TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Informatik Professur für Datenschutz und Datensicherheit

Cybercrime: Notwendigkeiten für sichere Datenübertragung auch im Alltag

Tim Lackorzyński, Stefan Köpsell
<tim.lackorzynski@tu-dresden.de, stefan.koepsell@tu-dresden.de>

Technisches Fachgespräch
„Sichere Datenübertragung für den Gebäudebetrieb und die Mieterkommunikation“

Berlin, 11.10.18

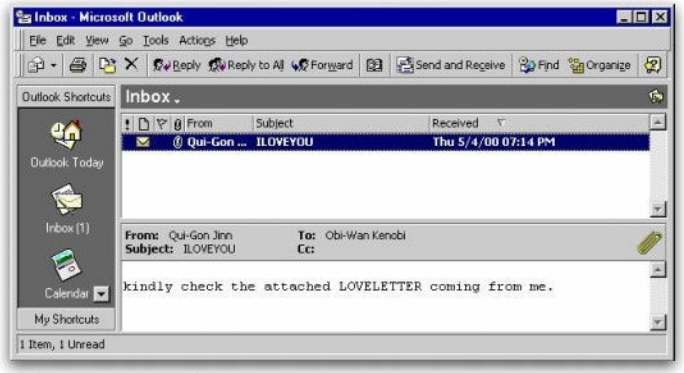
zwanzig20 PARTNERSCHAFT FÜR INNOVATION

GEFÖRDERT VOM Bundesministerium für Bildung und Forschung

Stand der IT Heute

Die Versäumisse von Gestern...

- IT-Infrastruktur ohne Sicherheit
- Folge:
  - Viren, Würmer
  - Spam
  - Windows



(Bild:Sophos)

- Neueste Beispiele:
  Erpressungstrojaner à la Locky, Petya, TeslaCrypt

(Bild:heise Security)

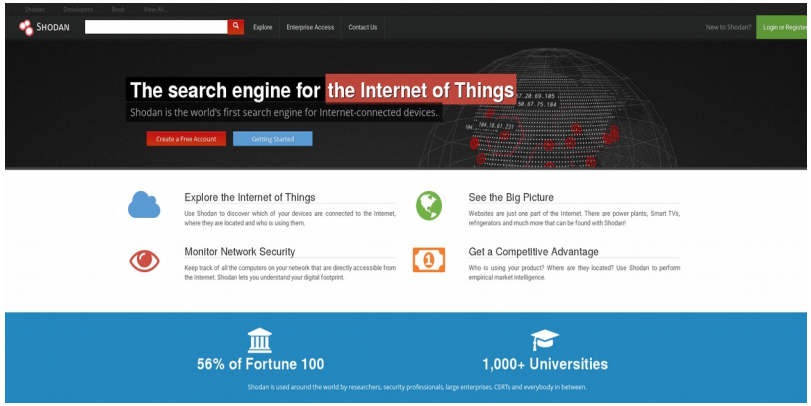
Stand der IT Heute

… die Fehler von Heute …

- IoT?
- Smart Home?
- Smart Grids?
- Industrie 4.0?

→ Vernetzung von Geräten, die nicht vernetzt werden sollten:

- SCADA
- Krankenhausinfrastruktur
- Hochöfen
- …



(www.shodan.io)

(Spiegel Online)

Stand der IT Heute und Morgen

… das Bedrohungspotential von Morgen

Beispiele:

- Stuxnet
- NotPetya

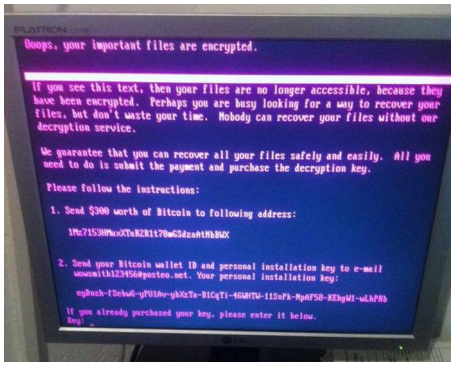
(Bild:Ralph Langner)

