Universität Rostock

Traditio et Innovatio

Zusammenwachsen von Gebäudeautomation und Computernetzwerken - Eine erste Sicherheitsanalyse

Thomas Mundt und Peter Wickboldt
Universität Rostock

Ausnahmsweise, weil es von Bedeutung ist - wir sind sonst nicht so eitel:

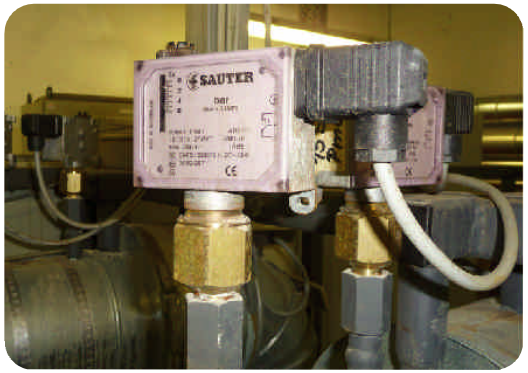
- Peter Wickboldt ist Referatsleiter „Betriebstechnik und Logistik“ im Dezernat „Technik, Bau, Liegenschaften“ der Verwaltung der Universität Rostock.

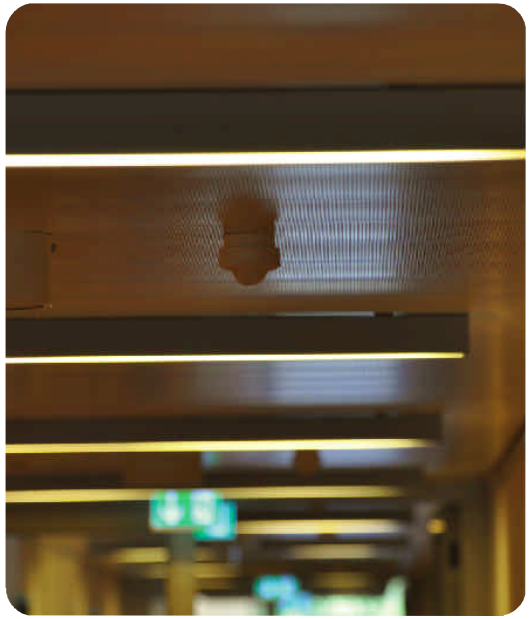
- Thomas Mundt ist wissenschaftlicher Mitarbeiter in der Arbeitsgruppe „Informations- und Kommunikationsdienste“ des Instituts für Informatik der Universität Rostock.

Moderne Gebäude - Hohe Automatisierungsdichte


Zugang
nur für
Mitarbeiter


Achtung reduzierter
Sauerstoffgehalt !
Eingeschränkter Zutritt


SAUTER



Die Universität Rostock

Studierende	13.890
Professuren	292
Mitarbeiter	1.452
Anzahl der Gebäude	160
Hauptnutzfläche	136.000m²




Ein erstes Testobjekt

- Übergabe des Konrad-Zuse-Hauses an die Universität Rostock 2012
- Nutzer sind IT-Dienste (Rechenzentrum) der Universität Rostock und Institut für Informatik
- KNX – Bussystem für Beleuchtungssteuerung und Klimatisierung
  - T. M. (der Forscher): da kann ich doch mal „reinhören“
  - P. W. (der „Verwalter“): auf frischer Tat ertappt - Gewährleistungsansprüche weg?

Zusammenarbeit Wissenschaft / Verwaltung

- Nutzer zeigt die Probleme offener Protokollstrukturen an
- Verwaltung reagiert erst ablehnend, dann „einsichtig“
- Problem verstanden – Notwendigkeit der Zusammenarbeit erkannt (Akzeptanz der Kompetenz)

Methodik

- Angelehnt an BSI Standard 100-2 und 3 für Computernetzwerke.
- Erfassen der Netzwerk-Struktur - Netzplanerhebung.
- Erfassung der Anwendungen.
- Erhebung der angeschlossenen Geräte.
- Organisatorische Aspekte. Wer hat Zugang? Wie werden Zugänge verteilt und weitergegeben? Werden Zugriffe protokolliert?

