

Reinventing Cyber Security

DENKANSTÖSSE ZU CYBER SECURITY

Prof. Dr. Reinhard Posch

Konventioneller Schutz reicht langfristig nicht aus

Die Herausforderungen der Cyber Security sind die Geschwindigkeit mit der neue Bedrohungen auf dem Horizont auftauchen in Kombination mit der eher trägen Situation beim privaten aber auch professionellen Benutzer.

Betroffene werden erst dann aktiv, wenn sie die Bedrohung „spüren“. Diese Situation führt auch zu zunehmender „Überwachung“ und es gilt diese Spirale zumindest in der Ganghöhe zu beschränken.

Das Resultat ist oft zunehmende Ratlosigkeit auf der einen Seite und, wie die Praxis zeigt, ein mehr als linearer Anstieg der empfundenen Überwachungsnotwendigkeit.

Das Vertrauen können wir nur dann stärken, wenn es gelingt, das Auseinanderentwickeln zu stoppen.

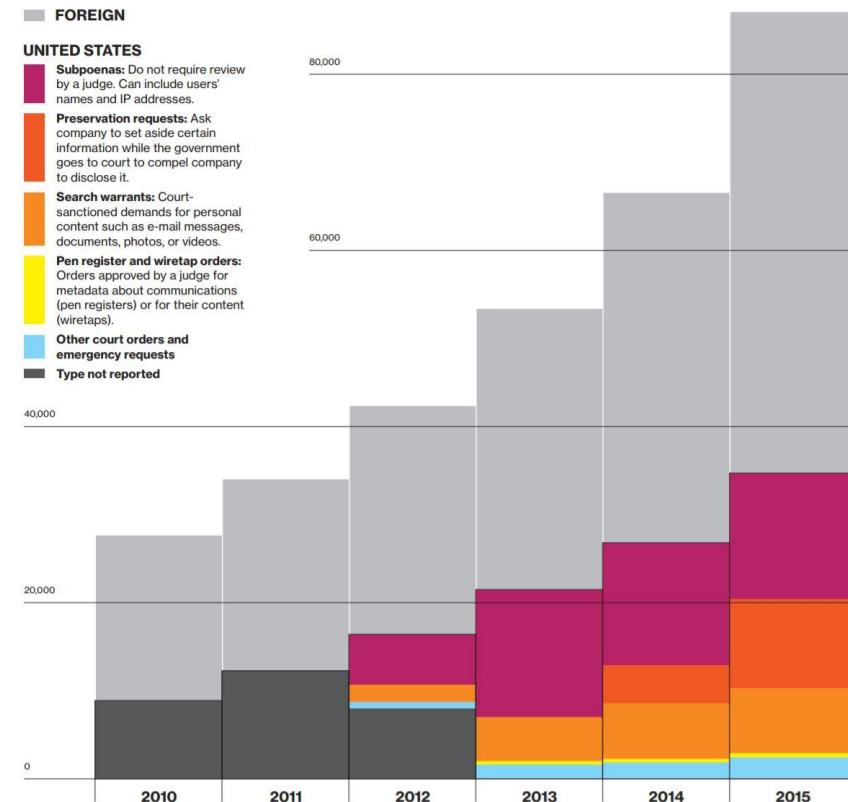
MIT TECHNOLOGY REVIEW
VOL. 120 | NO. 2

TECHNOLOGYREVIEW.COM

Upfront

Hand Over the Data

Governments are getting more user data from Internet companies every year, as people leave more traces of their lives online and law enforcement officials become increasingly reliant on that information. These figures, from Google's "transparency report," show how many times authorities in the U.S. and other countries have requested evidence about people who use the company's services.



