SCHUTZ KRITISCHER SYSTEME UND INFRASTRUKTUREN

Peter Weidenbach

peter.weidenbach@fkie.fraunhofer.de

AGENDA

- Kurzvorstellung: Fraunhofer FKIE
- Awareness Live Demo
- Stand Heute
- IT-Sicherheitsdreiklang
  - Prävention
  - Detektion
  - Reaktion
- Praxistipps

FRAUNHOFER FKIE

Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie







Fraunhofer FKIE erforscht und entwickelt Modelle, Methoden und Werkzeuge für
Kontroll- und Steueraufgaben in vernetzten Systemen («Vernetzte Operationsführung«)

Forschungsgebiete

- Sensordatenfusion
- Kommunikationssysteme
- Informationstechnik für Führungssysteme
- Mensch-Maschine-Systeme
- Systemergonomie
- Kognitive Mobile Systeme
- Cyber Analysis & Defense
- Cyber Security
- Usable Security and Privacy

Standorte	Wachtberg und Bonn
Gegründet	1963
Fraunhofer	seit 8/2009
Mitarbeiter	> 400
Budget	> 30 Mio €
Institutsleiter	Prof. Dr. Peter Martini
Website	www.fkie.fraunhofer.de

FRAUNHOFER FKIE

Mission Statement

A Printer Ransomware

- Live Demo

Einzelfall?

Alert!

Intel stopft neue Si
Management Engir

21.11.2017 11:37 Uhr – Christof Winde

Intel-Chipsatz B150

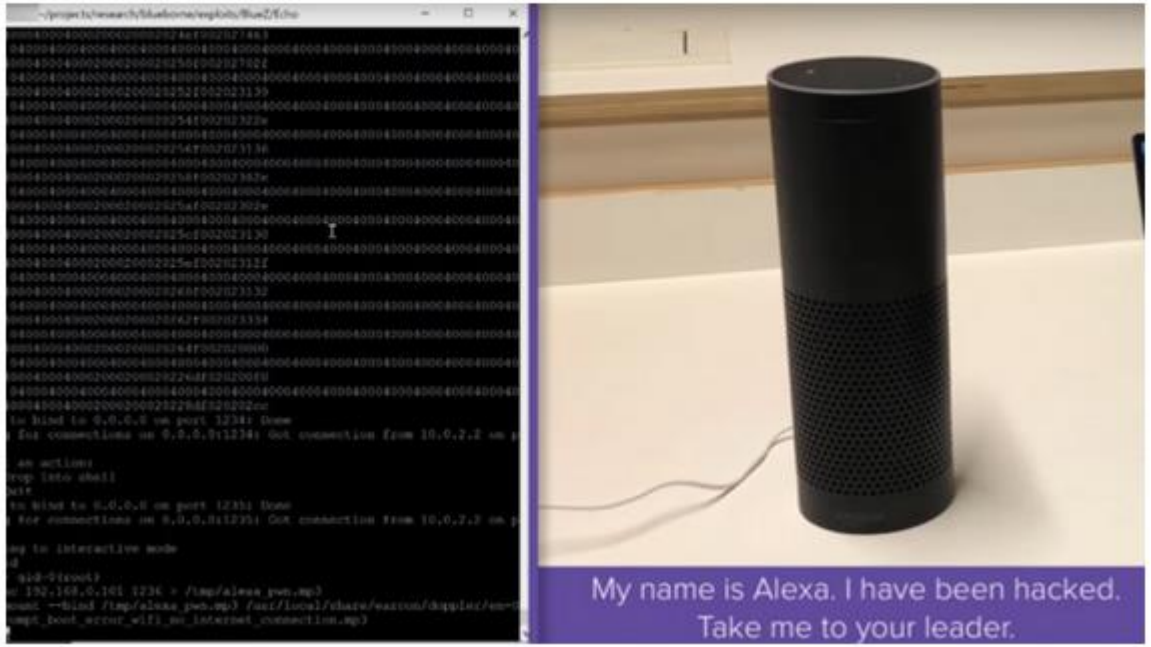
(Bild: Fortinet)

Alert!

