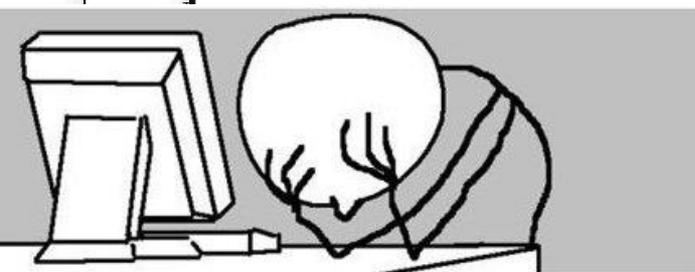
Every story has a beginning. For me, the story of Cambridge Analytica and Facebook that has unfolded so spectacularly this week began in a cafe in Holloway, north London, at the beginning of 2017.

sponsored backers behind it.

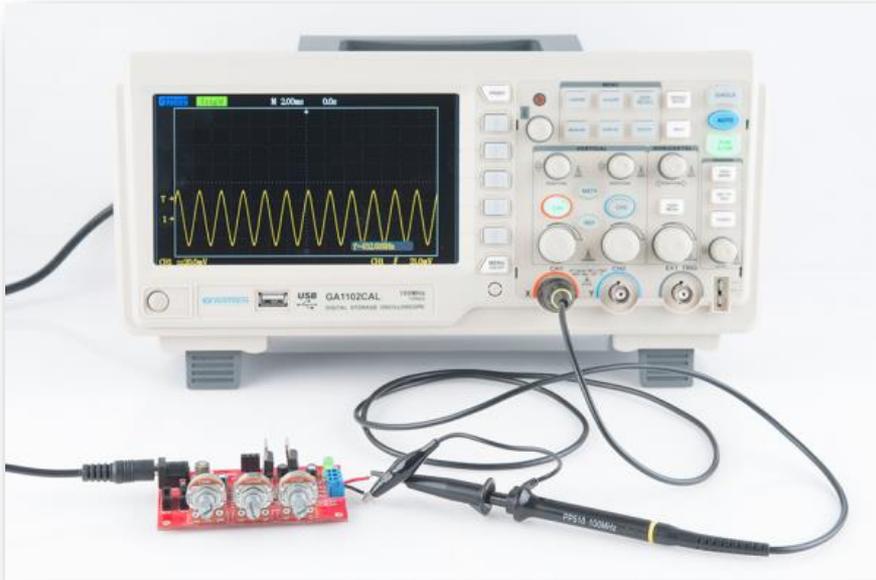
Three U.S. intelligence officials, who do not want to be identified by name, said they believed that the company had been used to spy on the Obama administration and the State Department.

Security / Thorsten Strufe

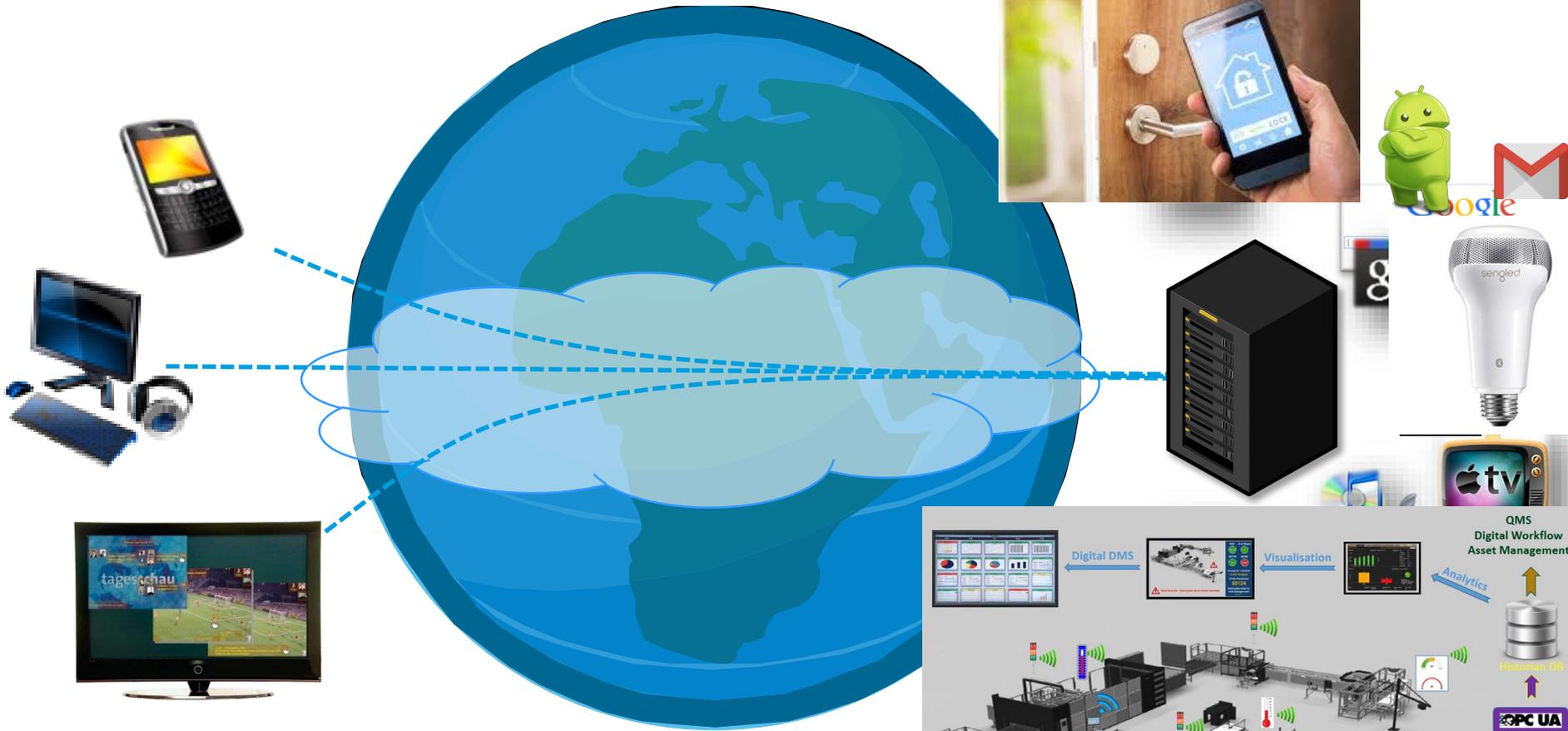
- most viewed
- Kavanaugh clerk hire casts light on link to judge forced to quit in #MeToo era
 - Live Indonesia tsunami: death toll rises to 844 as rescuers struggle to get to victims - live
 - 'Banned in 46 countries' - is Faces of Death the most shocking film ever?
 - How would Gandhi's celibacy tests with naked women be seen today?
Ian Jack
 - Quipping Paul Pogba underlines rift with Mourinho after West Ham defeat



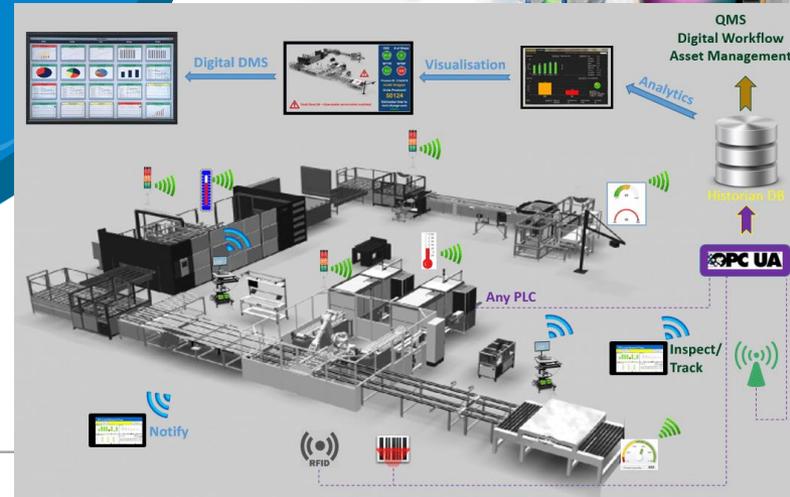
Zugang früher...



Vernetzte Dienste heute...



- 1: Zentrale Anbieter (Hersteller)
- 2: Globaler Zugang über das Internet



Milliarden neuer IoT-Geräte

- sind Rechner
- laufen mit Standardsoftware (Linux)
- besitzen Schnittstellen zum Internet
- Selten Fokus auf Sicherheit bei der Entwicklung
- oft Standard-Passwörter
- oft schlecht programmiert, „wartungsfrei“

- Extrem lange Lebenszyklen (Hersteller lange pleite...)

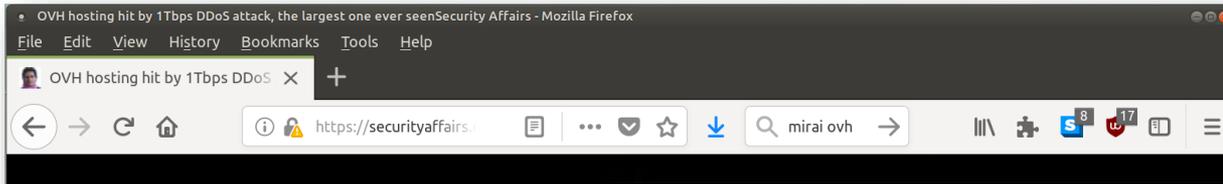
Verbunden mit dem Internet, Breitbandausbau für SOHO/Privat

- mehr Internetanschlüsse
- bessere Verbindung zum Internet
- Flatrate/Always On

Vorteile für Cyber-Kriminelle

- mehr Angriffspunkte
- mehr verfügbare Bandbreite -> Distributed-Denial-of-Service

Distributed Denial of Service...



OVH hosting hit by 1Tbps DDoS attack, the largest one ever seen

September 25, 2016 By Pierluigi Paganini

The hosting company OVH was hit by a massive DDoS attack that hit its servers seen on the Internet.

The hosting provider OVH faced 1Tbps DDoS attack last week. The OVH founder and CTO Octave Klaba reported the 1Tbps sources of the attack.

```
log /home/vac/logs/vac.log-last | egrep "pps" | awk '{print $1,$2,$3,$6}' | sed "s/1,2,3,7,8,10,11 -d '|'" | sed "s/.....pps/" | cut -f 2,3,4,5,6,7 -d rep "gone" | sed "s/gone|/"
```

```
Sep|18|10:49:12|tcp_ack|20Mpps|232Gbps  
Sep|18|10:58:32|tcp_ack|15Mpps|173Gbps  
Sep|18|11:17:02|tcp_ack|19Mpps|224Gbps  
Sep|18|11:44:17|tcp_ack|19Mpps|227Gbps
```

The Mirai Botnet Was Part of a College Student Minecraft Scheme | WIRED - Mozilla Firefox

How a Dorm Room Minecraft Scam Brought Down the Internet

GARRETT M. GRAFF SECURITY 12.13.17 03:55 PM

HOW A DORM ROOM MINECRAFT SCAM BROUGHT DOWN THE INTERNET

BEN BOURS/WIRED

SHARE 8841

THE MOST DRAMATIC cybersecurity story of 2016 came to a quiet conclusion Friday in an

3 FREE ARTICLES LEFT THIS MONTH

Get unlimited access + a free YubiKey. **Subscribe**

Sign In CLOSE X



Privacy and Security Chair for Priv

Distributed-Denial-of-Service-Angriffe — lukratives Geschäft für Cyber-Kriminelle...