Worldwide number of "Internet-connectable" devices

2011 ● **8.0 BILLION**

2012 ● **9.3 BILLION**

2013 ● **11.1 BILLION**

2014 ● **13.1 BILLION**

2015 ● **15.2 BILLION**

2016 ● **17.4 BILLION**

DATA FROM IHS JARVIS

IoT – das neue Risikopotential

Botnets will get larger
and more powerful simply
because the number of
vulnerable devices will go
**UP BY ORDERS
OF MAGNITUDE
OVER THE NEXT
FEW YEARS.**

BOTNET OF THINGS

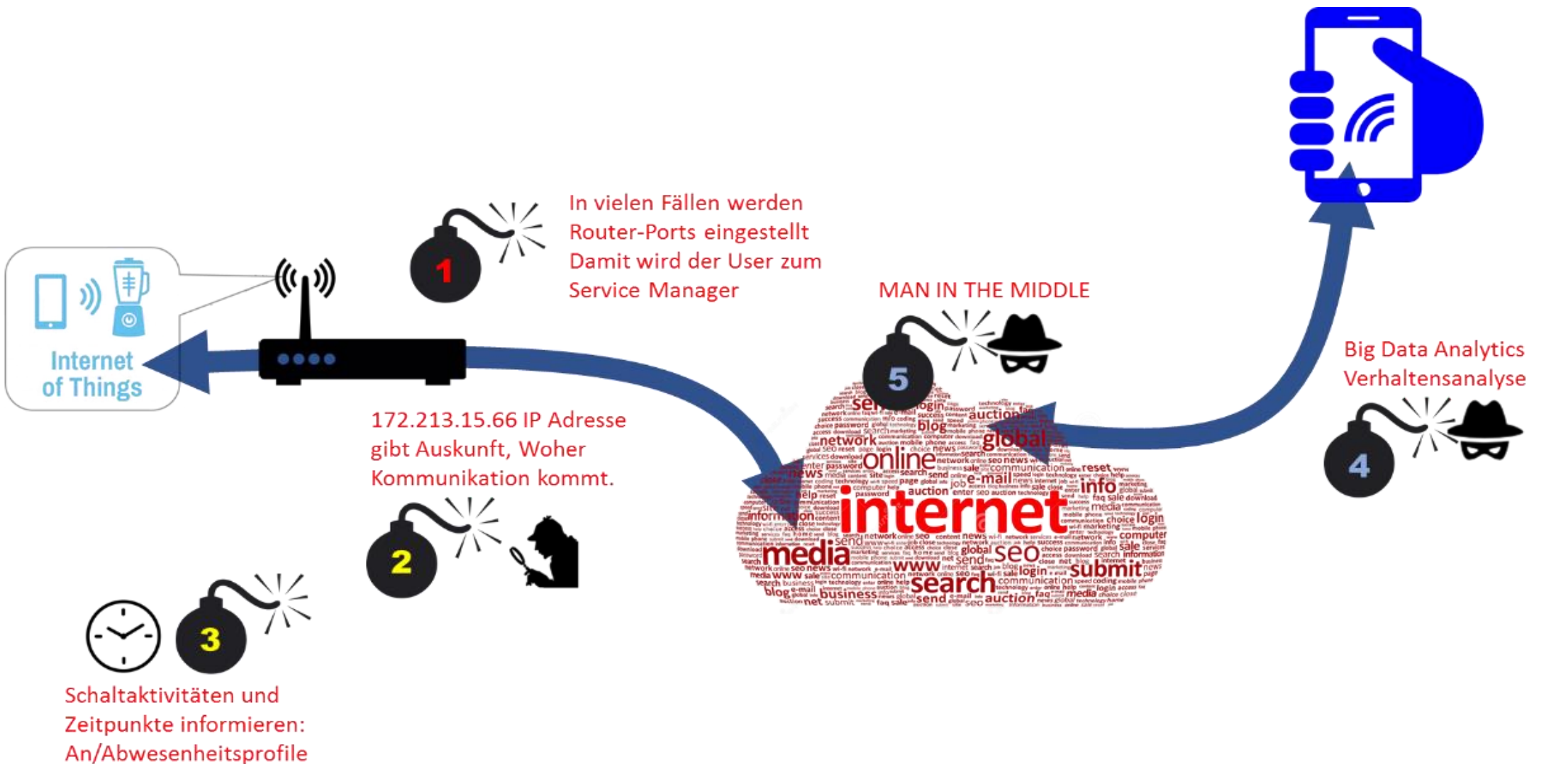
Im Falle der gekaperten Videokameras wurde uns ein erster Vorgeschmack serviert, was durch das Internet der Dinge auf uns zukommt.