Bundesamt für Sicherheit in der Informationstechnik

BSI-Standard 100-2
IT-Grundschutz-Vorgehensweise

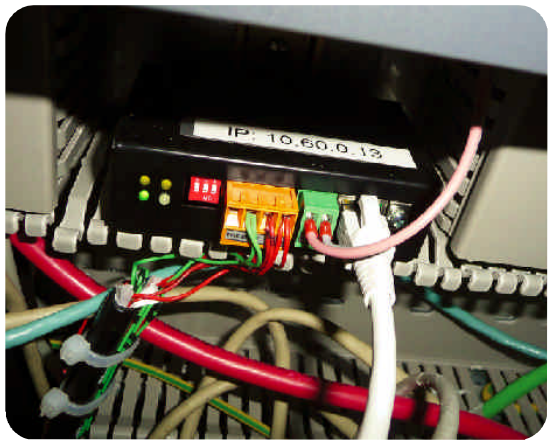
Methodik

- Schutzbedarf-Feststellung.
  - Mögliche Angriffe.
  - Mögliche Schäden.
  - Bestimmung des Aufwands für einen Angriff und damit eine Abschätzung der möglichen Eintrittswahrscheinlichkeit.
- Bestimmung des Risikos.

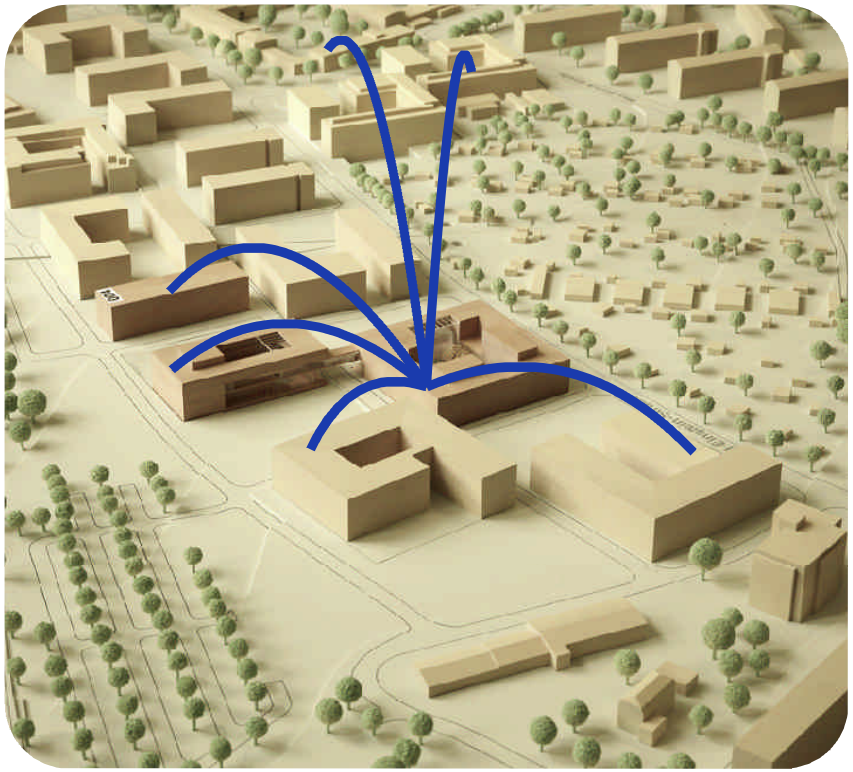
Methodik

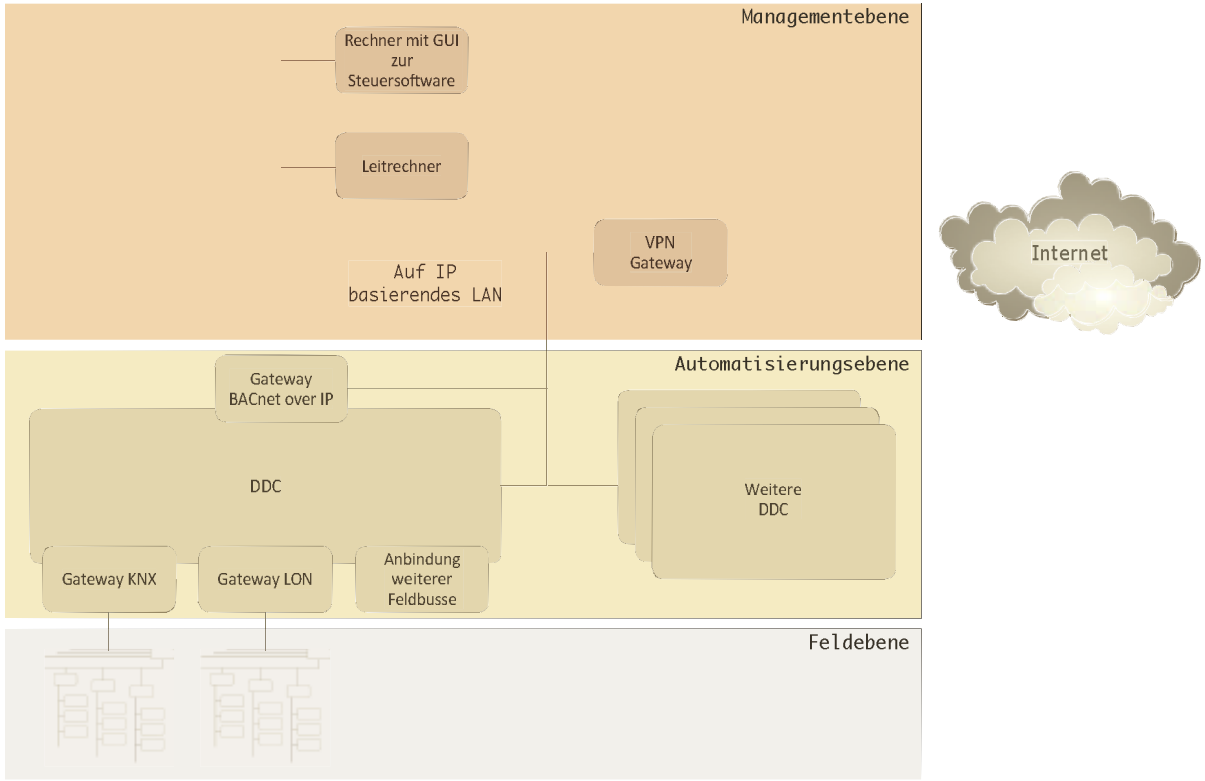
- Weitere Aspekte:
  - Sicherheit der verwendeten Protokolle.
  - Innerer Aufbau und Grundkonfiguration der Geräte.
  - Wie sieht die Dokumentation aus? Ist Dokumentation vorhanden? Wurde Konfiguration / Sourcecode mit „eingekauft“?