The screenshot shows a web browser window with a single tab titled "DDoS-Attacken gegen gri...". The address bar contains the URL "www.heise.de/newsticker/meldung/DDoS-Attacken-gegen-griechische-Banken-3028007.html". The main content area displays the article title "DDoS-Attacken gegen griechische Banken" in a large, bold font. Below the title is the "heise Security" logo and the date "01.12.2015 10:47 Uhr". To the right of the date is a speaker icon and the text "vorlesen". Below the text is a large image of hands typing on a computer keyboard. At the bottom of the article preview, the text reads: "Armada Collective weitert DDoS-Angriffe in Europa aus und erpresst nun Kreditinstitute in Griechenland."

Armada Collective weitert DDoS-Angriffe in Europa aus und erpresst nun Kreditinstitute in Griechenland.

Schadsoftware — eine lukrative Einnahmequelle für Cyber-Kriminelle



Krypto-Trojaner Locky wütet in Deutschland: Über 5000 Infektionen pro Stunde

19.02.2016 06:15 Uhr – Ronald Eikenberg vorlesen

!!! WICHTIGE INFORMATIONEN !!!!

Alle Dateien wurden mit RSA-2048 und AES-128 Ziffern verschlüsselt.
Mehr Informationen über RSA können Sie hier finden:
<http://de.wikipedia.org/wiki/RSA-Kryptosystem>
http://de.wikipedia.org/wiki/Advanced_Encryption_Standard

Die Entschlüsselung Ihrer Dateien ist nur mit einem privaten Schlüssel und einem Entschlüsselungsprogramm, welches sich auf unserem Server befindet, möglich.
Um Ihren privaten Schlüssel zu erhalten, folgen Sie einem der folgenden Links:

1. <http://6dbxgqam4crv6rr6.tor2web.org/7D>
2. <http://6dbxgqam4crv6rr6.onion.to/7D>
3. <http://6dbxgqam4crv6rr6.onion.cab/7D>

Die neue Ransomware Locky findet hierzulande offenbar massenhaft Opfer, darunter auch ein Fraunhofer-Institut. Inzwischen haben die Täter ihrem Schädling sogar Deutsch beigebracht.

Kriminelle bieten Mirai-Botnetz mit 400.000 IoT-Geräten zur Miete an

25.11.2016 10:52 Uhr - Dennis Schirmmacher



(Bild: Bleepingcomputer.com)

Zwei Hacker sollen derzeit auf Kundenfang gehen und Mirai-Botnetze zur Miete anbieten. Dabei werben sie unter anderem mit einer optimierten Version des DDoS-Tools Mirai. Sicherheitsforscher zeigen den Live-Status des gesamten Mirai-Botnetzes an.

Schadsoftware: Ein diversifizierter Markt



[Tom-b, <http://de.wikipedia.org/wiki/Datei:Botnet.svg>]

Hacker Tools — Kali Linux

A screenshot of a web browser displaying the Kali Linux website. The browser's address bar shows "www.kali.org". The website has a dark blue header with the "KALI LINUX" logo on the left and navigation links for "BLOG", "DOWNLOADS", "TRAINING", "DOCUMENTATION", and "COMMUNITY" on the right. The main content area features a large graphic with a mountain range under a cloudy sky. The text on the page includes: "The most advanced penetration testing distribution, ever.", "From the creators of BackTrack comes Kali Linux, the most advanced and versatile penetration testing distribution ever created. BackTrack has grown far beyond its humble roots as a live CD and has now become a full-fledged operating system. With all this buzz, you might be asking yourself: - [What's new ?](#)", "KALI LINUX", "the quieter you become, the more you are able to hear", "PENETRATION TESTING, REDEFINED.", and "A Project By Offensive Security".

Kali Linux | Rebirth of BackTrack x

www.kali.org

KALI LINUX™

BLOG DOWNLOADS TRAINING DOCUMENTATION COMMUNITY

The most advanced penetration testing distribution, ever.

From the creators of BackTrack comes Kali Linux, the most advanced and versatile penetration testing distribution ever created. BackTrack has grown far beyond its humble roots as a live CD and has now become a full-fledged operating system. With all this buzz, you might be asking yourself: - [What's new ?](#)

KALI LINUX

"the quieter you become, the more you are able to hear"

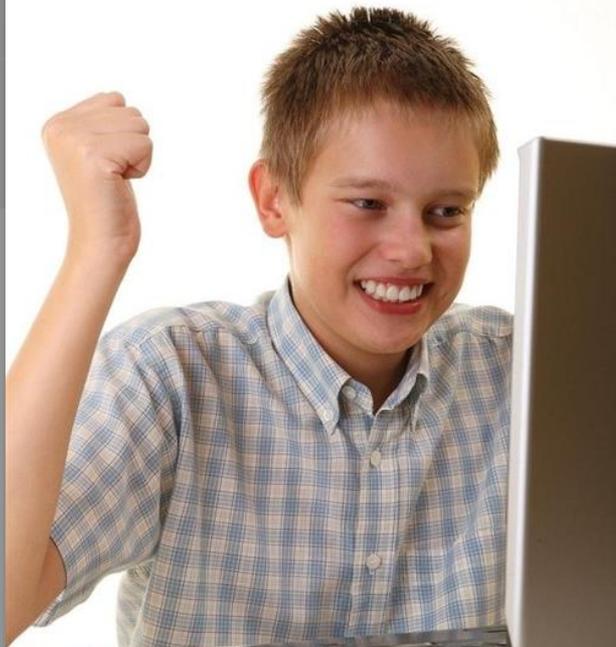
PENETRATION TESTING, REDEFINED.

A Project By Offensive Security

Hacker Tools — Metasploit

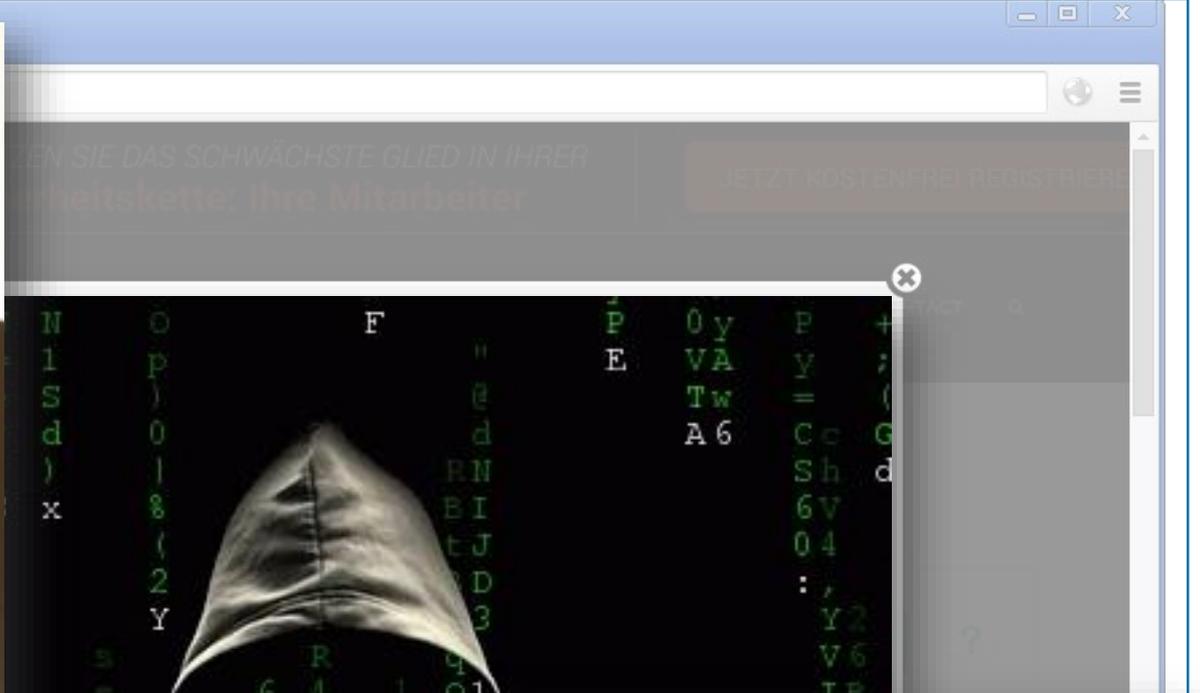


SUCCESS!!



1337 EV1L HAXOR!11!

memegenerator.net



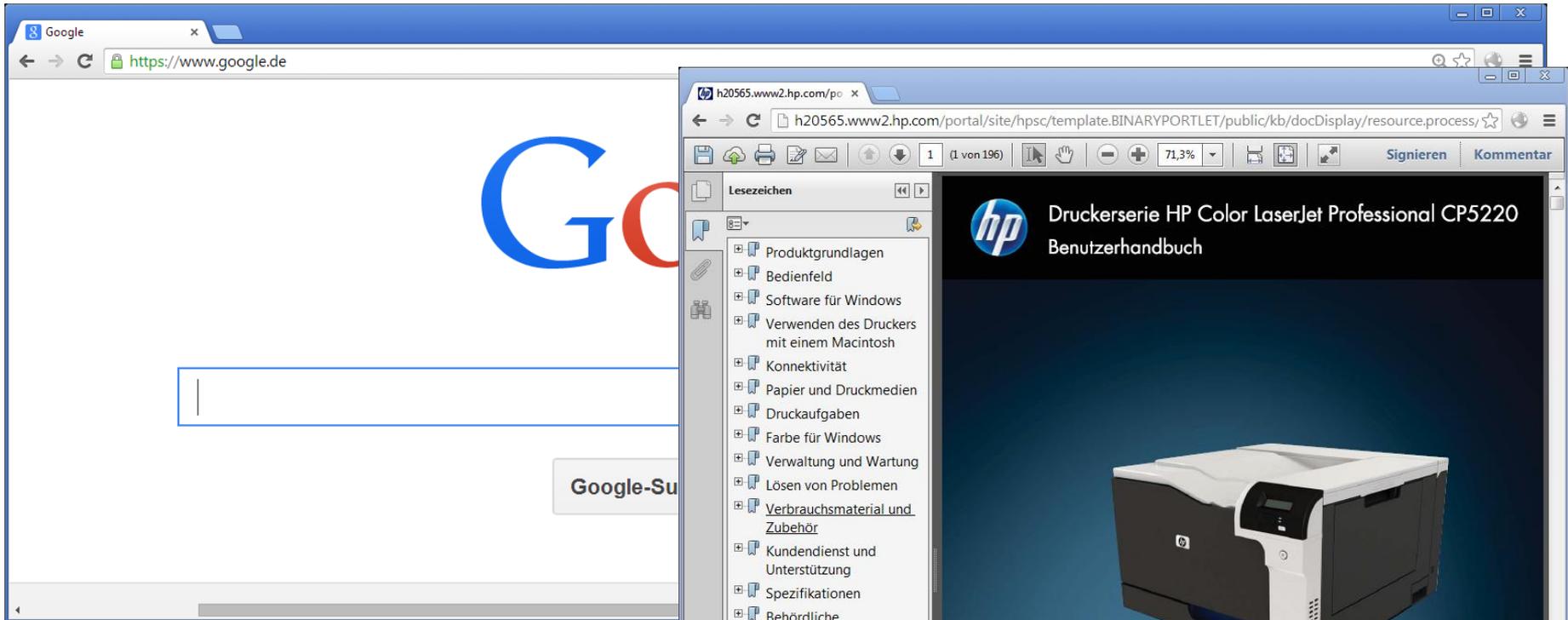
HUCH? KANN'S DENN SEIN?