IoT ist oft ein „UNATTENDED SERVICE“ ohne Systembetreuung.

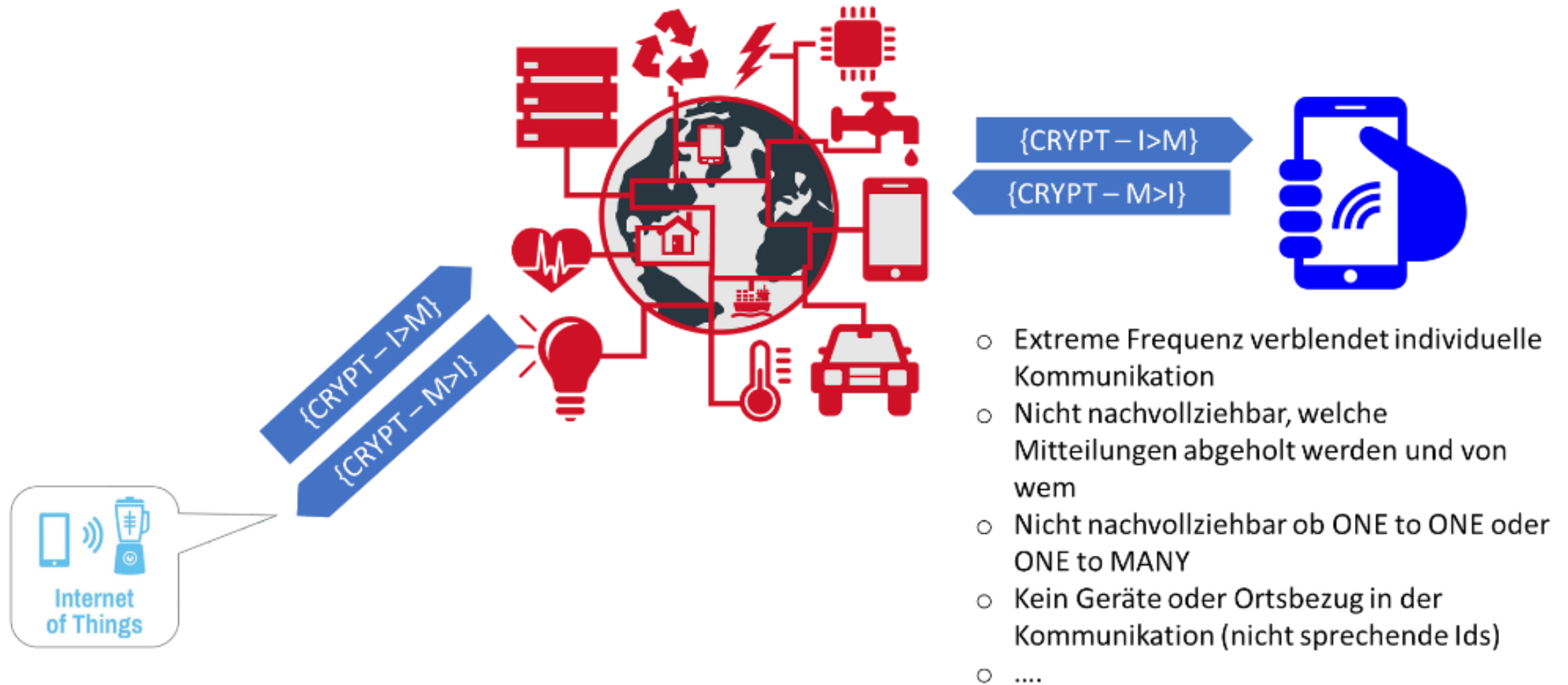
Wenn der Verkehr dichter wird, brauchen wir Regeln und Mechanismen, die im Normalfall auch sicherstellen, dass diese Regelungen auch wirksam sind.

Basis dafür ist jedenfalls ein gesteigertes Bewusstsein, welche Gefährdung mit dem Betrieb einhergehen kann. Zumindest eine minimale Beratung beim Kauf wäre von herausragender Wichtigkeit.

