Fujitsu CeBIT 2017

#CeBIT17

FUJITSU

shaping tomorrow with you

Human Centric Innovation

Driving Digital Transformation

Vernetzte Produktion im IoT-Zeitalter - durch Firewalls gut gesichert?

Irfan Ramma

IT Security Consultant

Enterprise & Cyber Security CE

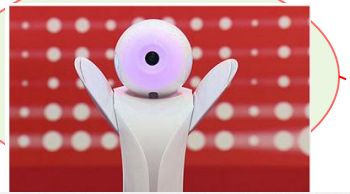
Agenda

- IoT Geräte
- Bestandteile von IoT Geräten (Zutaten)
- Angriffs Vektoren bei IoT
  - Warum ist Security bei IoT wichtig?
- Wie können moderne Firewalls helfen?
  - “Real-Time Security“ - Abschied vom Überlebens-Modus
  - IoT Absicherung mittels Sece Zone’s Model
- Womit beschäftigen sich Profi-Hacker beim Thema IoT?

IoT Geräte

- Smart: **Home**, **Farming, Manufacturing**
  - …Lampen
  - ...Kamera’s
  - …Digitale-Assistenten
  - …Toaster
  - …Staubsauger

IoT - Lösungen



Connecting People and ICT with "RoboPin"

Intelligent Care
IoT Solution UBIQUITOUSWARE

Driver Safety
IoT Solution UBIQUITOUSWARE

Eyewear towards low vision aid

Diversity commucation tool "LiveTalk"

AI driven IoT (e.g Zinrai)

Bestandteile von IoT Geräten (Zutaten)

FUJITSU

- OS, Applikation (+ Webservices)
- Datenbanken (+ Daten)
- Netzwerke (+ WiFi)
- Hardware (+ Sensoren)

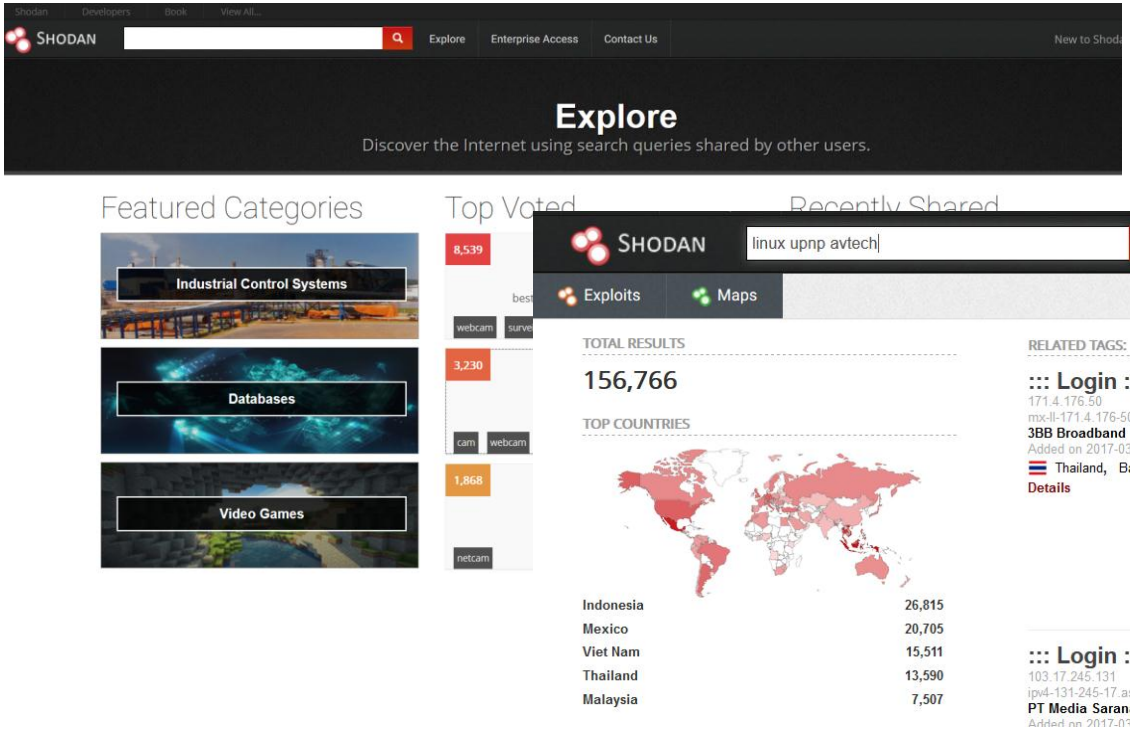
Angriffs Vektoren:
Warum ist IoT Security wichtig?