BlueBorne: Bluetooth-Schwachstellen auch in Amazon Echo und Google Home

16.11.2017 15:45 Uhr – Olivia von Westernhagen

vorlesen

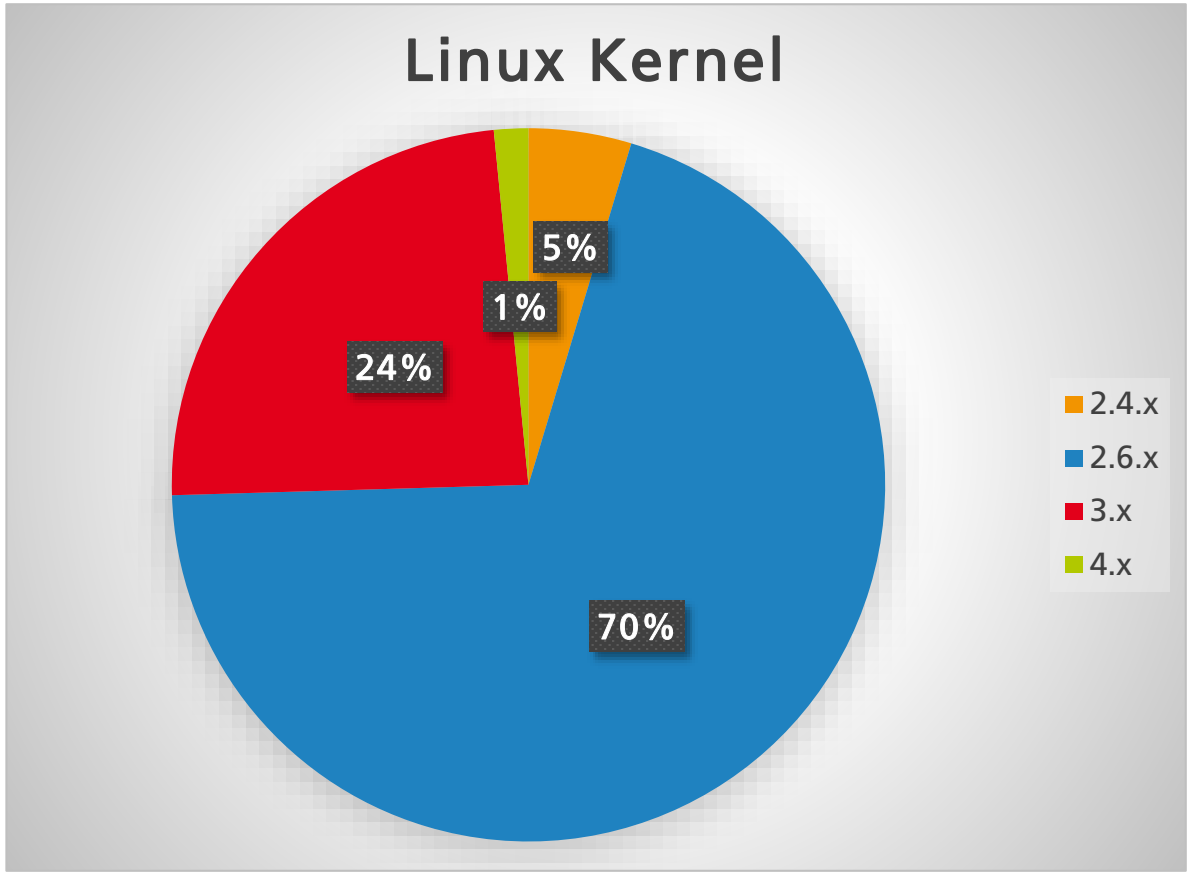


(Bild: YouTube / Armis)

Quelle: Heise Security

Fraunhofer FKIE

Wie sicher sind Geräte und Anlagen heute?



CVE-2017-1000251

published 2017-09-12

“The native Bluetooth stack in the Linux Kernel (BlueZ), starting at the Linux kernel version 2.6.32 and up to and including 4.13.1, are vulnerable to a stack overflow vulnerability in the processing of L2CAP configuration responses resulting in Remote code execution in kernel space.”