BIN ICH ETWA SCHON DRIN!?

memegenerator.net

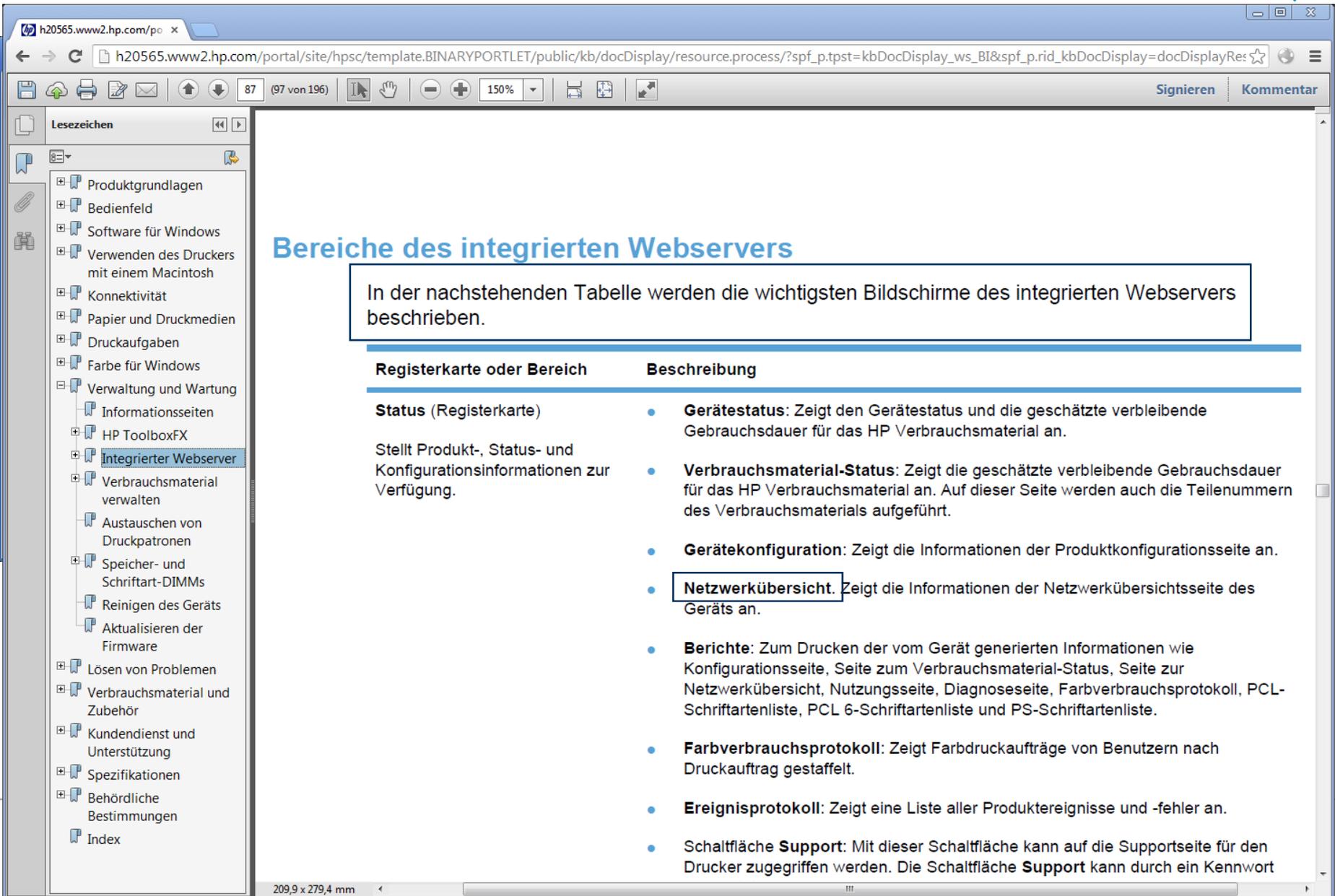
Notwendige Hacking-Werkzeuge



Suchmaschine

Benutzerhandbücher

Notwendige Hacking-Werkzeuge



The screenshot shows a web browser window with the URL `h20565.www2.hp.com/portal/site/hpsc/template.BINARYPORTLET/public/kb/docDisplay/resource.process/?spf_p.tpst=kbDocDisplay_ws_BI&spf_p.riid_kbDocDisplay=docDisplayRes`. The left sidebar contains a navigation menu with the following items:

- Produktgrundlagen
- Bedienfeld
- Software für Windows
- Verwenden des Druckers mit einem Macintosh
- Konnektivität
- Papier und Druckmedien
- Druckaufgaben
- Farbe für Windows
- Verwaltung und Wartung
 - Informationsseiten
 - HP ToolboxFX
 - Integrierter Webserver**
 - Verbrauchsmaterial verwalten
 - Austauschen von Druckpatronen
- Speicher- und Schriftart-DIMMs
- Reinigen des Geräts
- Aktualisieren der Firmware
- Lösen von Problemen
- Verbrauchsmaterial und Zubehör
- Kundendienst und Unterstützung
- Spezifikationen
- Behördliche Bestimmungen
- Index

Bereiche des integrierten Webservers

In der nachstehenden Tabelle werden die wichtigsten Bildschirme des integrierten Webservers beschrieben.

Registerkarte oder Bereich	Beschreibung
Status (Registerkarte)	<ul style="list-style-type: none">Gerätstatus: Zeigt den Gerätestatus und die geschätzte verbleibende Gebrauchsdauer für das HP Verbrauchsmaterial an.
Stellt Produkt-, Status- und Konfigurationsinformationen zur Verfügung.	<ul style="list-style-type: none">Verbrauchsmaterial-Status: Zeigt die geschätzte verbleibende Gebrauchsdauer für das HP Verbrauchsmaterial an. Auf dieser Seite werden auch die Teilenummern des Verbrauchsmaterials aufgeführt.Gerätekonfiguration: Zeigt die Informationen der Produktkonfigurationsseite an.Netzwerkübersicht: Zeigt die Informationen der Netzwerkübersichtsseite des Geräts an.Berichte: Zum Drucken der vom Gerät generierten Informationen wie Konfigurationsseite, Seite zum Verbrauchsmaterial-Status, Seite zur Netzwerkübersicht, Nutzungsseite, Diagnosesseite, Farbverbrauchsprotokoll, PCL-Schriftartenliste, PCL 6-Schriftartenliste und PS-Schriftartenliste.Farbverbrauchsprotokoll: Zeigt Farbdruckaufträge von Benutzern nach Druckauftrag gestaffelt.Ereignisprotokoll: Zeigt eine Liste aller Produktereignisse und -fehler an.Schaltfläche Support: Mit dieser Schaltfläche kann auf die Supportseite für den Drucker zugegriffen werden. Die Schaltfläche Support kann durch ein Kennwort

shodan.io — die etwas andere Suchmaschine...



Shodan

Developers Book View All... Show API Key

SHODAN

Explore Downloads Reports Enterprise Access Contact Us My Account

The search engine for **Webcams**

Shodan is the world's first search engine for Internet-connected devices

Create a Free Account Getting Started

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

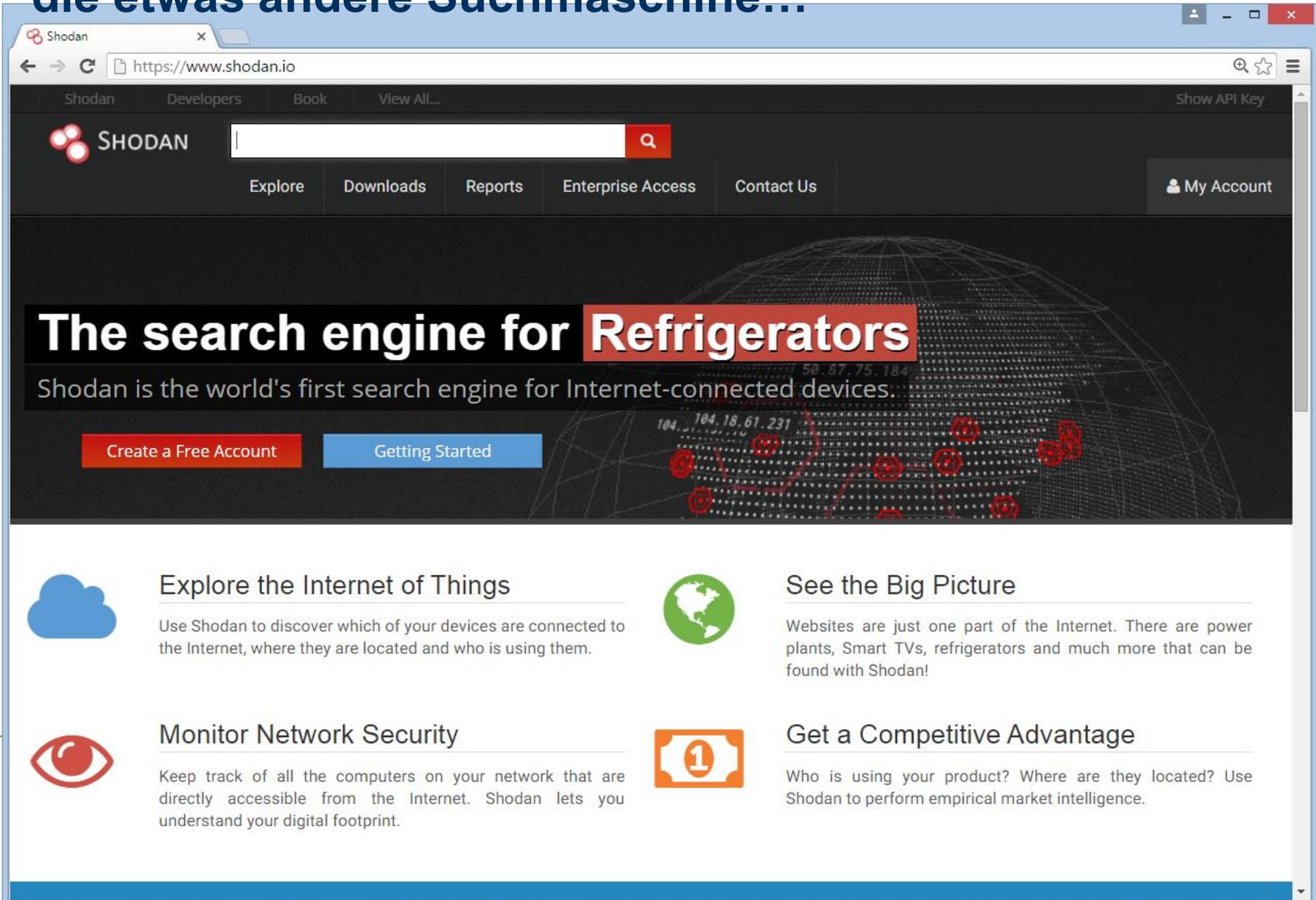
Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

shodan.io — die etwas andere Suchmaschine...