Professionalisiertes Umfeld:

- Staaten:
  - USA: NSA, TAO…
  - (Russland: APT28)
  - Israel: Unit 8200
  - China: PLA Unit 61398…
  - Nordkorea: Bureau 121
  - (Syrien: Syrian Electronic Army)
  - …
- Privatwirtschaft:
  - Hacking Team
  - Gamma International Ltd./GmbH
  - Vupen
  - Zero-Day-Märkte, Exploit Kits, Bot-Netze, Silk Road…

Stand der IT Heute und Morgen

- **… das Bedrohungspotential von Morgen**



(Bild:Wikipedia)

- NotPetya [1]
  - Maskiert als „normale“ Ransomware
  - **Eigentlich: Cyberangriff auf Ukraine** (höchstwahrscheinlich) aus Russland
  - Betroffene, u.a.:
    - Unternehmen: Antonov
    - Mobilfunk: Kyivstar, Vodafone Ukraine, lifecell
    - Transport/Energie: Kiev Metro, UkrGasVydobuvannya, WOG, Kyiv International Airport
    - Banken: Prominvestbank, Ukrsotsbank, KredoBank, Oshchadbank...
    - TV-Sender: STB, ICTV, ATR
  - Kollateralschäden, u.a.:
    - Maersk [2]
    - Merck & Co.
  - Schaden wird auf insgesamt $10 Mrd. geschätzt

[1] https://en.wikipedia.org/wiki/2017_cyberattacks_on_Ukraine

[2] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Stand der IT Heute und Morgen

- **… das Bedrohungspotential von Morgen**

- McAfee:
  - *„Cybercrime is a growth industry.”*
  - *„The combination of high value, low risk, and low ‘work factor’ […] makes cybercrime a winning proposition.” [1]*
- Allianz rechnet mit 10x-Wachstum bei Versicherungen gegen Cybercrime [2]

Das Internet ist Spielwiese für unterschiedlichste Interessen:

- **Militärische**
- **Politische**
- **Monetäre**

[1] http://www.mcafee.com/hk/resources/reports/rp-economic-impact-cybercrime2.pdf

[2] https://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf

IT von Morgen: Internet of Things

Was?
- Intelligente Geräte:
  - Smart Watches, TV, Light bulbs...
- Intelligente Netze:
  - Smart Grid, Smart Home, Industrie 4.0

(Bild:www.cbronline.com)

Warum?
- Komfort, Automation, Effizienzsteigerung

... und eigentlich ...
- „IoT ist die Zukunft.“
- „Das nächste große Ding!“

Aber:
- Keine richtige Problemdefinition
- Diffuse Ziele: Sensor-Aktor-Systeme, Vernetzung, Intelligenz