FUJITSU

- Die nächste Schwachstelle wird kommen.
  Die Frage ist: Wie gut können wir uns vorbereiten?

- Tendenz: Missbrauch von Ressourcen
  - Hosting für Tor Knoten?
  - Post-Exploitation – Ausnutzung von Platformen für Angriffe auf die lokale IT
  - Sind meine IoT Geräte im Bot-Net-Verbund (DDoS)?
    Wenn nicht, bin ich mir Sicher?

Beispiel Standard Passwörter



Angriff Vektoren auf IoT (OWASP Top 10)

FUJITSU

- 1 Insecure Web Interface
- 2 Insufficient Authentication/Authorization
- 3 Insecure Network Services
- 4 Lack of Transport Encryption/Integrity Verification
- 5 Privacy Concerns
- 6 Insecure Cloud Interface
- 7 Insecure Mobile Interface
- 8 Insufficient Security Configurability
- 9 Insecure Software/Firmware
- 10 Poor Physical Security

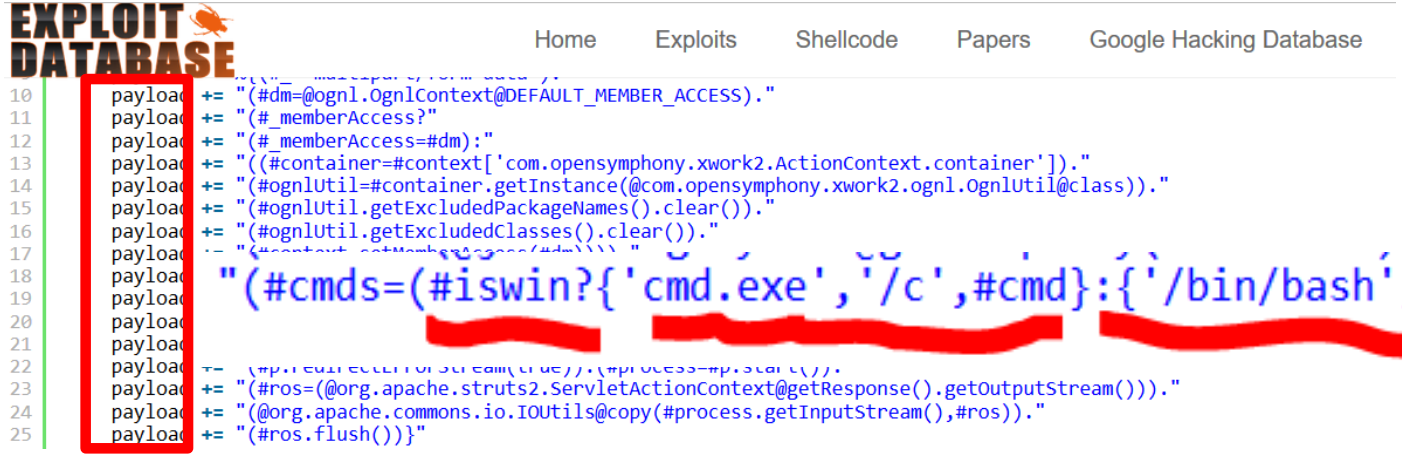
Insecure Web Interface , Insecure Networkservices

FUJITSU

- weak passwords , account lockout mechanism
- Code Injection : XSS, SQLi,CSRF vulnerabilities
- HTTPS to protect transmitted information
- change the default username and password
- Speicherfehler (Bufferoverflow)

Wie können moderne Firewalls helfen?