The screenshot shows the Shodan website homepage. At the top, there is a navigation bar with links for 'Shodan', 'Developers', 'Book', and 'View All...'. A search bar is prominently displayed with the Shodan logo and a search icon. Below the search bar are navigation links for 'Explore', 'Downloads', 'Reports', 'Enterprise Access', and 'Contact Us', along with a 'My Account' button. The main content area features a large banner with the text 'The search engine for Refrigerators' and 'Shodan is the world's first search engine for Internet-connected devices'. Two buttons, 'Create a Free Account' and 'Getting Started', are visible. Below the banner are four feature sections: 'Explore the Internet of Things', 'See the Big Picture', 'Monitor Network Security', and 'Get a Competitive Advantage', each with an icon and a brief description.

Shodan

https://www.shodan.io

SHODAN

Explore Downloads Reports Enterprise Access Contact Us My Account

The search engine for Refrigerators

Shodan is the world's first search engine for Internet-connected devices

Create a Free Account Getting Started

 **Explore the Internet of Things**
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

 **See the Big Picture**
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

 **Monitor Network Security**
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

 **Get a Competitive Advantage**
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

shodan.io — die etwas andere Suchmaschine...

PRIVACY
AND
SECURITY



Shodan

Shodan Developers Book View All... Show API Key

SHODAN

Explore Downloads Reports Enterprise Access Contact Us My Account

The search engine for Buildings

Shodan is the world's first search engine for Internet-connected devices

Create a Free Account Getting Started

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

shodan.io — die etwas andere Suchmaschine...

PRIVACY
AND
SECURITY



Shodan

Shodan Developers Book View All... Show API Key

SHODAN

Explore Downloads Reports Enterprise Access Contact Us My Account

The search engine for Power Plants

Shodan is the world's first search engine for Internet-connected devices

Create a Free Account Getting Started

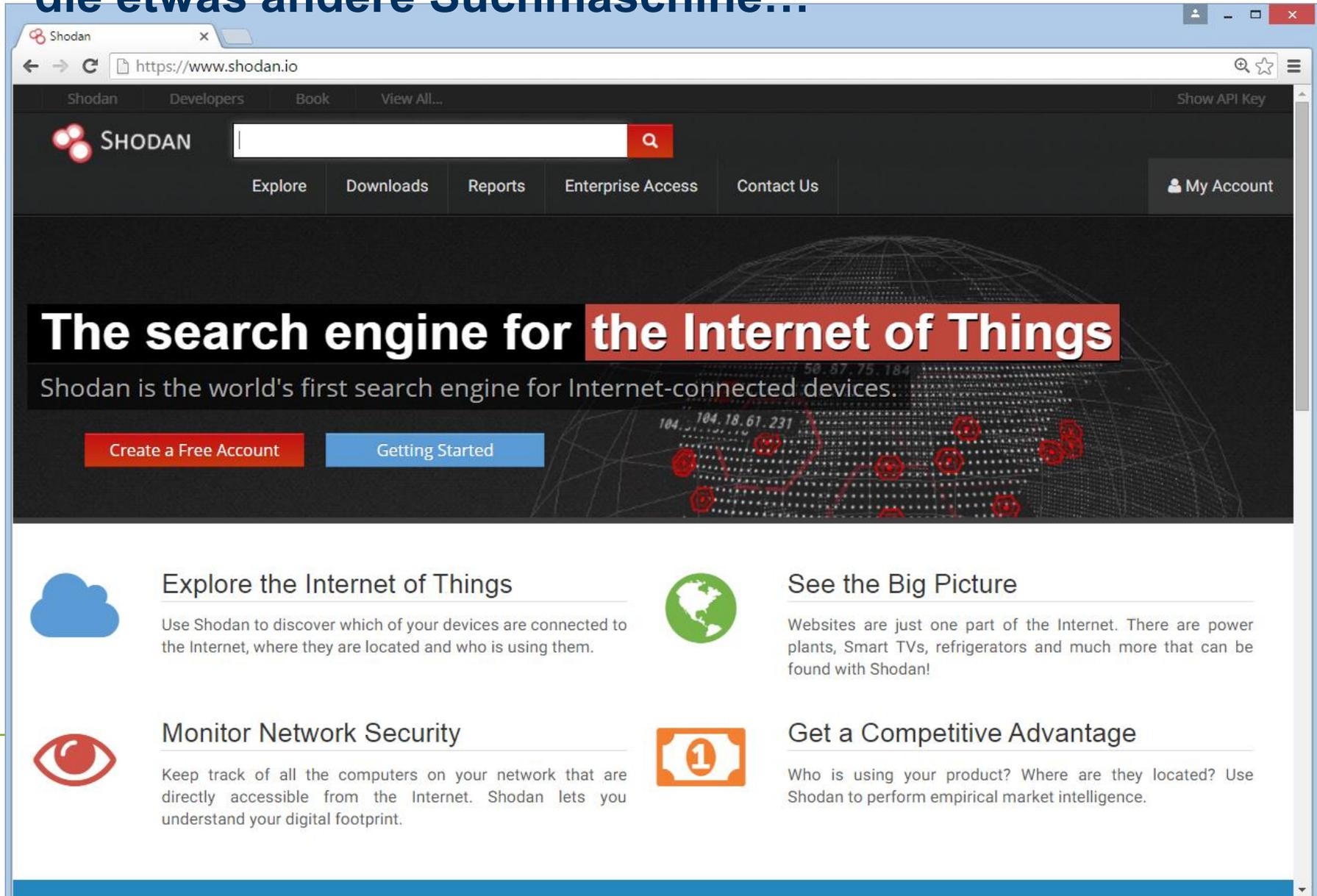
Explore the Internet of Things
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

shodan.io — die etwas andere Suchmaschine...



The screenshot shows the Shodan website homepage. At the top, there is a navigation bar with links for 'Shodan', 'Developers', 'Book', and 'View All...'. A search bar is prominently displayed with the Shodan logo and a search icon. Below the search bar are navigation links for 'Explore', 'Downloads', 'Reports', 'Enterprise Access', and 'Contact Us', along with a 'My Account' button. The main content area features a large banner with the text 'The search engine for the Internet of Things' and 'Shodan is the world's first search engine for Internet-connected devices'. Two buttons, 'Create a Free Account' and 'Getting Started', are positioned below the banner. The background of the banner shows a globe with IP addresses and red circular markers. Below the banner are four feature sections, each with an icon and a brief description.

Shodan

https://www.shodan.io

SHODAN

Explore Downloads Reports Enterprise Access Contact Us My Account

The search engine for the Internet of Things

Shodan is the world's first search engine for Internet-connected devices

Create a Free Account Getting Started

 **Explore the Internet of Things**
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

 **See the Big Picture**
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

 **Monitor Network Security**
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

 **Get a Competitive Advantage**
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

shodan.io — die etwas andere Suchmaschine...



The screenshot shows a web browser window with the URL <https://www.shodan.io/report/awAOSFjr>. The page title is "DSL Router - Shodan". The search bar contains "DSL Router" and shows a search button. Below the search bar, there are navigation links: "Explore", "Downloads", "Reports", "Enterprise Access", "Contact Us", and "My Account". The main content area displays "DSL Router" in large white text on a dark background, followed by the text "Search for dsl router returned 334,690 results on 18-04-2016". Below this, there is a world map on the left and a "Top Countries" list on the right.

Country	Count
1. Brazil	64,463
2. United States	58,740
3. India	45,518
4. Viet Nam	24,643
5. Spain	17,727
6. Suriname	13,814
7. Bolivia, Plurinational State of	9,415
8. Iran, Islamic Republic of	8,689
9. Canada	7,522
10. China	5,839

So schlimm kann es nicht sein? Folgen der steigenden Vernetzung/IT-Durchdringung



Gehackte US-Sender: Zom

www.heise.de/newsticker/meldung/Gehackte-US-Sender-Zombie-Apokalypse-hat-begonnen-1802232.htm

IuG SaC VHS CCG LNDW Weitere Lesezeichen

12.02.2013 09:22 « Vorige | Nächste »

Gehackte US-Sender: Zombie-Apokalypse hat begonnen

vorlesen / MP3-Download

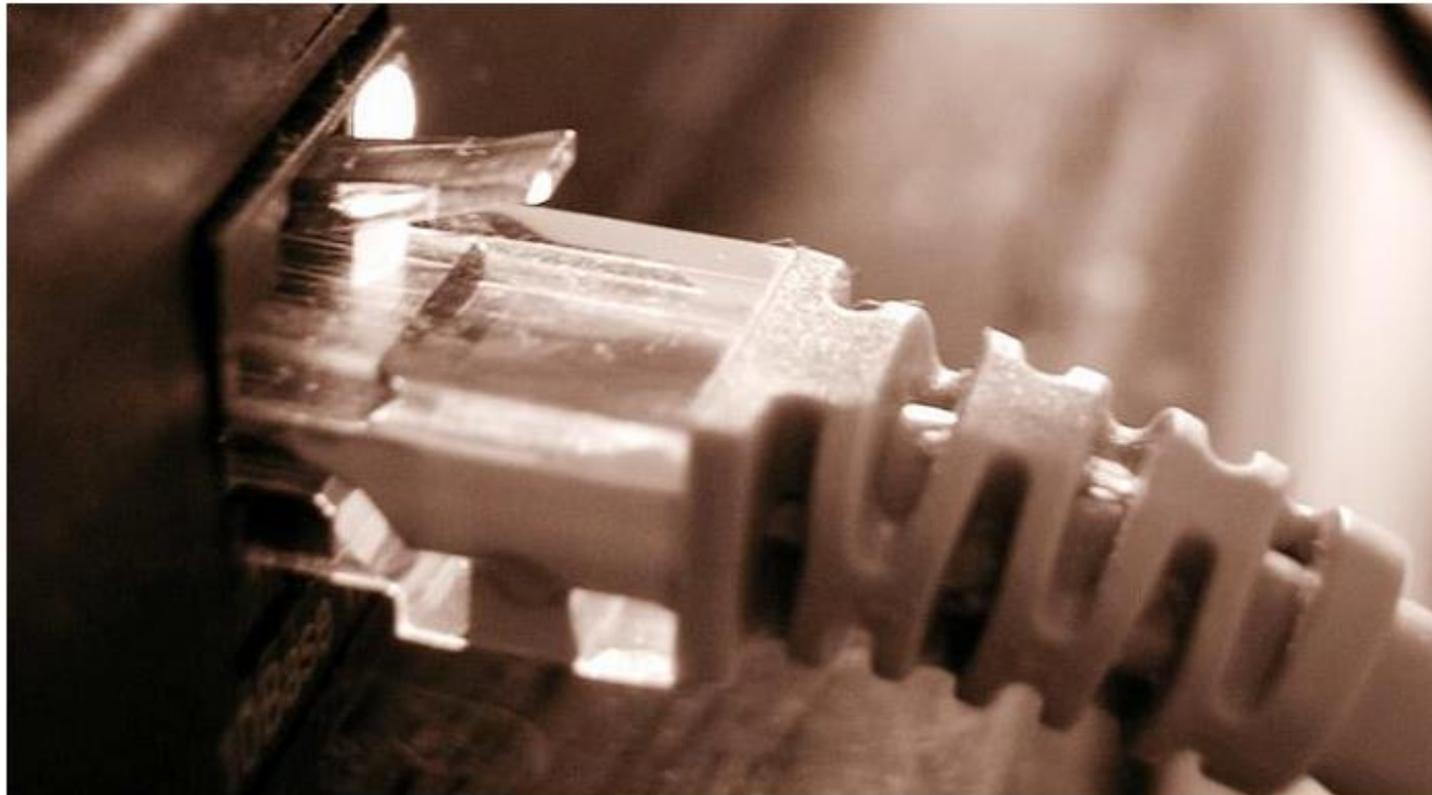
In den USA haben zwei lokale Fernsehsender am Montagabend vor Zombies gewarnt, die die Lebenden attackieren. Wie die [Great Falls Tribune](#) aus Montana und die [Upper Michigan Source](#) aus Michigan berichten, hätten sich Unbekannte in das Notfallwarnsystem der Sender KRTV und Public TV 13 gehackt und die Ausstrahlung der Eilmeldung bewirkt. Eine verzerrte Stimme erklärte demnach während des laufenden Programms, dass sich Leichen aus ihren Gräbern erheben und die Lebenden angreifen. Die Fernsehzuschauer wurden gewarnt, sich keinesfalls den Toten zu nähern, "denn sie sind extrem gefährlich".