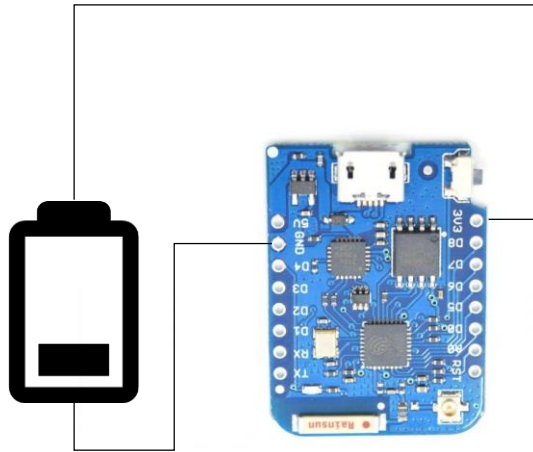
IoT - WAS NUN?



IoT – Was nun



FAKE HOTSPOT – CYBERTHREAD OF THINGS



Kosten des Angriffs: **3€ frei Haus**

Software: **Open Source**

Größe: **3x2,5 cm
2,9 Gramm**

- Sammeln einer Liste von offenen bzw. durch „ACCEPT“ verbindbaren WLANS
- Anbieten von „wahrscheinlichen“ WLANS mit derartigen Namen und mit Einstiegsseite gleichen Aussehens
- Bei Click von WEITER: „ Das hätten Sie nicht machen sollen ich bin ein Belehrungsbuddy aber der Angreifer hätte hier folgendes Machen können:
 - Daten sammeln
 - Etwas auf dem Gerät speichern / installieren
 -

Eine USB-Batterie (zum Nachladen von Handies – als Giveaway de facto gratis) reicht für einen 12 Stunden Betrieb und bei Nutzung von Powersave viel länger.

„USER EXPERIENCE 1“

A

freewave

Willkommen bei Freewave!

Durch das Klicken auf „Verbinden“ bestätige ich, die **Nutzungsbedingungen** gelesen zu haben und sie zu akzeptieren.

FLUGHAFEN GRAZ
... und so nah ist die Welt

Verbinden

Flughafen Graz

Nutzungsbedingungen

Der Betreiber des Standorts, der Freewave anbietet und Freewave ermöglichen Ihnen (= Nutzer) die Nutzung des Internets. Damit dieses Angebot auch weiterhin bestehen bleibt, sind einige Regeln zu beachten: Der Nutzer verpflichtet sich, diesen Internetzugang nur in dem vom Betreiber des Standorts vorgesehenen Bereich zu nutzen. Der Nutzer verpflichtet sich, jede Nutzung zu unterlassen, welche die öffentliche Ordnung und Sicherheit oder die Sittlichkeit gefährdet oder welche gegen Gesetze verstößt und andere Internetnutzer belästigt oder verängstigt. Der Nutzer verpflichtet sich insbesondere, diesen Internetzugang nicht für File-Sharing Programme zu nutzen. Außerdem verpflichtet sich der Nutzer, Bandbreite nicht exzessiv zu nutzen, da dieser Internetzugang mit anderen Nutzern geteilt wird. Freewave behält sich vor, einzelne Endgeräte (z.B. Laptops, Notebooks, PDAs, etc) für die Verwendung von Freewave sowie bestimmte Ports zu sperren. Dem Nutzer sind alle Risiken des Internets bekannt und er ist allein für seinen Schutz (z.B. aktuelles Antiviren-Programm, Nicht-Starten von verdächtigen Programmen/Dateien, etc) verantwortlich. Freewave übernimmt keine Haftung für Fehler, Störungen oder Schäden, die durch die Nutzung des Internets über Freewave oder durch Konfigurationsänderungen des Endgeräts durch den Nutzer entstehen. Freewave übernimmt keine Gewähr dafür, dass die angebotenen Dienste ohne Unterbrechung zugänglich sind und dass die gewünschten Verbindungen immer hergestellt werden können. Der Ersatz von Schäden jeglicher Art, inklusive Folgeschäden Dritter und Schäden aus Ansprüchen Dritter ist in jedem Fall, soweit gesetzlich zulässig, ausgeschlossen.