CVE: 2017-5638 - Apache Struts2 S2-045

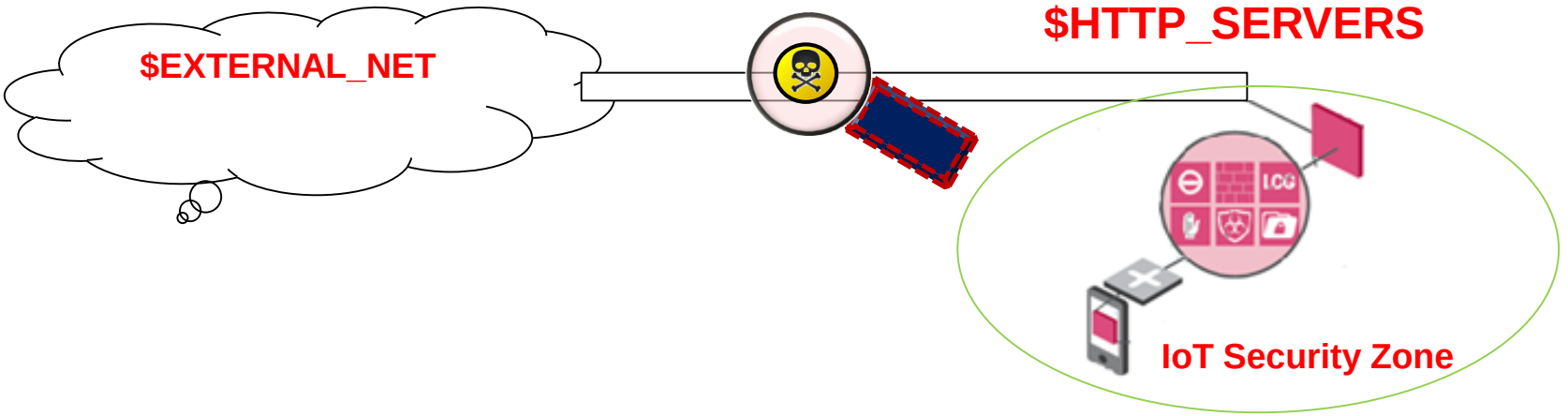



```
try
    headers = {'User-Agent': 'Mozilla/5.0', 'Content-Type': payload}
    request = urllib2.Request(url, headers=headers)
    page = urllib2.urlopen(request).read()
except httplib.IncompleteRead, e:
    page = e.partial
```

Security Baseline Zoning

FUJITSU

- alert http $EXTERNAL_NET any -> $HTTP_SERVERS any (msg:"ET WEB_SPECIFIC_APPS Possible Apache Struts OGNL Expression Injection (CVE-2017-5638) M2"; flow:to_server,established; content:"Content-Type|3a|"; http_header; nocase; content:"multipart/form-data"; http_header; content:"{"; http_header; nocase; content:"}"; http_header; pcre:"/^Content-Type\x3a(?=[^\r\n]*?multipart\/form-data)[^\r\n]*?\{[^\r\n]*?\}/Hmi"; classtype:web-application-attack; sid:2024044; rev:2;)



Suricata and Snort Signatures

EMERGING THREATS

Difference: 2024044 (vs. 1)

Revision 1 2017-03-13 - TWikiGuest

Line: 1 to 1

Added:

>

>

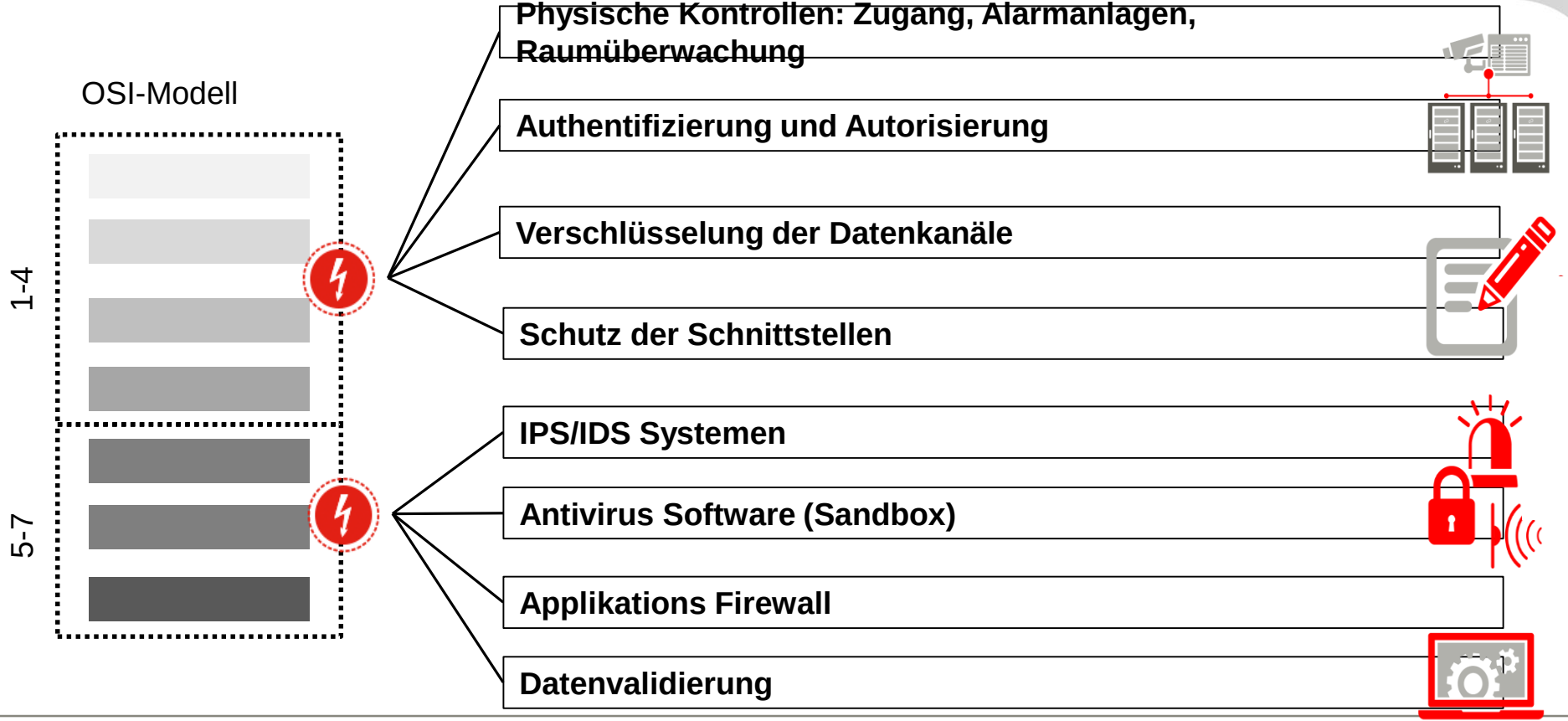
alert http $EXTERNAL_NET any -> $HTTP_SERVERS any (msg:"ET WEB_SPECIFIC_APPS Possible Apache Struts OGNL Expression Injection (CVE-2017-5638) M2"; flow:to_server,established; content:"Content-Type|3a|"; http_header; nocase; content:"multipart/form-data"; http_header; content:"{"; http_header; nocase; content:"}"; http_header; pcre:"/^Content-Type\x3a(?=[^\r\n]*?multipart\/form-data)[^\r\n]*?\{[^\r\n]{15,}\}/Hmi"; classtype:web-application-attack; sid:2024044; rev:3;)

Suricata and Snort Signatures – Mirai Botnet

FUJITSU

alert udp $HOME_NET any -> any 53 (msg:"ET TROJAN Mirai Botnet Domain Observed"; content:"|01 00 00 01 00 00 00 00 00 00|"; depth:10; offset:2; content:"|05|tr069|02|pw|00|"; nocase; distance:0; fast_pattern; reference:url,blog.opendns.com/2016/12/13/query-volumes-mirai-dgas/; classtype:trojan-activity; sid:2023637; rev:1;)

Wie können moderne Firewalls helfen?
Z.B. durch Multi Layer Schutz



Firewall Lösungsanbieter

Check Point®
SOFTWARE TECHNOLOGIES LTD.