Großstörung bei der Telekom: Angreifer nutzten Lücke und Botnetz-Code

heise Security 29.11.2016 16:37 Uhr - Fabian A. Scherschel

vorlesen



Einen Tag nachdem bekannt wurde, dass die großflächige Störung bei der Telekom auf einen - größtenteils missglückten - Hackerangriff zurückzuführen ist, wird klarer, was passiert ist. Die Angreifer zielten mit Botnetz-Code auf eine Sicherheitslücke.





DDoS-Attacke legt Twitter, Netflix, Paypal, Spotify und andere Dienste lahm

heise online 21.10.2016 22:13 Uhr - Holger Bleich

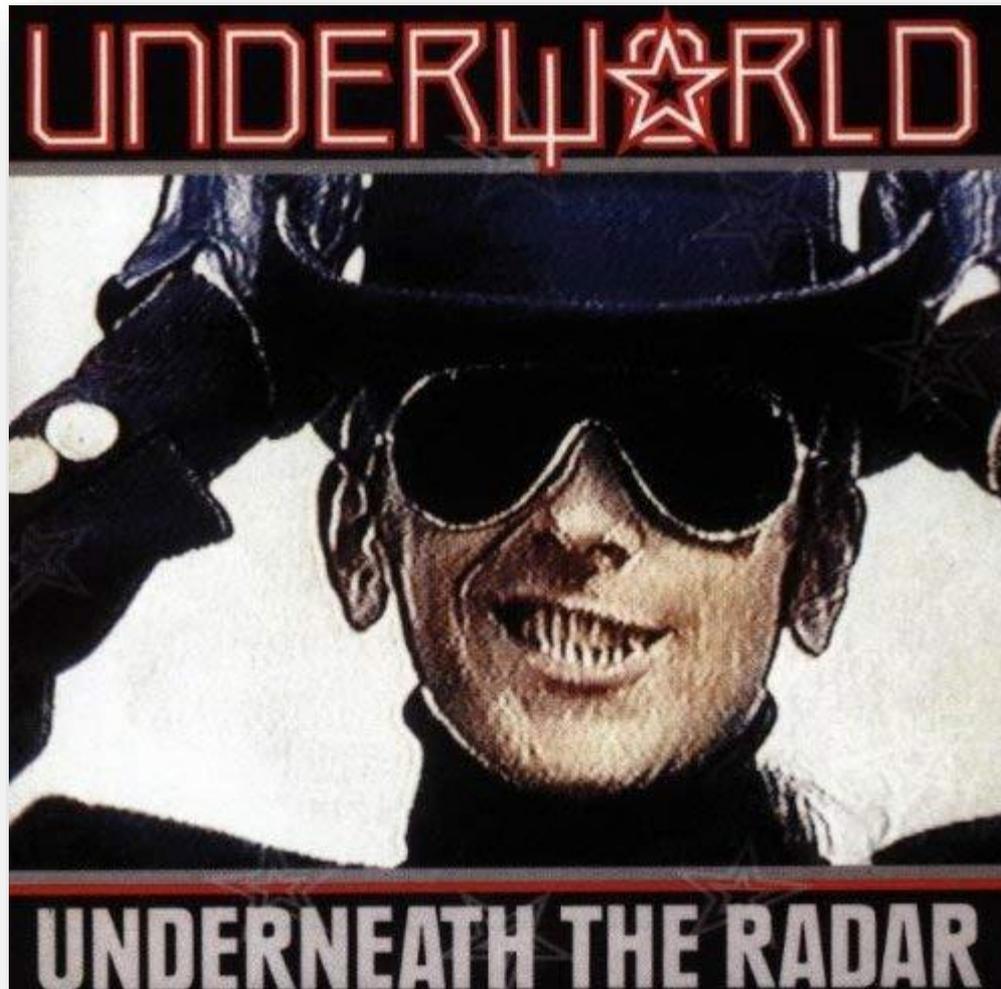
vorlesen



Wegen einer massiven DDoS-Attacke sind die Services großer US-Internetdienste, darunter unter anderem Twitter, Paypal, Netflix und Spotify, am Freitagabend in Teilen der USA und Europas zeitweise nicht zu erreichen.

Unknown.. Unseen.. We make no sign on screen..

PRIVACY
AND
SECURITY



Smart Home: Hacker übernehmen Kontrolle über Thermostat

09.08.2016 19:32 Uhr - Volker Briegleb

vorlesen



Dieses Thermostat heizt nur noch gegen Bitcoin. (Bild: [Ken Munro auf Twitter](#))

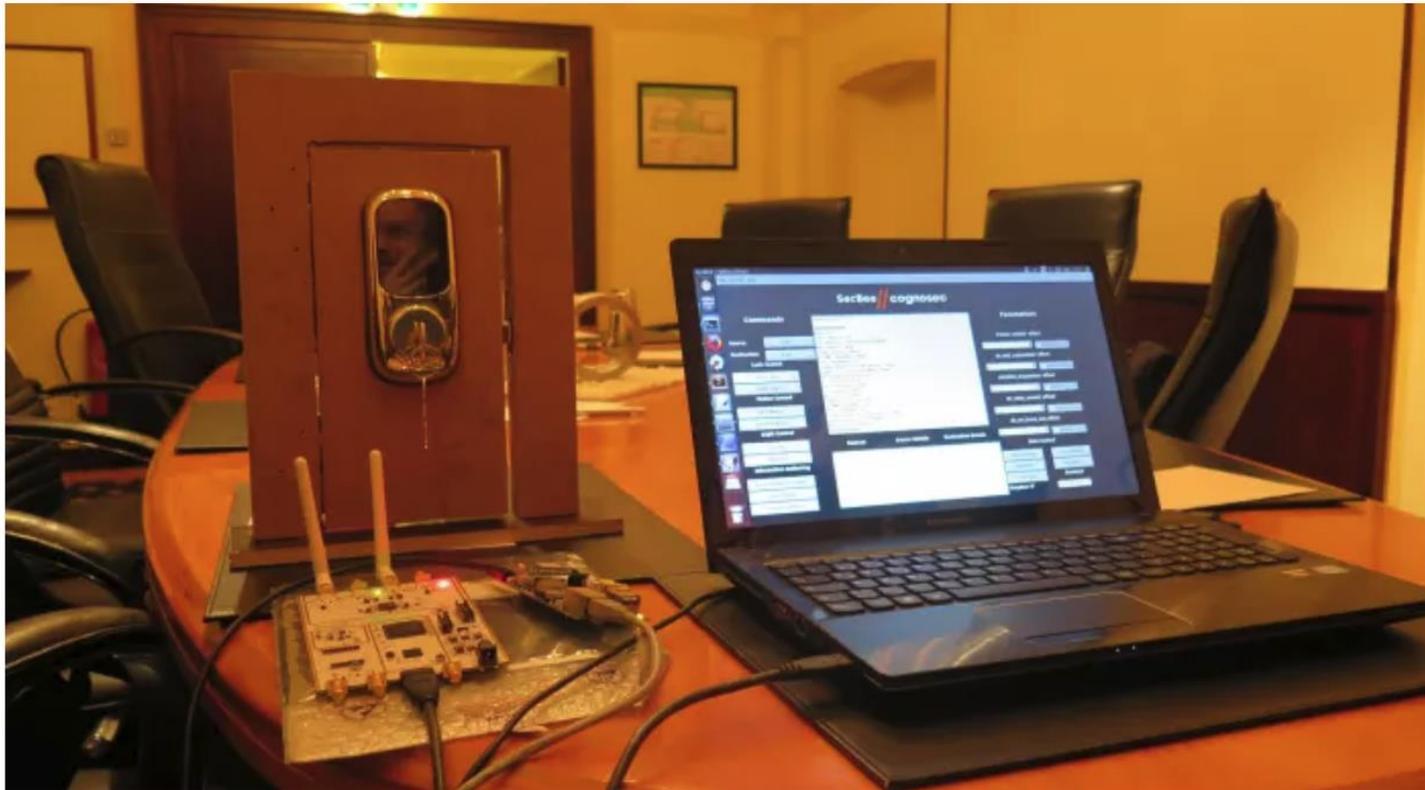
Die Sicherheitsexperten Andrew Tierney und Ken Munro haben auf der Hacker-Konferenz Def Con gezeigt, wie sie ein "smartes" Thermostat kapern können. Wirklich schwer hat es ihnen die Hardware dabei nicht gemacht.



Deepsec: ZigBee macht Smart Home zum offenen Haus

UPDATE

21.11.2015 13:01 Uhr - Daniel AJ Sokolov



Demonstration an einem handelsüblichen ZigBee-Türschloss. Raspbee wird vom SDR-Board USRP B210 (links mit weißen Antennen) unterstützt. (Bild: Daniel AJ Sokolov)

ZigBee-Funknetze weisen nach neuen Erkenntnissen von Sicherheitsforschern eklatante Sicherheitsmängel auf. Die Technik wird beispielsweise bei der Steuerung von Türschlössern eingesetzt.

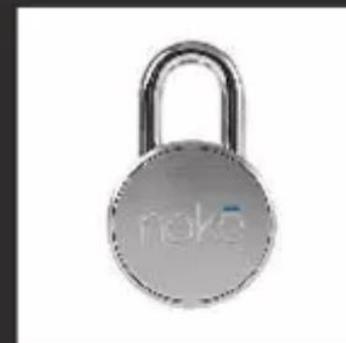
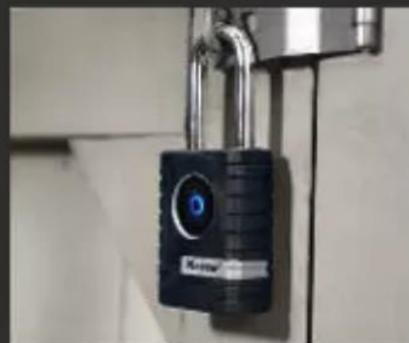
Smart Home: Bluetooth-Schlösser senden Passwort im Klartext

10.08.2016 18:50 Uhr – Volker Briegleb

vorlesen

>>> Uncracked Locks

- * Noke Padlock
- * Masterlock Padlock
- * August Doorlock
- * Kwikset Kevo Doorlock



An vier Schlössern bissen sich die Hacker die Zähne aus. (Bild: Präsentation)

Hacking-Spaß mit dem "smarten" Haushalt: Auf der Defcon 24 in Las Vegas haben Sicherheitsexperten gezeigt, mit welchen verhältnismäßig einfachen Mitteln so ein Smart Lock auszutricksen geht.