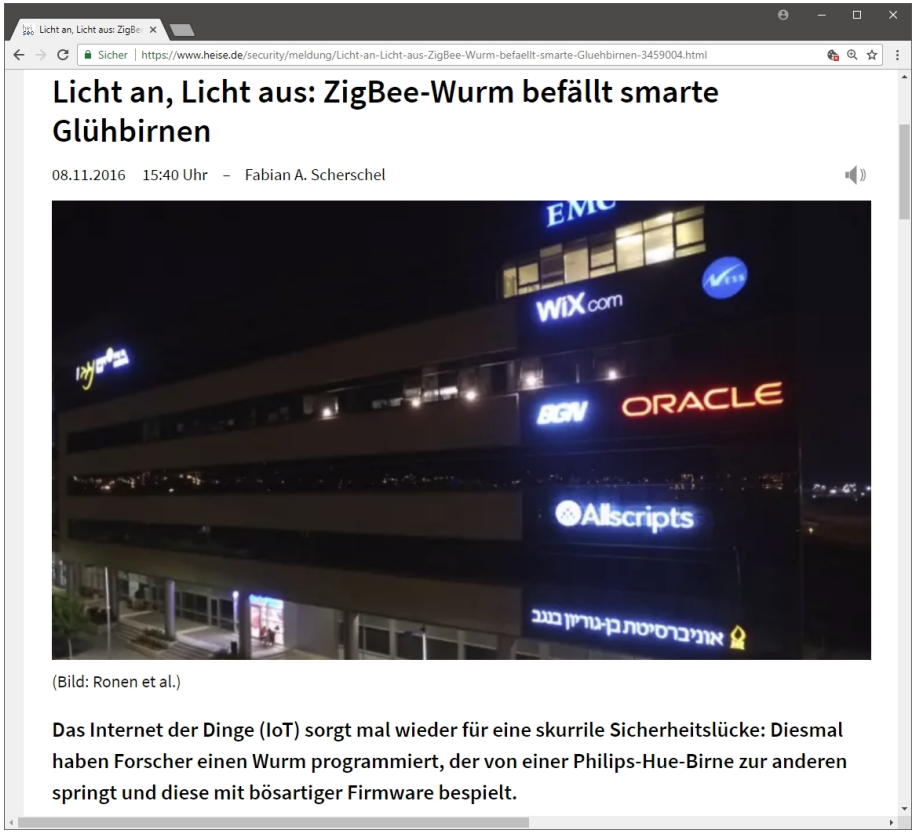
→ „Erster sein“ bzw. „dabei sein“ ist Muss
→ „Was“ und „Wie“ ist zweitrangig

Internet of Things - Beispiele

Philips Hue
- Endlich buntes Licht per Handy einstellen

Vorteile:
- Neuartig
- Smart
- Bequem

Nachteile:
- Neuer Angriffsvektor geöffnet



(Bild:heise online)

Internet of Things – Beispiele

Hello Barbie

- Puppe, die mit Kindern reden kann
- Wie: Mikrofon plus Internetanschluss

Vorteile:

- Neuartig
- Smart

Nachteile:

- Wanze im Kinderzimmer
- Hersteller hat direkten Kanal zu Kind
- Wurde schon gehackt

- Ähnliche Puppe namens Cayla wurde bereits verboten

(Bild:www.mattel.com/)

Internet of Things - Beispiele

IoT-Geräte:

- Sehen aus, wie Puppen, Glühbirnen, Fernseher ...
- ... sind aber Computer

- Laufen mit Standardsoftware (Linux)
- Besitzen Kommunikationsschnittstellen (WLAN, Bluetooth, ZigBee...)

→ IoT-Geräte sind „normale“ PCs

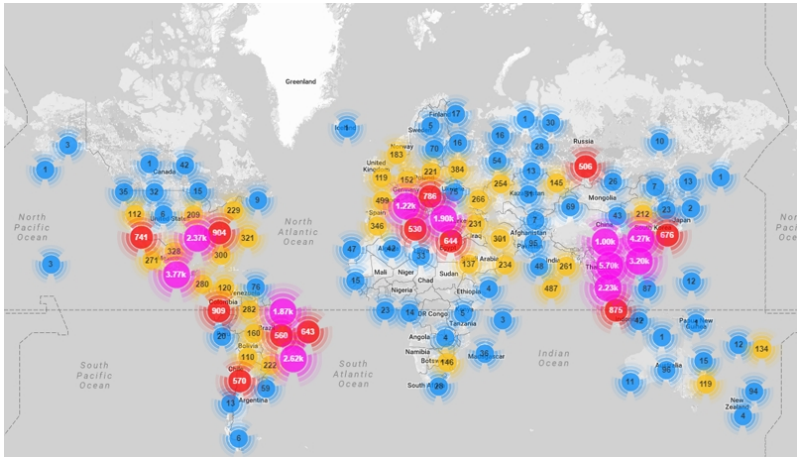
→ „Normale“ Teilnehmer am Internet

(Bild:www.somersetrecon.com)