Wie gehen Hersteller mit Sicherheitslücken um?

- D-Link DWR-932B FW. 2.02 (eu)
  - Fernwartungszugang (SSH)
  - Hartcodiertes Passwort

```
#!/bin/sh
[…]
DAEMON=/usr/sbin/dropbear
NAME=dropbear
DESC="Dropbear SSH server"

DROPBEAR_PORT=22
DROPBEAR_EXTRA_ARGS=
```

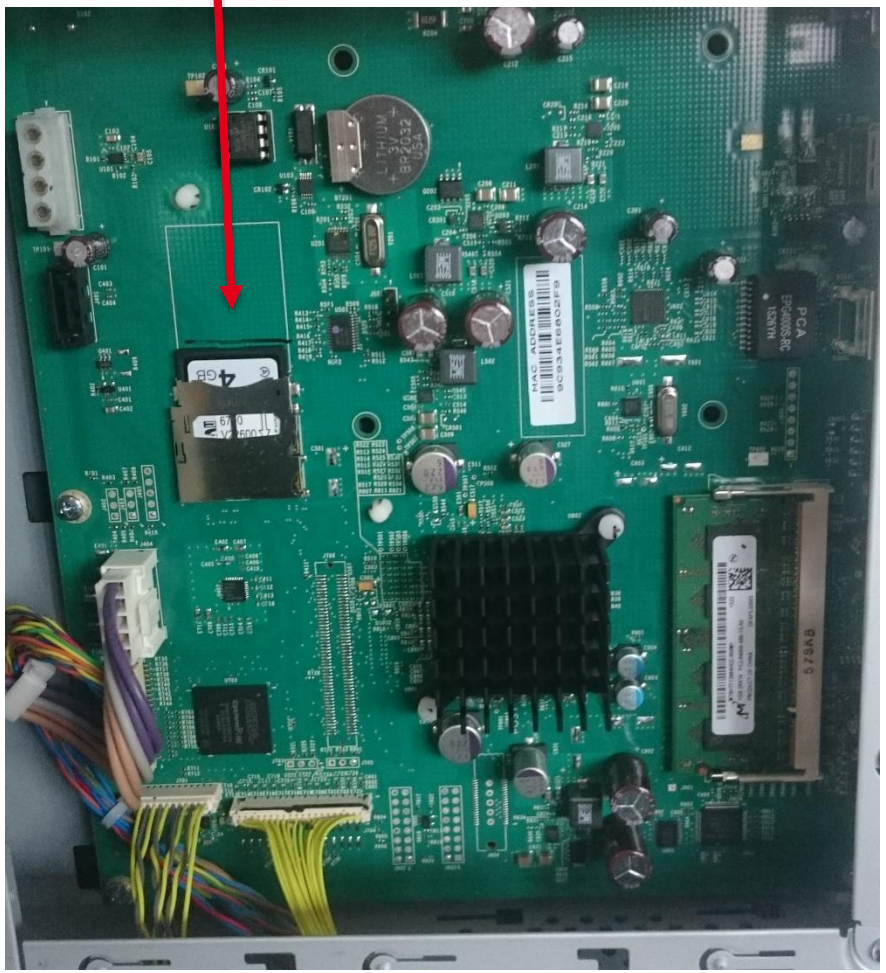
- D-Link DWR-932B FW. 2.03 (eu)
  - Wartungszugang geschlossen?

```
#!/bin/sh
[…]
DAEMON=/usr/sbin/dropbear
NAME=dropbear
DESC="Dropbear SSH server"

DROPBEAR_PORT=999999999
DROPBEAR_EXTRA_ARGS=
```

Auch Hardware ist Sicherheitsrelevant

Malware hier einfügen!