Smartes Türschloss August war zu gastfreundlich

01.04.2015 15:09 Uhr – Ronald Eikenberg

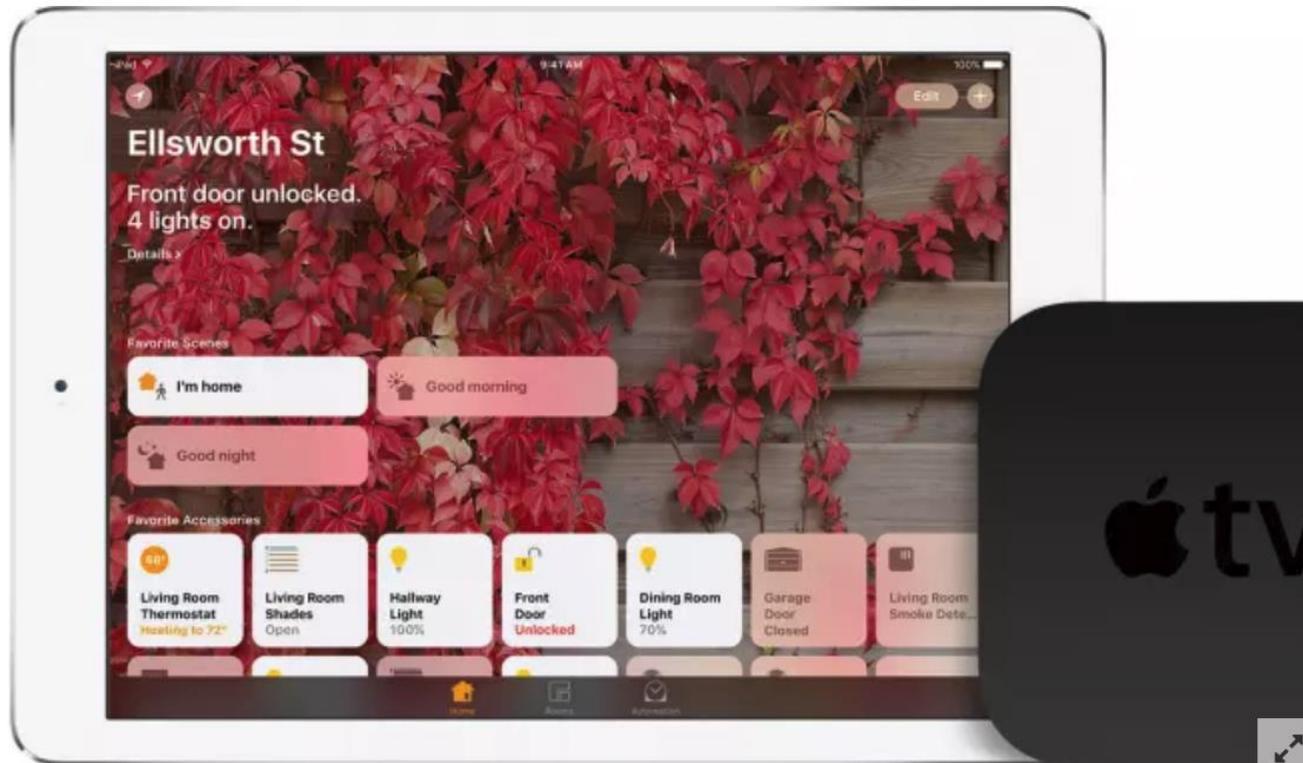


Durch eine Lücke in vernetzten Türschlössern konnten sich deren Besitzer unangemeldet untereinander besuchen.



Apples HomeKit: Schwachstelle erlaubte angeblich unerlaubten Fernzugriff ^{UPDATE}

08.12.2017 09:15 Uhr – Leo Becker



Die Steuerung der HomeKit-Geräte ist mit Apples vorinstallierter Home-App möglich – und per Siri. Für Automatisierung und Fernzugriff erfordern einen Home-Hub wie Apple TV. (Bild: Apple)

Mit Apples HomeKit vernetzte Smart-Home-Geräte – darunter auch Türschlösser – ließen sich einem Bericht zufolge von Unbefugten fernsteuern. Als Gegenmaßnahme hat Apple die Remote-Funktionalität für (berechtigte) Dritte abgedreht.

Früher...



Vorsicht
bei Gesprächen!
feind hört mit!

CES 2016: Glühbirne hört mit

30.12.2015 10:39 Uhr – Daniel AJ Sokolov

🔊 vorlesen



Lineup der Sengled-Birnen. Sengled Voice ist die zweite Birne von links. (Bild: Daniel AJ Sokolov)

Sengled versieht LED-Birnen mit Mikrophon. Für Überwachung sowie Sprachinteraktion mit der Cloud ist das richtig kommod.



Licht an, Licht aus: ZigBee-Wurm befällt smarte Glühbirnen

08.11.2016 15:40 Uhr – Fabian A. Scherschel



(Bild: Ronen et al.)

Das Internet der Dinge (IoT) sorgt mal wieder für eine skurrile Sicherheitslücke: Diesmal haben Forscher einen Wurm programmiert, der von einer Philips-Hue-Birne zur anderen springt und diese mit bössartiger Firmware bespielt.

34C3: Vernetzter Staubsauger-Roboter aus China gehackt

28.12.2017 11:00 Uhr - Stefan Krempel

vorlesen

Device Overview



(Bild: CC by 4.0 34C3 media.ccc.de)

Sicherheitsexperten haben das Verschlüsselungssystem des Saug-Roboters "Mi Robot Vacuum" von Xiaomi ausgehebelt. Dabei fanden sie auch heraus, welche Daten das Gerät lokal und in der Cloud speichert.



"HomeHack"-Angriff macht aus smarten Staubsaugern Spionage-Tools

26.10.2017 15:30 Uhr - Olivia von Westernhagen



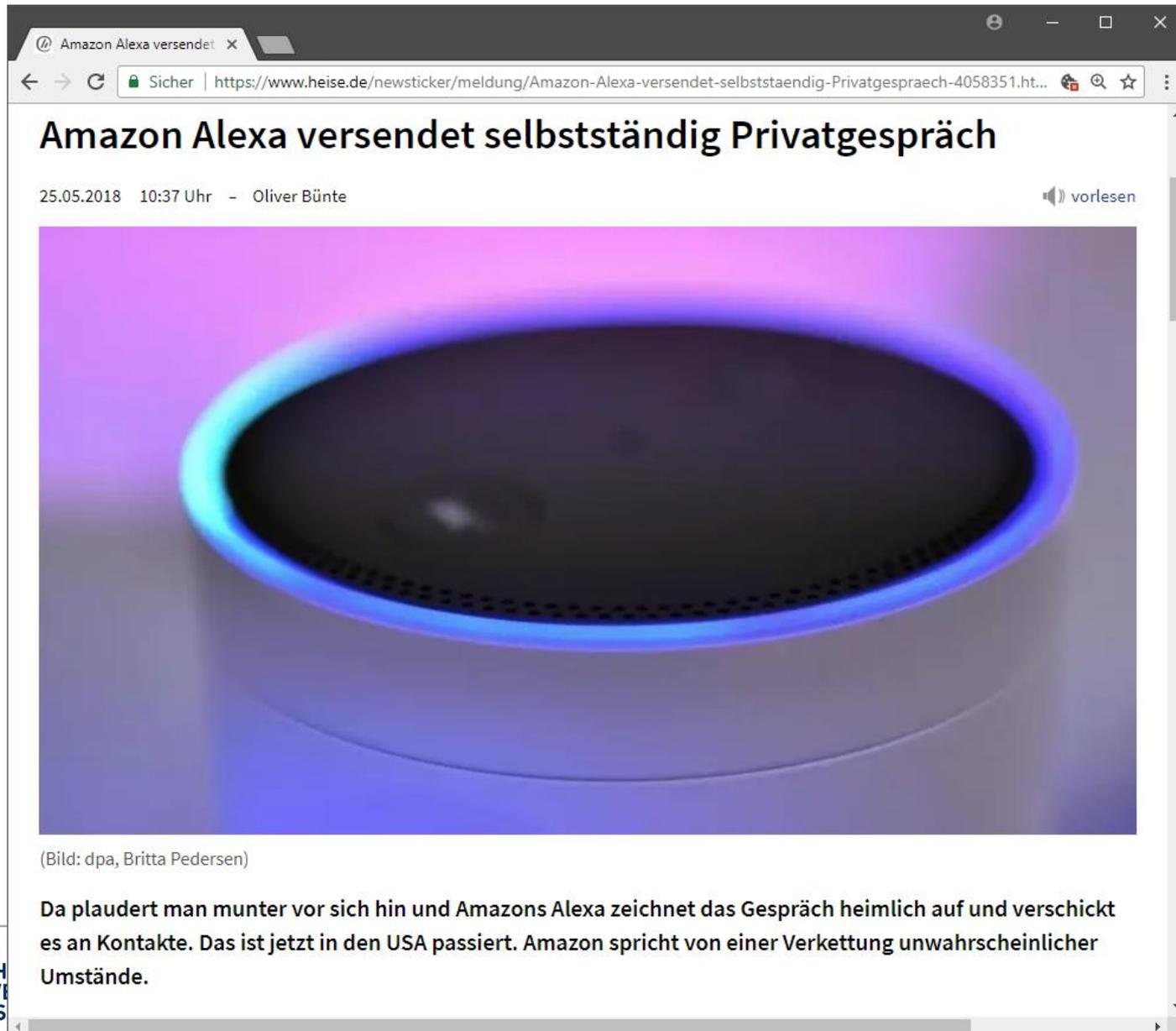
Im Video zeigt Check Point das Eigenheim eines Saugroboter-Besitzers aus der Perspektive eines Angreifers.
(Bild: [Check Point / YouTube](#))

Friedliche Haushaltshelfer im Smart Home können unter bestimmten Voraussetzungen zu fiesen Spionen werden: Ein Proof-of-Concept-Angriff auf eine Steuerungs-App für smarte LG-Geräte offenbarte gravierende Sicherheitsprobleme. Updates stehen bereit.

...und heute



...und heute



The screenshot shows a web browser window with the title "Amazon Alexa versendet" and a URL from heise.de. The article title is "Amazon Alexa versendet selbstständig Privatgespräch". The author is Oliver Bünte, dated 25.05.2018 at 10:37 Uhr. The main image is a close-up of an Amazon Echo smart speaker with its blue light ring glowing. Below the image is a caption "(Bild: dpa, Britta Pedersen)". The text below the image reads: "Da plaudert man munter vor sich hin und Amazons Alexa zeichnet das Gespräch heimlich auf und verschickt es an Kontakte. Das ist jetzt in den USA passiert. Amazon spricht von einer Verkettung unwahrscheinlicher Umstände."