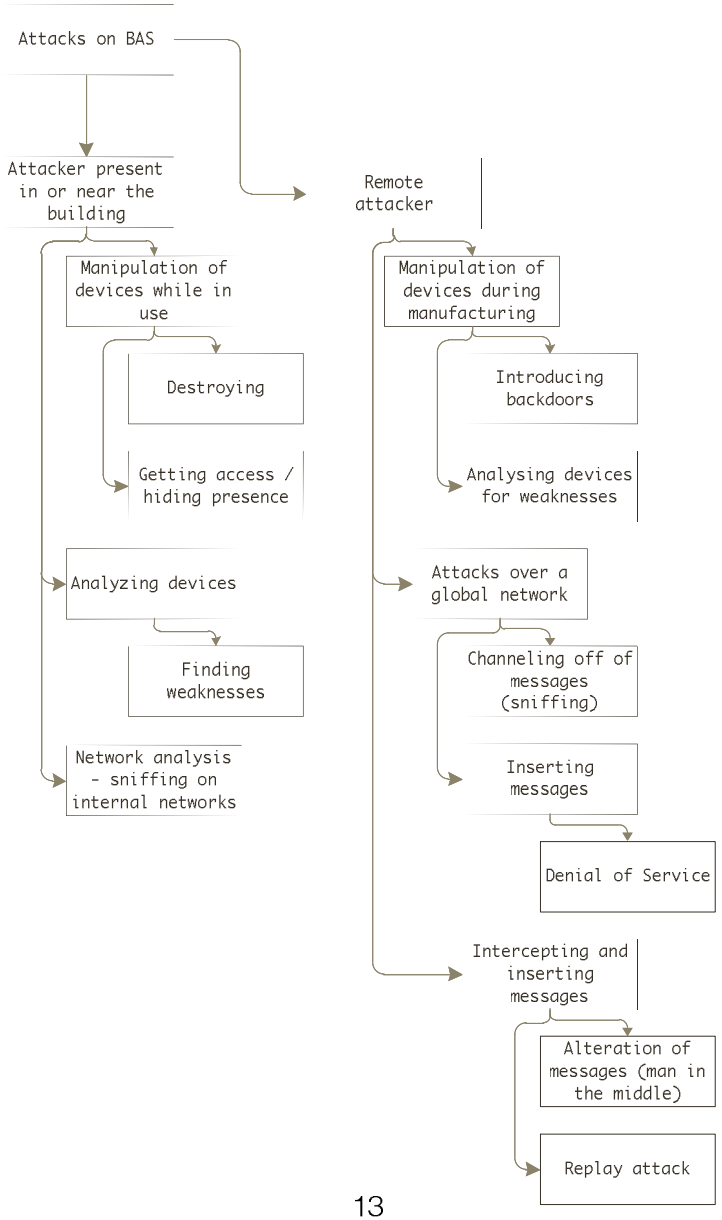
Viele Netzübergänge und Adapter



Allgemeine Netzstruktur






Attacks on BAS
Attacker present in or near the building
Manipulation of devices while in use
Destroying
Getting access / hiding presence
Analyzing devices
Finding weaknesses
Network analysis - sniffing on internal networks
Remote attacker
Manipulation of devices during manufacturing
Introducing backdoors
Analysing devices for weaknesses
Attacks over a global network
Channeling off of messages (sniffing)
Inserting messages
Denial of Service
Intercepting and inserting messages
Alteration of messages (man in the middle)
Replay attack

Auswahl denkbarer Angriffe und Schäden

- **Mechanische Überlastung** von z.B. Jalousie-Motoren oder Stellmotoren von Lüftungen durch wiederholtes, pausenloses Öffnen und Schließen.