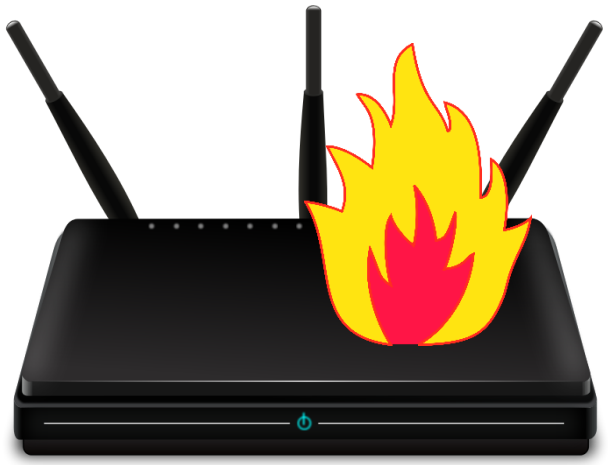
IT-Sicherheitsdreiklang

- Prävention
  - Erfolgreiche Angriffe verhindern / erschweren
  - Mögliche Folgen minimieren
- Detektion
  - Einbruchserkennung
    - Validitätsprüfung
    - Plausibilitätsprüfung / Anomalieerkennung
- Reaktion
  - Schaden eindämmen
  - Systeme bereinigen
  - Sicherheitskonzept überarbeiten

Prävention - Teaser: Aufspüren von Sicherheitslücken

Prävention - Aufspüren von Sicherheitslücken

- Live Demo



Praxistipps - Prävention

- Mitarbeiter schulen und sensibilisieren!
- Backups mit „AIR-GAP“
- „Standard“-Passwörter ändern
- Software / Firmware aktuell halten auch auf Geräten und Anlagen
- Netze konsequent trennen
- Fernwartungszugang nur über verschlüsselte Kanäle mit Authentifizierung
- „Notfallpläne“ erstellen
- …

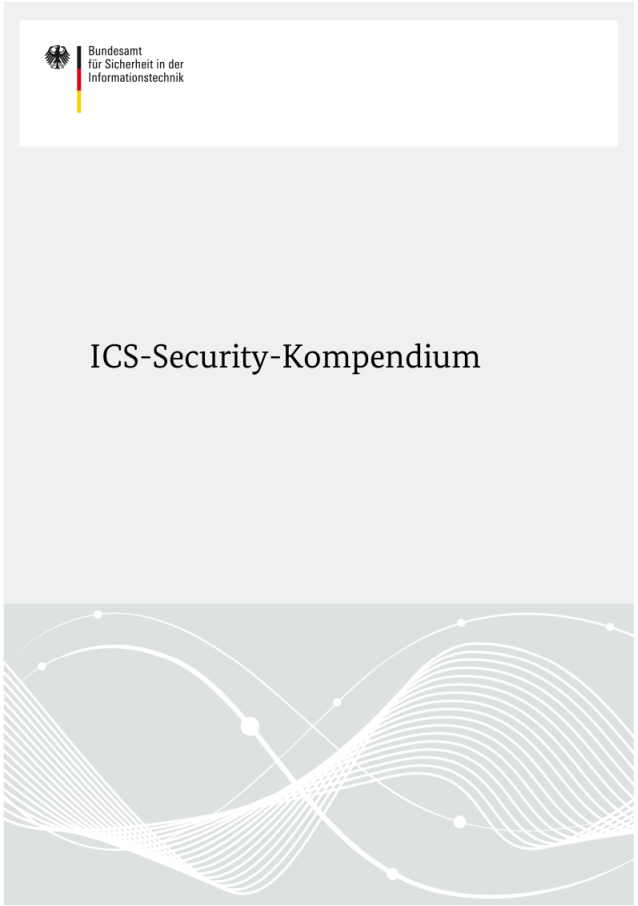
Praxistipps - Detektion

- Mitarbeiter schulen!
- „Secure Boot“ oder ähnliches wo möglich
- Malware Scanner
- Intrusion Detection Systeme
- Log-/Alert-Management
- …

Praxistipps - Reaktion

- Im Vorfeld den Ernstfall trainieren (Red-Team / Blue-Team)
- Notfallpläne umsetzen
- Vorfall untersuchen (lassen)
- Sicherheitskonzept überarbeiten
- …

Mehr Praxistipps



https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/ICS/Empfehlungen/ICS/empfehlungen_node.html

SCHUTZ KRITISCHER SYSTEME UND INFRASTRUKTUREN

Peter Weidenbach

peter.weidenbach@fkie.fraunhofer.de