Internet of Things - Beispiele

Mirai

- Malware, welche gezielt bestimmte Heimrouter und IoT-Geräte infizierte
- Genutzt für DDos-Angriffe auf u.a. Website von Brian Krebs
- ~200.000 betroffene Geräte
- Erzeugter Traffic: 620 Gbps



(Bild:www.incapsula.com/)

- Angriffsvektor:
  - Standardpasswörter, z.B.:

```
root      xc3511
root      vizxv
root      admin
admin     admin
root      888888
root      xmhdipc
root      default
root      juantech
root      123456
root      54321
…
```

Internet of Things – Stand Heute

Hype IoT:

- Angeheizt durch große Mengen Fördergelder/Investitionen in IoT
- Erzeugt Druck Marktanteile zu gewinnen
  → Druck Produkte zu entwickeln/verkaufen

Start-up-Mentalität:

- Kein Budget für ordentliche Softwareentwicklung
- Stattdessen ständig neue Features bauen und Marketing
- IoT-Geräte bestehen aus Hard- und Software
  - Software hat untergeordnete Priorität
  - Softwarequalität und -sicherheit hat keine Priorität
- Fire-and-forget: Software beim Kunden wird nicht gepflegt, neue SW mit neuer HW-Revision neu verkauft
- Jegliche persönliche Daten haben Geldwert, selbst wenn man sie nicht unmittelbar monetarisieren kann, d.h. Anreiz alles zu sammeln ist da

Internet of Things – In Zukunft

Trend:

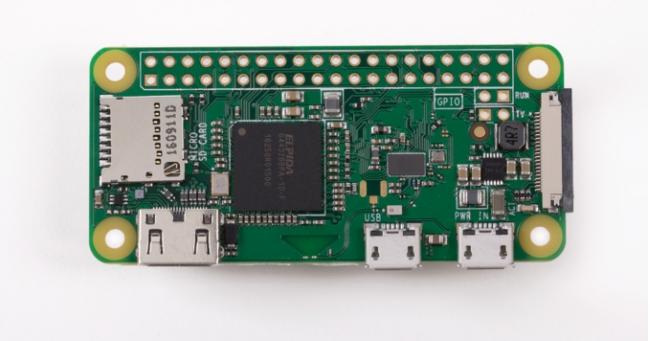
- Hardware-Plattformen immer kleiner und billiger
- Breitbandiger Anschluss ans Internet

Technische Folgen:

- Milliarden neue Geräte im Internet
  → Riesige Zahl an angreifbaren Geräten
- Enorme Angriffspotentiale
- Angriffe werden zunehmend auch Besitzer der IoT-Geräte selbst betreffen

Gesellschaftliche Folgen:

- Überall vorhandene, unsichtbare, ans Internet angeschlossene Wanzen...
- ... welche Menschen überwachen und deren Verhalten ständig analysieren



(Bild:www.raspberrypi.org)

(Bild:www.iotphils.com)

Zusammenfassung

- IoT wird bedeutendste Infrastruktur der Zukunft
  - IoT hat direkten Einfluss auf physische Sphäre
  - IoT wird den Menschen selbst betreffen, zuerst Wearables, später Kybernetik

- Cyberwar im „normalen“ Internet findet schon statt
  - Cybercrime ist absoluter „Wachstumsmarkt“

- Riesiges Potential für Missbrauch

- **IoT heißt IT-System**
  → Paradigmen aus IT-Welt müssen umgesetzt werden
  - Verschlüsselung, Authentikation
  - SW-Update-Zyklen
  - SW-Management-Prozesse
  - (BSI-)Zertifizierungen für kritische Infrastrukturen
  - Sicherheit ist ein Prozess!

Vielen Dank!

Tim Lackorzyński
<tim.lackorzynski@tu-dresden.de>