Automatische Stimmanal x

Sicher | <https://www.heise.de/newsticker/meldung/Emotionserkennung-fuer-Therapie-und-Marketing-4058882.html>

Automatische Stimmanalysen übertreffen menschliche Experten

29.05.2018 07:30 Uhr - Eva Wolfangel vorlesen



(Bild: [Gino Crescoli](#), gemeinfrei)

Unsere Stimme verrät viel über uns – das zieht für Psychotherapie und Marketing ebenso nützliche wie erschreckende Anwendungen nach sich.



Autoindustrie tritt Smart-Home-Initiative bei

07.10.2015 16:52 Uhr - Axel Kossel

🔊 vorlesen



(Bild: Continental)

Vernetzte Autos mit der Haussteuerung sprechen zu lassen und E-Autos als Stromspeicher zu nutzen, klingt nach einer guten Idee. Doch dafür fehlen Standards, was die Automobilindustrie nun ändern will.



BMW steuert via IFTTT das Smart Home

27.01.2016 11:38 Uhr - Jo Bager

vorlesen

if  **then** 

Open your garage door as you're arriving home

by [bmwlab](#) 0 6

if  **then** 

Receive an email with a map to where you just parked

by [bmwlab](#) 520 11

if  **then** 

Turn on your hue lights when you arrive home

by [bmwlab](#) 53 4

if  **then** 

Send a text message to your kids when you're near

if  **then** 

Read your @mentions from your BMW dashboard

if  **then** 

When you are near the grocery store send a

Wer einen BMW mit ConnectedDrive Services fährt, kann jetzt mit einem Widget für den Automatisierungsdienst IFTTT zum Beispiel das Garagentor hochfahren lassen, wenn er auf dem Weg nach Hause ist.

Telekom Smart Home: BMW sendet Heiz-Kommando an Wohnung

IFA 05.09.2015 13:41 Uhr - Nico Jurrán

vorlesen



Gesteuert und kontrolliert via Apps der verschiedenen Marken über das Internet.

Verbunden via Funk mit allen kompatiblen Geräten verschiedener Marken.

Die Schnittstelle für alles: die QIVICON Home Base.

Nutzer der Telekom-App können jetzt das Beleuchtungssystem Lightify des Leuchtmittelherstellers Osram sowie alle vernetzen Geräte von Miele per Smartphone einbinden. Zudem spielen auch Smartwatches und ConnectedDrive von BMW mit.



Angreifer könnten aktuelle BMW-Modelle über Mobilfunk kapern

23.05.2018 10:02 Uhr – Dennis Schirmmacher



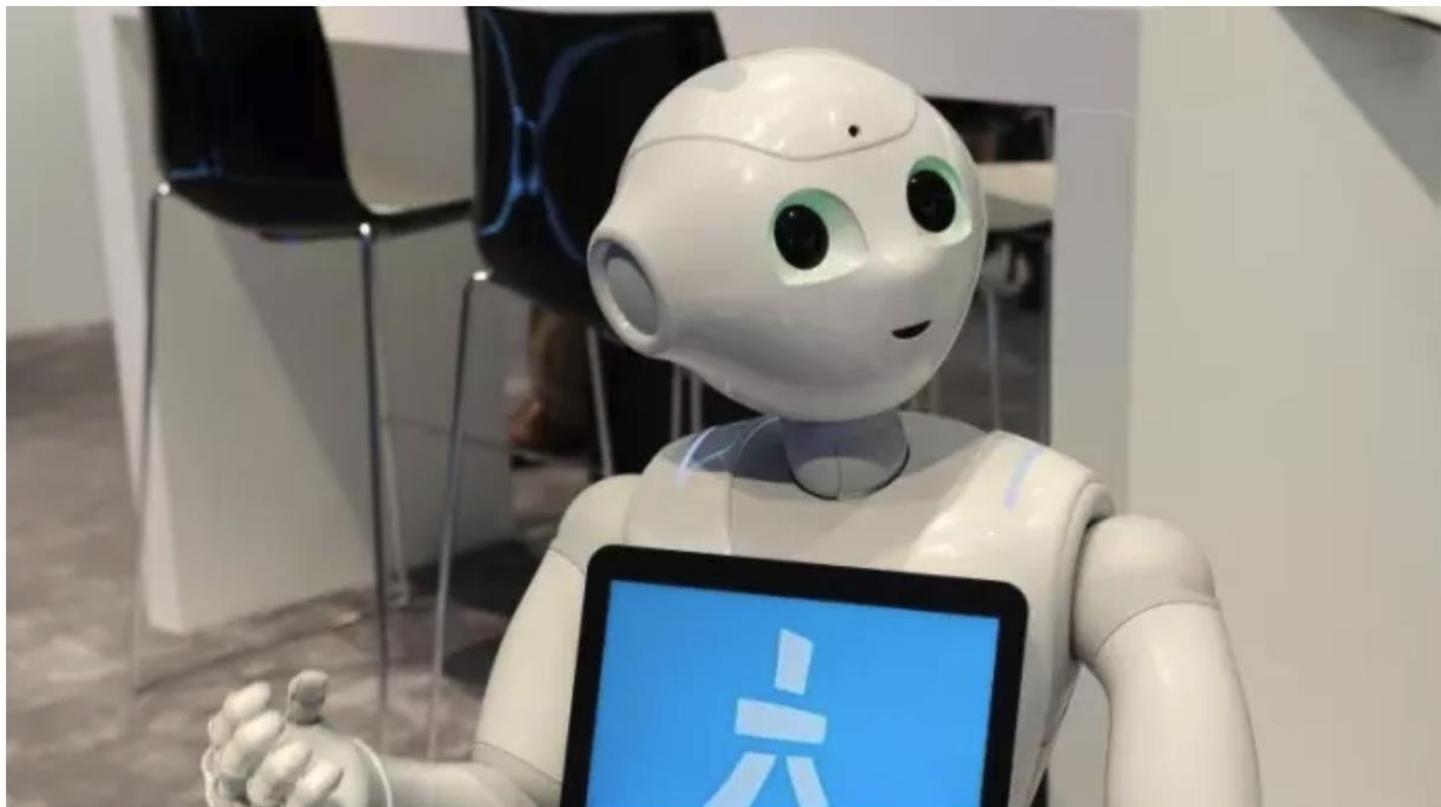
(Bild: [Keen Security Lab](#))

Sicherheitsforscher haben Sicherheitslücken im Infotainment-System von verschiedenen BMW-Modellen ausgenutzt und so die Kontrolle übernommen. Ein Angriff aus der Ferne ist aber ziemlich aufwendig.



Roboter Pepper kämpft mit massiven Sicherheitsproblemen

30.05.2018 15:24 Uhr - Oliver Bünte



Pepper ist von Haus aus freundlich, hat aber Sicherheitslücken, die ihn gefährlich machen können. (Bild: dpa, Andrej Sokolow)

Die "feindliche" Übernahme von einem Roboter ist ein Horrorszenario. Beim Service-Roboter Pepper ist das möglich, wie Wissenschaftler herausgefunden haben.



Sicherheitsprobleme & Fehler

Vermeidbare Fehler

- basieren auf (grob) fahrlässigem Verhalten
- Fehlerursachen sind lange und allgemein bekannt

- konkrete Implementierung
- Designfehler

—Vermeidungsaufwand gering, Beispiele:

- Verstoß gegen das „least privileges“-Prinzip
- Fehlende Überprüfung unsicherer Eingaben
- „Security by Obscurity“
- Mangelhaftes Notfall-Management

„Verzeihbare“ Fehler

—Aufwand zur Vermeidung mindestens hoch, Beispiele:

- bisher unbekannte Fehler in kryptographischen Verfahren / Protokollen
- Fehler in Prozessoren
- bisher unbekannte Fehler in Standardkomponenten

Wichtig: **Notfallplan!**

Verletzung von „least privileges“ — ungesicherte Remotezugänge



XXXairocon: Router von f x

www.heise.de/security/meldung/XXXairocon-Router-von-fuenf-Herstellern-mit-Standardpasswort-2793242.html

 **Alert!**

XXXairocon: Router von fünf Herstellern mit Standardpasswort

28.08.2015 14:18 Uhr - Fabian A. Scherschel  vorlesen



Unter anderem sind Asus und ZTE betroffen. Über den Telnet-Port können die Angreifer die betroffenen Geräte kapern. Die Hersteller lassen sich mit Updates viel Zeit.

Verletzung von „least privileges“ — ungesicherte Remotezugänge

IP-Kameras von Aldi

www.heise.de/security/meldung/IP-Kameras-von-Aldi-als-Sicherheits-GAU-3069735.html

Security > News > 7-Tage-News > 2016 > KW 2 > IP-Kameras von Aldi mit massiven Sicherheitslücken

 **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.

Gravierende Design-Fehler führen zu erheblichen Bedrohungen



heise.de Fatales Sicherheitsleck bei x

www.heise.de/security/meldung/Fatales-Sicherheitsleck-bei-Kabel-Deutschland-Vodafone-bedrohte-Millionen-Kabel-Kunden-3054052.html

Fatales Sicherheitsleck bei Kabel Deutschland/Vodafone bedrohte Millionen Kabel-Kunden