© 2017 Freewave GmbH. Alle Rechte vorbehalten.

B

DIES IST EINE AWARENESS AKTIVITÄT VON A-SIT
ES WURDE KEIN SCHADEN IRGENDWELCHER ART VERURSACHT!

IRGENDWO HABEN SIE UNVORSICHTIG GEKLICKT

A-SIT
Zentrum für sichere
Informationstechnologie - Austria

„USER EXPERIENCE 2“

A

BUNDESKANZLERAMT  **ÖSTERREICH**

Security Information

Please note that, due to the public nature of the service offered, all the data you send or receive can also be viewed by third parties, unless the connection you are using is a secure one. This particularly applies to services that require registration, such as webmail.

General Information

Introduction

Until further notice, the Bundeskanzleramt will place at the disposal of visitors certain hotspots with the identifier "BKA-Gast" (Federal Chancellery Visitor). These hotspots will enable persons equipped with a WiFi-enabled device to gain a connection to the Internet via WiFi in accordance with the currently applicable conditions.

WiFi is a local network which provides a cable-free connection between the hotspot and the user's device. The radio range, transmission speed and data transmission capacity between the hotspot and the user's device all depend on the distance, the choice of location, the number of persons simultaneously using the same hotspot, the surrounding infrastructure and the user's device, as well as on various sources of disturbance such as radio shadows and other circumstances and influences.

Help and support

If any problems occur or visitors have any further questions regarding the use of the above-mentioned Internet services, they should contact the Bundeskanzleramt during office hours (weekdays: 8 a.m. to 6 p.m.) on the IT hotline (Tel.: + 43 1 53115/202777).

B

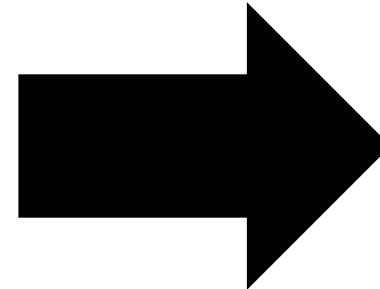


AUFWAND FÜR DEN ANGREIFER

Für den Angriff ist das Wissen eines ca. zweitsemestrigen Studenten notwendig, etwas C++ und ein wenig Phantasie

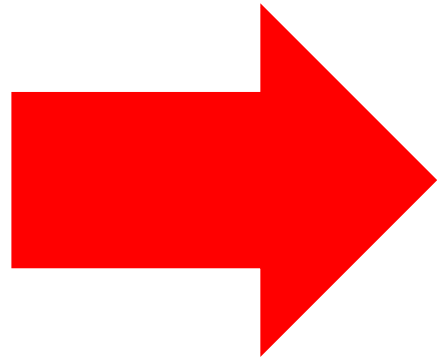
- Google Search – „Captive Portal“ etwa 2 Stunden
- ca. 180 LINES OF CODE davon ca 160 direkt aus Sample Code aus dem Internet, inkl. Testen 3 Stunden
- Download der Starting Page des Access Point und anpassen der Links bzw. direkt einbetten der Bilder mit einem Online Tool „convert to dataurl“ erzeugbar. 1 Stunde