SONICWALL™

FORTINET®

Restorepoint

SOPHOS

tufin

RSA®

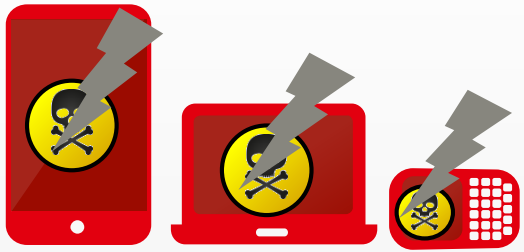
NSS LABS NGFW 2016

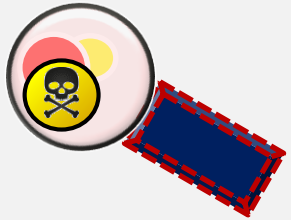
FUJITSU

Product	Security Effectiveness		Value in US$ (TCO per Protected Mbps)		Overall Rating
Barracuda Networks F600.E20	92.4%	Below Average	$14	Above Average	Neutral
Check Point 13800 NGFW Appliance	99.6%	Above Average	$25	Above Average	Recommended
Cisco ASA 5585-X SSP-60	96.5%	Above Average	$51	Below Average	Neutral
Cisco FirePOWER Appliance 8350	96.3%	Above Average	$23	Above Average	Recommended
Cyberoam CR2500iNG-XP	58.1%	Below Average	$22	Above Average	Neutral
Dell SonicWALL SuperMassive E10800	98.1%	Above Average	$24	Above Average	Recommended
Forcepoint Stonesoft NGFW 1402	97.6%	Above Average	$26	Above Average	Recommended
Fortinet FortiGate 3200D	99.6%	Above Average	$9	Above Average	Recommended
Hillstone Networks SG-6000-E5960	99.0%	Above Average	$6	Above Average	Recommended
Huawei Technologies USG6650	98.1%	Above Average	$7	Above Average	Recommended
Juniper Networks SRX5400E	98.0%	Above Average	$97	Below Average	Neutral
Palo Alto Networks PA-7050	95.9%	Above Average	$31	Below Average	Neutral
WatchGuard Technologies XTM 1525	87.7%	Below Average	$18	Above Average	Neutral