23.12.2015 12:00 Uhr - Ronald Eikenberg vorlesen



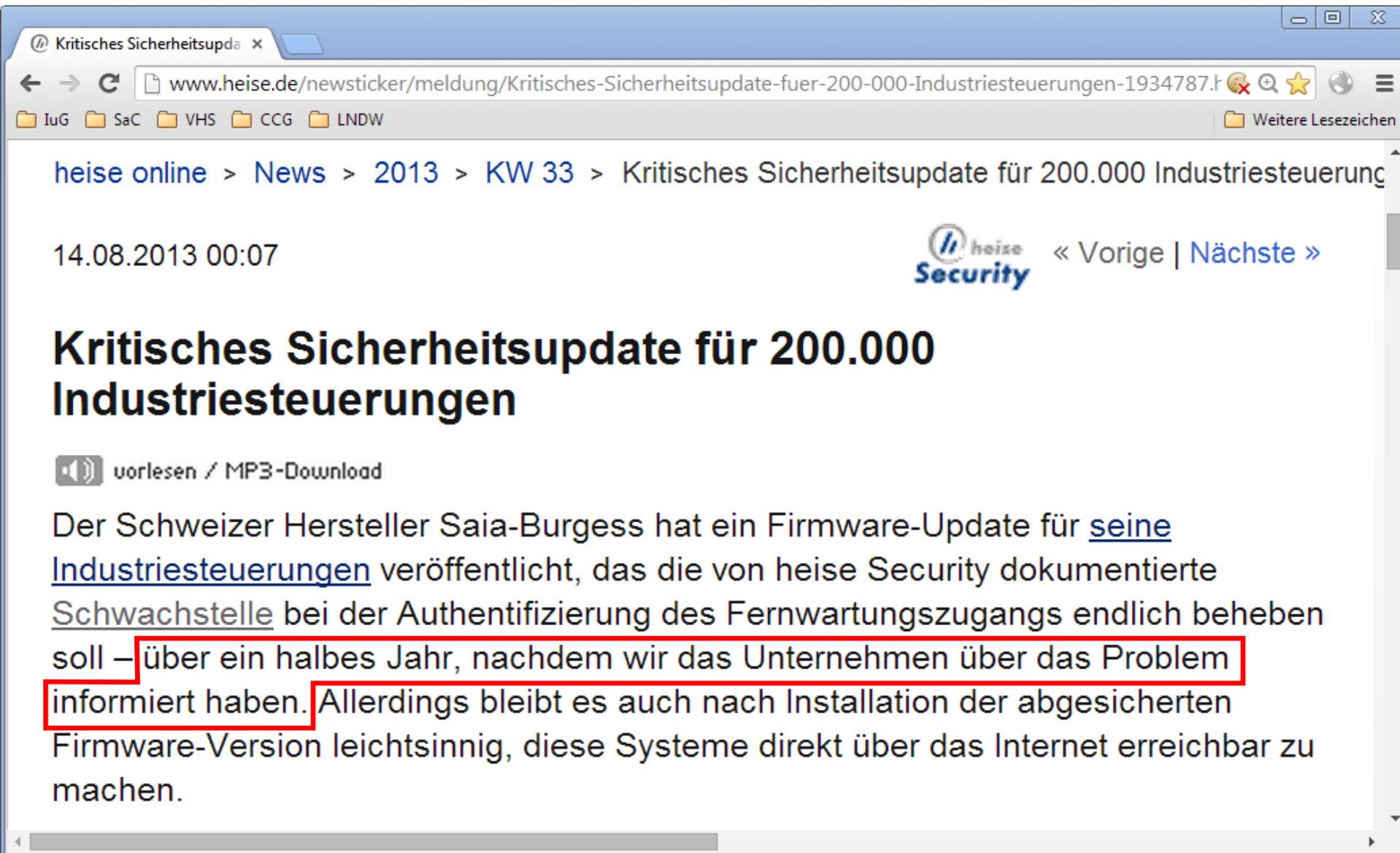
Kabel Deutschland



vodafone

Durch ein schlecht abgesichertes Wartungsnetz waren 2,8 Millionen Kunden von Kabel Deutschland/Vodafone bis vor kurzem akut gefährdet. Angreifer hätten VoIP-Anschlüsse übernehmen und Modems kapern können.

Fehlende Notfallpläne



The screenshot shows a web browser window with the following elements:

- Browser tab: "Kritisches Sicherheitsupda x"
- Address bar: "www.heise.de/newsticker/meldung/Kritisches-Sicherheitsupdate-fuer-200-000-Industriesteuerungen-1934787.f"
- Navigation icons: back, forward, refresh, home, search, star, globe, menu.
- Folder shortcuts: IuG, SaC, VHS, CCG, LNDW.
- Page breadcrumb: "heise online > News > 2013 > KW 33 > Kritisches Sicherheitsupdate für 200.000 Industriesteuerung"
- Date: "14.08.2013 00:07"
- Logo: "heise Security" with a blue diamond icon.
- Navigation: "« Vorige | Nächste »"
- Section Header: "Kritisches Sicherheitsupdate für 200.000 Industriesteuerungen"
- Audio icon and text: "vorlesen / MP3-Download"
- Main text: "Der Schweizer Hersteller Saia-Burgess hat ein Firmware-Update für seine Industriesteuerungen veröffentlicht, das die von heise Security dokumentierte Schwachstelle bei der Authentifizierung des Fernwartungszugangs endlich beheben soll – über ein halbes Jahr, nachdem wir das Unternehmen über das Problem informiert haben. Allerdings bleibt es auch nach Installation der abgesicherten Firmware-Version leichtsinnig, diese Systeme direkt über das Internet erreichbar zu machen."

Netzwerkscans sind möglich und effektiv



Scan in Mobilfunknetzen f X

www.heise.de/security/meldung/Scan-in-Mobilfunknetzen-foerdert-tausende-ungeschuetzte-Geraete-zu-Tage-1653619.html

[Security](#) > [News](#) > [7-Tage-News](#) > [2012](#) > [KW 30](#) > Scan in Mobilfunknetzen fördert tausende ungeschü

« Vorige | Nächste »

Scan in Mobilfunknetzen fördert tausende ungeschützte Geräte zu Tage

27.07.2012 00:07 Uhr – Uli Ries  vorlesen

Mit einem simplen Portscanner hat der deutsche Sicherheitsforscher [Collin Mulliner](#) die Netze von europäischen Mobilfunkanbietern untersucht. Ergebnis: Haufenweise Geräte wie Smart Meter, Straßenverkehrskontrollsysteme, KfZ-Ortungshardware oder GSM-/GPRS-Ethernet-Router. Schutz durch Passwörter? Fehlanzeige.

shodan.io — die etwas andere Suchmaschine...



Shodan

Shodan Developers Book View All... Show API Key

SHODAN

Explore Downloads Reports Enterprise Access Contact Us My Account

The search engine for **Webcams**

Shodan is the world's first search engine for Internet-connected devices

Create a Free Account Getting Started

Explore the Internet of Things
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

“Nicht mehr die Maschine sagt, was passiert, sondern der Rohling weiß, wie er bearbeitet werden möchte“ [Wolfgang Wahlster, Vorsitzender DFKI]

„...Ziel ist die intelligente Fabrik, die sich durch Wandlungsfähigkeit, Ressourceneffizienz und Ergonomie sowie die Integration von Kunden und Geschäftspartnern in Geschäfts- und Wertschöpfungsprozesse auszeichnet. Technologische Grundlage sind Cyber-physische Systeme und das Internet der Dinge.“

„**Industriespionage** ist ein ganz wichtiges Thema bei Industrie 4.0‘. Viele Unternehmen, mit denen er darüber spreche, schätzen diese Bedrohung größer ein als die Gefahr, dass Hacker die vernetzten Maschinen lahmlegen.“ [Wahlster, heise online, <http://heise.de/-2042943>]

„Viele Ingenieure haben nie richtig gelernt, Software zu entwickeln.“

[Dieter Rombach, Fraunhofer IESE, <http://heise.de/-2042943>]

—Anmerkung: ... und wissen wenig über IT-Sicherheit!

→ Einbeziehung von IT-Sicherheitsexperten in Design, Entwicklung und Betrieb!

spürbare Konsequenz bei Vertrieb / Betrieb von unsicheren IT-Systemen

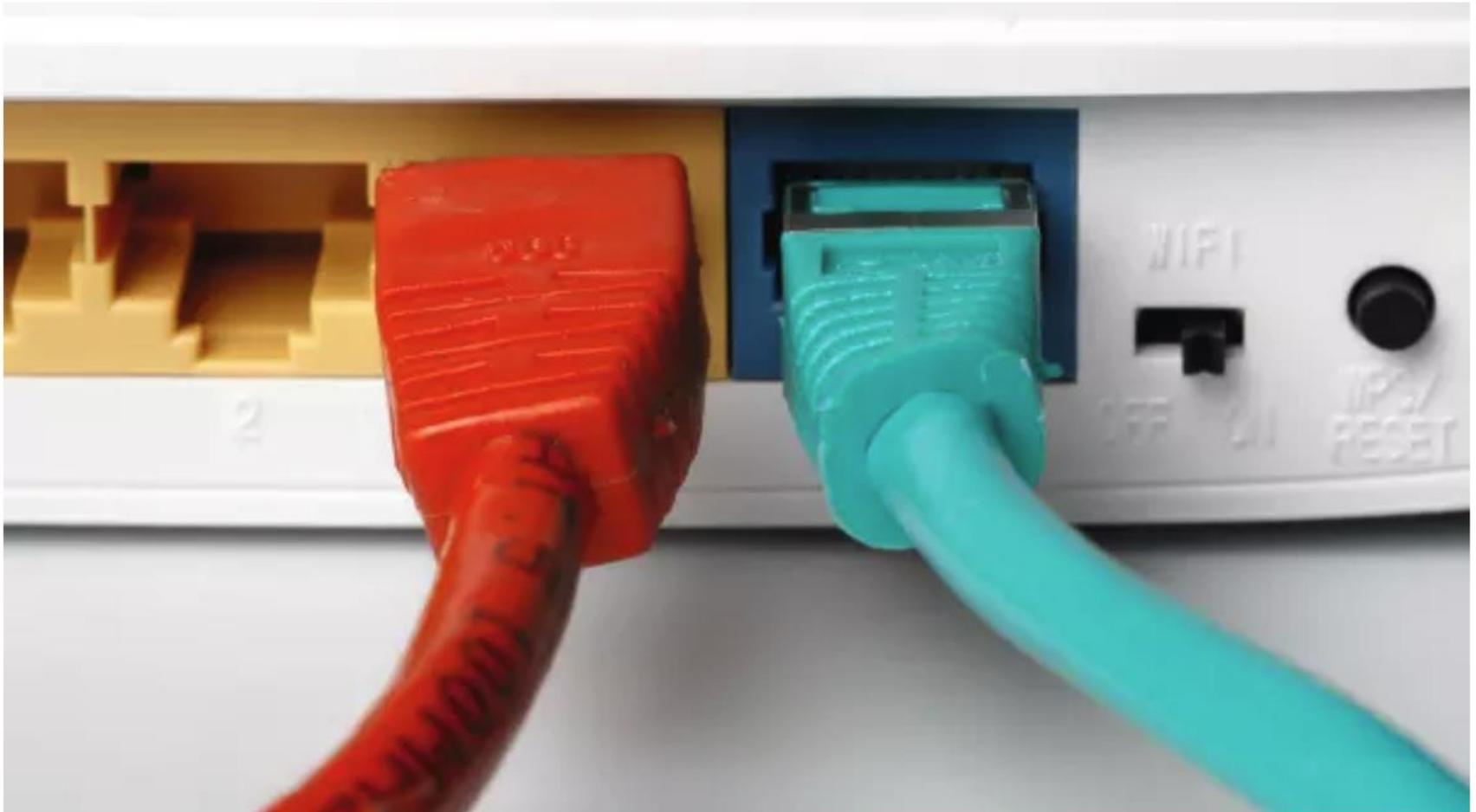
—(Produkt)haftung

—Schadenersatz ohne Nachweis eines konkreten Schadens

Verbraucherschützer wollen Garantie für Sicherheitsupdates bei Digitalprodukten

15.03.2017 06:39 Uhr - Stefan Krempl

vorlesen



Verbraucherschutzverbände haben zum "G20 Consumer Summit" einen Forderungskatalog und eine Studie vorgelegt, wonach 72 Prozent der Bürger in sechs Staaten die Datensammelwut von Firmen beklagen.

...wird in manchen Teilen der Welt schon umgesetzt

Asus muss 20 Jahre lang seine Router...

www.heise.de/newsticker/meldung/Asus-muss-20-Jahre-lang-seine-Routersicherheit-beaufsichtigen-lassen-3116487.html

Asus muss 20 Jahre lang seine Routersicherheit beaufsichtigen lassen

heise online 24.02.2016 12:45 Uhr - Andreas Wilkens vorlesen



Anders als von Asus angepriesen wiesen die Router der Taiwaner in den vergangenen Jahren heikle Schwachstellen auf. Weil dadurch US-Bürger Gefahren ausgesetzt waren, schritt die Federal Trade Commission ein.

Schluss

Nicht alles was geht ist automatisch gut...

Schwachstellen öffnen ist einfach

(sie zu schließen leider nicht immer)

Bewusstsein ist ein wichtiger Anfang – danach:

kommen Sie zu uns, wir helfen gerne!