➔ BINGO



```
1 // Captive Portal
2 // Author: [Redacted]
3 // Version: 1.0
4 // Description: A simple Captive Portal for a Raspberry Pi.
5 // It will show a splash screen and redirect the user to a website.
6 // It will also show a countdown timer.
7 // It will also show a progress bar.
8 // It will also show a status bar.
9 // It will also show a settings menu.
10 // It will also show a help menu.
11 // It will also show a about menu.
12 // It will also show a settings menu.
13 // It will also show a help menu.
14 // It will also show a about menu.
15 // It will also show a settings menu.
16 // It will also show a help menu.
17 // It will also show a about menu.
18 // It will also show a settings menu.
19 // It will also show a help menu.
20 // It will also show a about menu.
21 // It will also show a settings menu.
22 // It will also show a help menu.
23 // It will also show a about menu.
24 // It will also show a settings menu.
25 // It will also show a help menu.
26 // It will also show a about menu.
27 // It will also show a settings menu.
28 // It will also show a help menu.
29 // It will also show a about menu.
30 // It will also show a settings menu.
31 // It will also show a help menu.
32 // It will also show a about menu.
33 // It will also show a settings menu.
34 // It will also show a help menu.
35 // It will also show a about menu.
36 // It will also show a settings menu.
37 // It will also show a help menu.
38 // It will also show a about menu.
39 // It will also show a settings menu.
40 // It will also show a help menu.
41 // It will also show a about menu.
42 // It will also show a settings menu.
43 // It will also show a help menu.
44 // It will also show a about menu.
45 // It will also show a settings menu.
46 // It will also show a help menu.
47 // It will also show a about menu.
48 // It will also show a settings menu.
49 // It will also show a help menu.
50 // It will also show a about menu.
51 // It will also show a settings menu.
52 // It will also show a help menu.
53 // It will also show a about menu.
54 // It will also show a settings menu.
55 // It will also show a help menu.
56 // It will also show a about menu.
57 // It will also show a settings menu.
58 // It will also show a help menu.
59 // It will also show a about menu.
60 // It will also show a settings menu.
61 // It will also show a help menu.
62 // It will also show a about menu.
63 // It will also show a settings menu.
64 // It will also show a help menu.
65 // It will also show a about menu.
66 // It will also show a settings menu.
67 // It will also show a help menu.
68 // It will also show a about menu.
69 // It will also show a settings menu.
70 // It will also show a help menu.
71 // It will also show a about menu.
72 // It will also show a settings menu.
73 // It will also show a help menu.
74 // It will also show a about menu.
75 // It will also show a settings menu.
76 // It will also show a help menu.
77 // It will also show a about menu.
78 // It will also show a settings menu.
79 // It will also show a help menu.
80 // It will also show a about menu.
81 // It will also show a settings menu.
82 // It will also show a help menu.
83 // It will also show a about menu.
84 // It will also show a settings menu.
85 // It will also show a help menu.
86 // It will also show a about menu.
87 // It will also show a settings menu.
88 // It will also show a help menu.
89 // It will also show a about menu.
90 // It will also show a settings menu.
91 // It will also show a help menu.
92 // It will also show a about menu.
93 // It will also show a settings menu.
94 // It will also show a help menu.
95 // It will also show a about menu.
96 // It will also show a settings menu.
97 // It will also show a help menu.
98 // It will also show a about menu.
99 // It will also show a settings menu.
100 // It will also show a help menu.
```

ANGIFF UND SCHADENSPOTENTIAL

[illegible]

**DAS HIER BESCHRIEBENE
ERZEUGT NOCH KEINEN SCHADEN!!**

- Modifikation könnte aber:
 - ELEMENTE AUF DIE DEN BROWSER ZUGREIFEN KANN SAMMELN (GESPEICHERTE PASSWORTE ETC.)
 - EXPLIZITE ZUSTIMMUNG KANN ÜBER HIDDEN CLICKS ERREICHT WERDEN.
 - DA AUF ALLE DOMÄNEN REAGIERT IST DIE DOMÄNENBINDUNG VON BROWER STORAGE IRRLEVANT(Aufwand im Stundenbereich – Das „Thing mit Internet“ hat 256MB nicht flüchtigen Speicher)
- Mit etwas Aufwand kann auch ein Man in the Middle erzeugt werden – z.B. für Banking etc. UVAM.....

**UND WENN MILLIONEN WEBCAMS MIT
DERARTIGEM „INFIZIERT“ SIND**

???

Technologien und Services

KRYPTOGRAPHIE

Praktisch alle Sicherungsverfahren im Internet haben Kryptographie zur Basis.

Ansätze, die sich – auch zu vermeintlich positiven Zwecken – „dazwischen stellen“ können eine besondere Gefahr sein.

BEISPIEL – QUALIFIZIERTE WEBSITES

Wenn alle mitmachen hat dies ein besonderes Potential – erfordert allerdings auch ähnlich wie eID besondere Behandlung in Router etc.