“Real-Time Security“ - Abschied vom Überlebens-Modus

FUJITSU





Protect

- Defense in Depth
- ISMS
- …

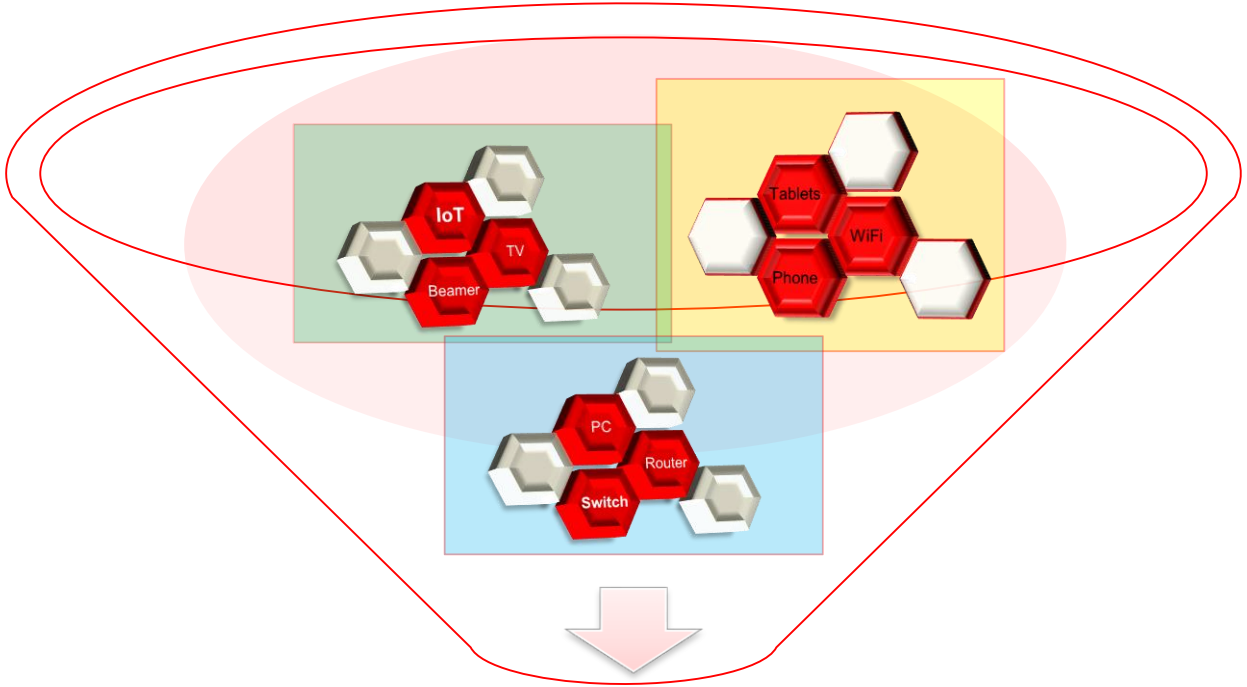
Monitor

- Sichtbarkeit
- Security Performance
- …

SoC

- Reaktive Aufklärung
- Analytics
- Threat Hunting
- …

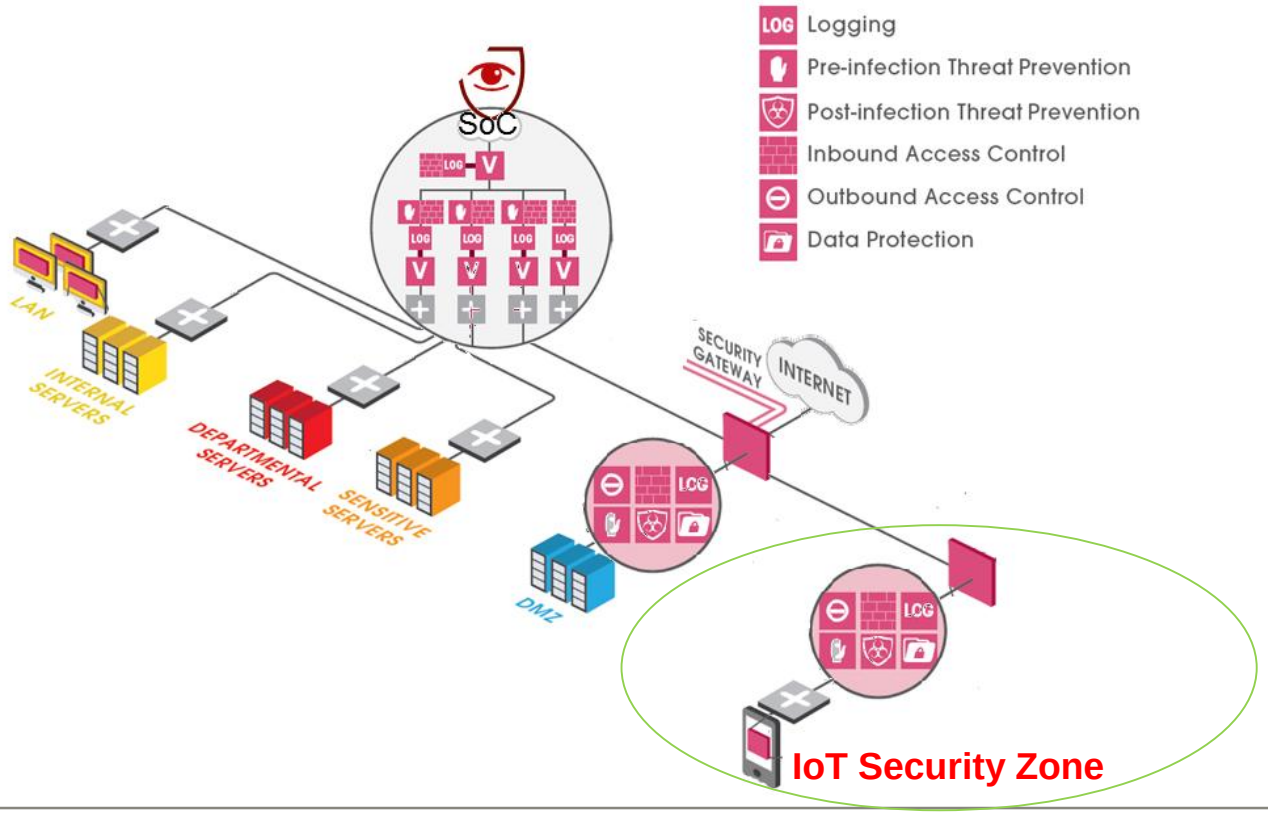
IoT Absicherung mittels Secure Zone's Model