- **Elektrische Überlastung** von z.B. Transformatoren durch gleichzeitiges Ein- oder Ausschalten von Verbrauchern mit induktiver Last.
- Vorzeitige **Alterung von Bauteilen**, z.B. Leuchtstoffröhren durch wiederholtes Zünden.
- **Manipulation von Schranken** oder automatischen **Türen**, so dass z.B. Autos beschädigt werden.
- **Türen** werden dauerhaft **verschlossen**. Mitarbeiter können sich nicht frei im Gebäude bewegen.

Auswahl denkbarer Angriffe und Schäden

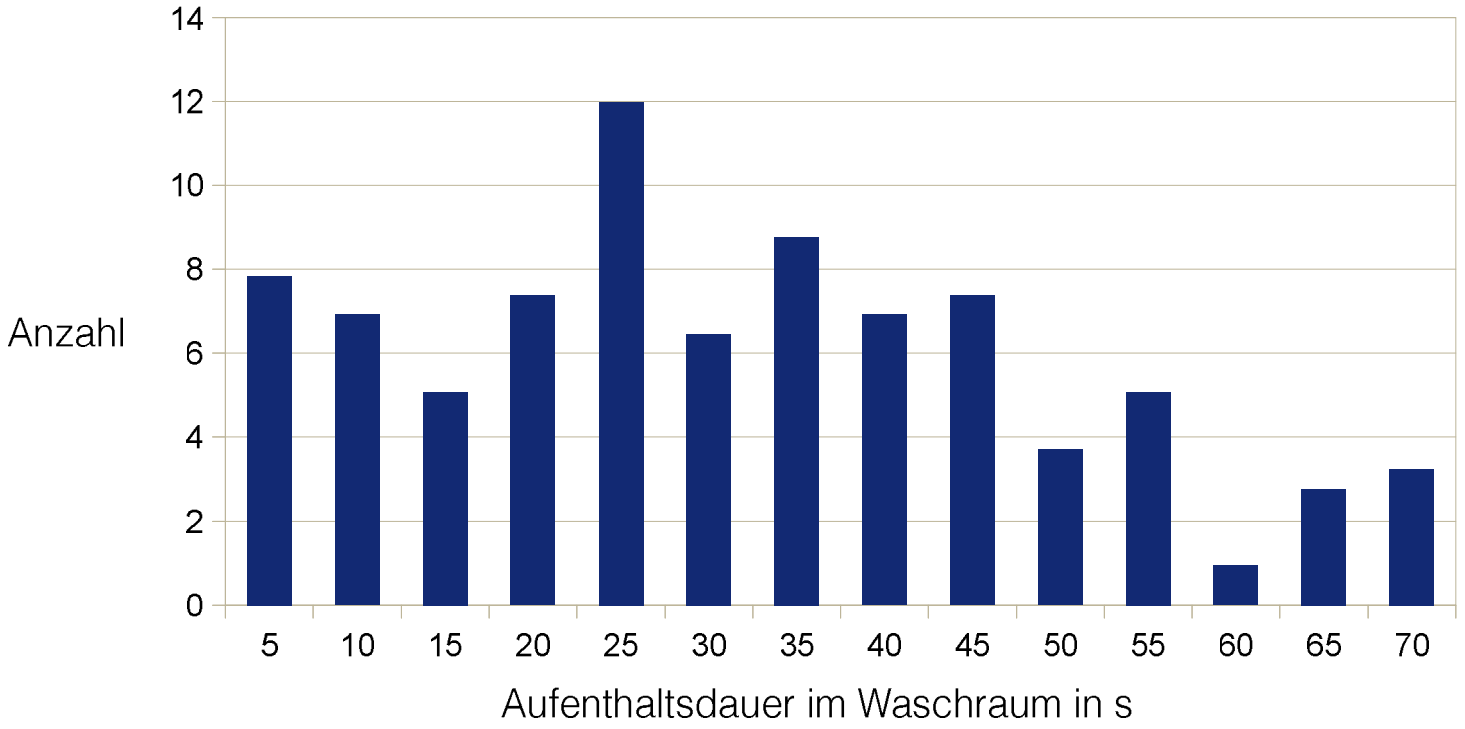
- Die **Klimatisierung** wird mit zu hoher oder zu niedriger Temperatur betrieben. Das wirkt sich auf Mitarbeiter aus, kann aber auch Auswirkungen auf installierte Technik haben. Insbesondere zu kühlenden Computertechnik reagiert sensibel auf deutlich **zu hohe Temperaturen**.