.....

eID

Identifikation von Services und Teilnehmer „MÜSSEN“ gestärkt werden. Eine Vielzahl von Angriffen nutzt Schwächen der Authentifizierung aus.

BEISPIEL BLOCKCHAIN

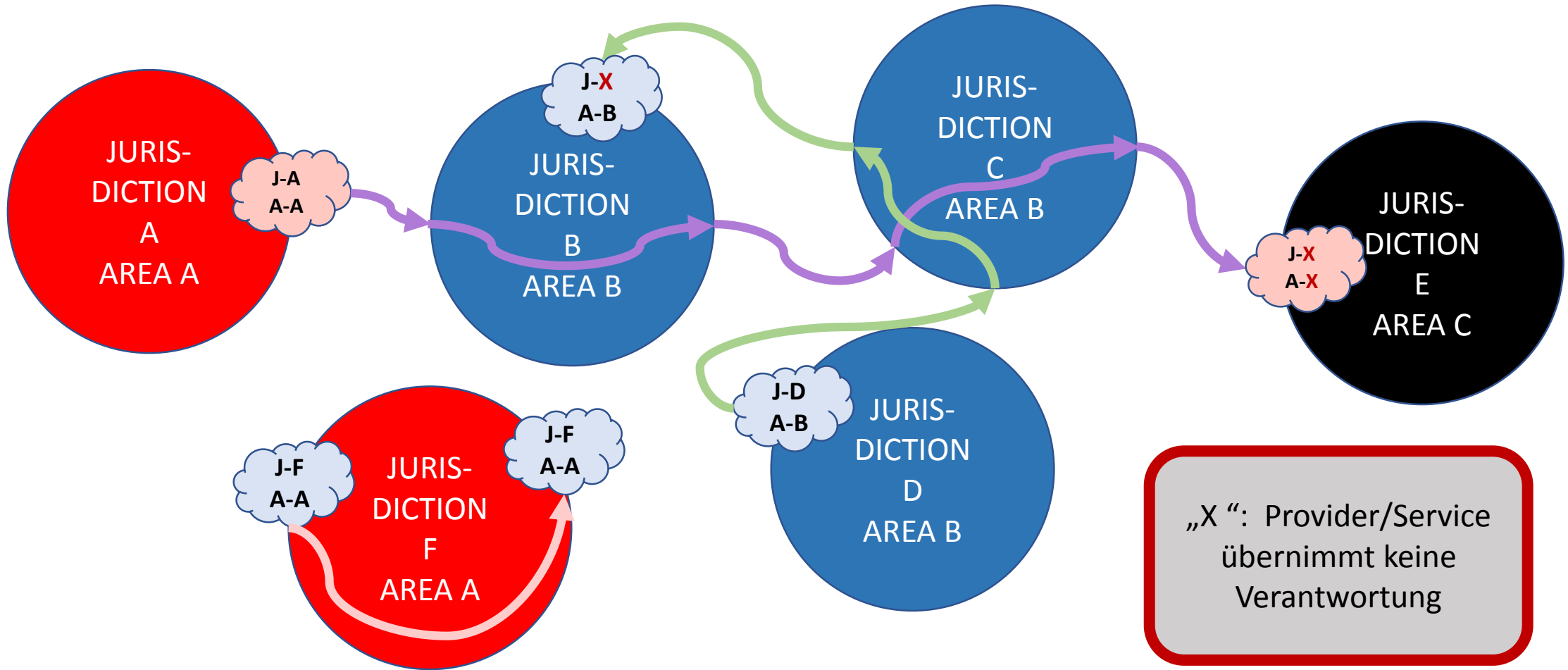
Als digitales LOGBUCH kann diese Technologie in vielen Bereichen – nicht nur im Bezahlbereich helfen, zwischen „GUT“ und „MALVERS“ zu unterscheiden.

.....