Die W- Fragen?

IoT Absicherung mittels Secure Zone's Model

Gruppieren & Mikro – Segmentierung (beispiel. Checkpoint)



IoT Absicherung mittels Secure Zone's Model

FUJITSU

- Schadcode Filter für netzwerkbasierte Angriffe (IPS Regel)
- WAF Schutz gegen gängige Webangriffe
  - Injection Schutz, Autolearning, Virtual Patching
- Micro - Segmentierung von IoT Geräten in Sicherheits Zonen
  - Benötigt das IoT Gerät Internet-Access? (ggf. Allow many / Deny all)
- Application Layer Gateways
  - Content Switching auf Protokoll ebene.
  - SSl Inspection
- Regelmäßige Schwachstellen Analyse
  - Vulnerability Scans, Penetration Test & bei Bedarf Incident Response

Womit beschäftigen sich Profi-Hacker?

FUJITSU

Potential Mission Areas for EDB

Firmware Targets

Internet of Things (e.g. Weeping Angel (Extending) Engineering Notes)

Vehicle Systems (e.g. VSEP)

ICS/SCADA

Network Devices (including but not limited to SOHO routers)

EFI

Software Targets

Linux/Unix

BSD

Owner: User #524297

Firmware Reverse Engineering

('toc' missing)

Firmware Images

We modified flashrom v0.9.7 (http://www.flashrom.org/Flashrom) to make it work with our 32MB flash from Macronix (MX25L25635FZ2I-10G). Eventually, we will attach the modified flashrom source code to this page when the source code is more stable.

S

Ex

Acc

Samsung F8000 Smart TV networking

(Weeping Ange

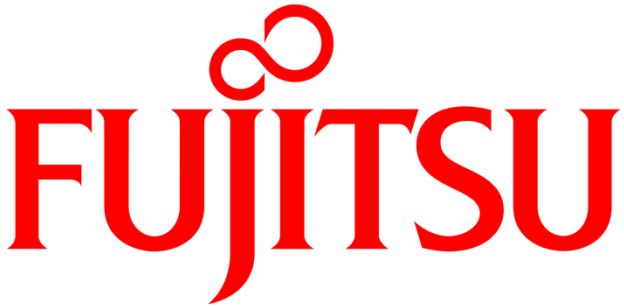
Embedded Devices Order Status
Devices Ordered

Device Name/Model	Sterility Code	Quanti
Raspberry Pi	2	8
Cotton Candy	2	5
[illegible]magic MK802 II New Generation Mini4 Android 4.0 PC	2	2
[illegible]magic MK802 IV Dual Core Android8 4.1 Jelly Bean Mini PC	2	2
Gumstix Card	1	
Zoom Torpedo Developm[illegible] Kit [illegible]M3730-30-256512R	2	5
Torpedo AM3703	2	8
FaceDancer (assembled)	2	10
Face Dancer (unassembled)	2	5
BeagleBoneBlack	0	10

Fragen?

FUJITSU

Vielen Dank für Ihre Aufmerksamkeit



shaping tomorrow with you