Jurisdiction Awareness

- Zentrale Aspekte im Zusammenhang mit Cyber Security sind IDENTITÄTEN und DAS FESTSTELLEN DER ZUORDENBAREN RECHTSORDNUNG.
- eIDaS bietet dazu Lösungen an – eID und ggf. Website Authentication.
- IoT wird dieses Thema noch verstärken
- Nahezu alle Angriffe haben eine **grenzüberschreitende Komponente**

Jurisdiction Awareness



Jurisdiction Awareness

**PROVIDER FÜGT DEM PAKET INFORMATION
ZUR HERKUNFT VERANTWORTLICH AN**

**BROWSER, ANWENDUNGEN UND
APPS KÖNNEN HERKUNFT PRÜFEN**

**SERVICES KÖNNEN
VERANTWORTUNG
ÜBENEHMEN**

Vielleicht ist es Zeit ganz Neues anzudenken



Die alten Technologien
von Übermorgen!

Dezentrale Strukturen.
könnten mehr Kontrolle
und Datenschutz bieten

Blockchain
CRYPTO
ENABLER FÜR
INNOVATIONEN

MIT TECHNOLOGY REVIEW
VOL. 120 | NO. 2

TECHNOLOGYREVIEW.COM

Upfront

One Startup's Vision to Reinvent the Web for Better Privacy

Blockstack's system would let you control your own personal data—for example, by revoking a site's access to it.

Venture capitalist Albert Wenger has done well by investing in Web businesses—he was an early backer of Etsy and Tumblr. But at his urging, Union Square Ventures, where he is a partner, is backing a company founded on the principle that the Web needs a rethink.

"We're living in a time period where the new incumbents like Amazon, Google, and Facebook have firmly established themselves and are near monopolists in their markets," says Wenger. "If we want a long-term, open playing field for innovation, we're going to need new, decentralized infrastructure."

Blockstack recently received \$4 million in funding from USV and others to try to establish that more open playing field. The startup is working on open-source software that will create a kind of parallel universe to the Web we know—one where users have more control of their data. Later this year, Blockstack will release software that lets you surf sites and apps created for this new digital domain using your existing Web browser. You will still be able to load sites by clicking links or typing Web addresses, but instead of creating accounts with each site, as people do with Google or Facebook, users of sites built on Blockstack's system will control their own digital identity (or identities). To use a site that

needs your information, you will grant access to a profile under your control alone. If you want to stop using a service, you can revoke its access to your profile and data and take it elsewhere. Sites will run all their code on your computer, in the browser.

"We're trying to turn the existing model on its head," says Ryan Shea, CEO and cofounder of Blockstack. "You can try to work with the existing model from within, but sometimes it's easier to step outside of it and build something new from a clean slate." Blockstack's vision is made possi-

ble by an identity system built to be independent of any one company, including Blockstack. It uses the digital ledger, or blockchain, underpinning the digital currency Bitcoin to track usernames and associated encryption keys that allow a person to control his or her data and identity. A collective of thousands of computers around the globe maintains the blockchain, and no one entity controls it. Blockstack's system uses the blockchain to record domain names, too, meaning there's no need for an equivalent to ICANN, the body that oversees Web domains today. Software built on top of the name and ID systems gives people control over their data. Microsoft is already collaborating with Blockstack to explore uses for its platform.

Blockstack's tweaks on how the Web functions may seem abstruse. But Shea argues that low-level features of the Web's design, like the lack of a built-in, independent identity system, are at the root of problems such as the dominance of large companies and the latitude they have to make use of user data. He says that companies will still be able to seek profits on the new platform, but power will be tilted more in favor of users.

The dream of a new kind of online sphere faces some significant obstacles, though. Bitcoin's design has proved to lack the capacity needed for a widely used currency—and it's not clear how to build similar, fully decentralized systems that have it, says Emin Gün Sirer, an associate professor at Cornell University. Such systems might also struggle to resolve disputes over things like copyright claims on domain names, he says. —Tom Simonite



Blockchain und Health-Records

Blockchain und CRYPTO INNOVATIONSENABLER

GESUNDHEITSDATEN

dezentral und auf
verschiedenste
Institutionen verteilt

GESUNDHEITSDATEN

hoher Bedarf an
Veränderungskontrolle

GESUNDHEITSDATEN hoher Bedarf an Vollständigkeit

Elektronische Akte,
Gesundheitsdaten

KANDIDAT FÜR BLOCKCHAIN

Das NEUE - CHANCE UND GEFAHR