- Die **Beleuchtung** wird dauerhaft abgeschaltet oder zum Blinken gebracht. Geräte gehen kaputt oder werden unnötig verschlissen. Mitarbeiter werden am Arbeiten gehindert. Ein **Reputationsschaden** kann auch auftreten, wenn mittels der Beleuchtungssteuerung **von außen sichtbare Nachrichten** auf der Fassade angezeigt werden.

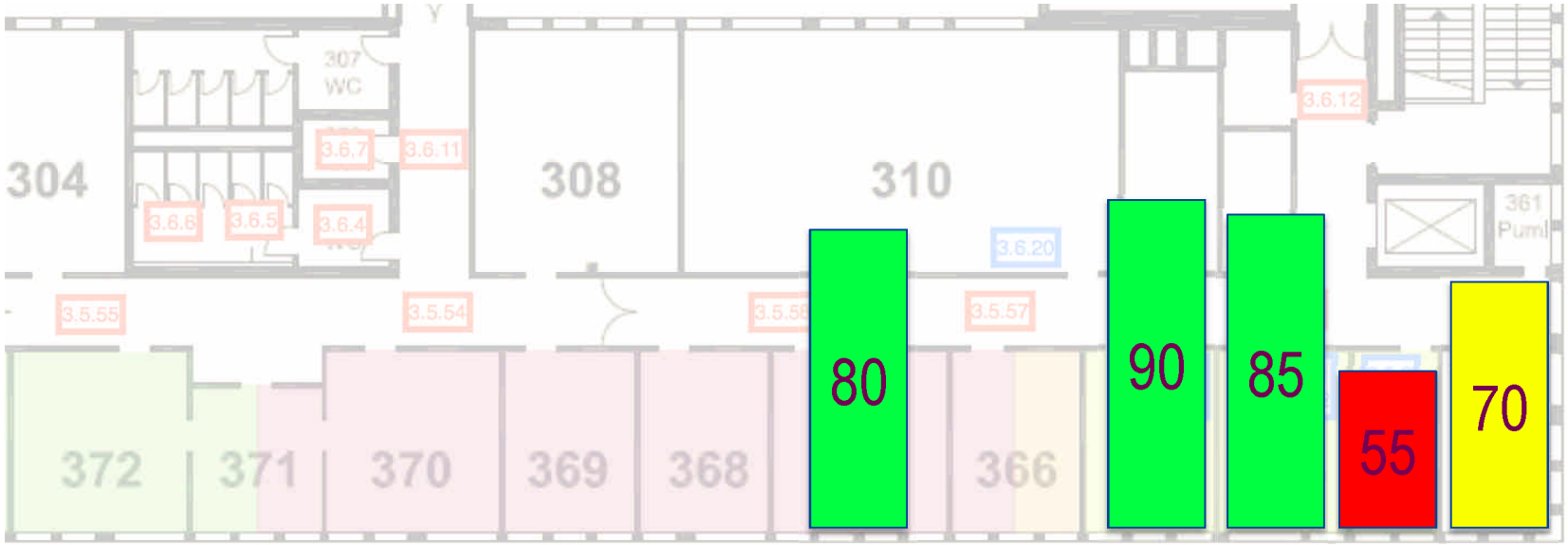
- Die Belüftung wird so gesteuert, dass ein **Unterdruck** im Raum das **Öffnen einer Tür verhindert** oder die Tür selbständig öffnet.

- In sensiblen Bereichen (z.B. solche mit chemischen oder biologischen Apparaturen) kann eine Änderung der Belüftung / Ablüftung zur **Freisetzung gefährlicher Substanzen** führen.

Auswahl denkbarer Angriffe und Schäden

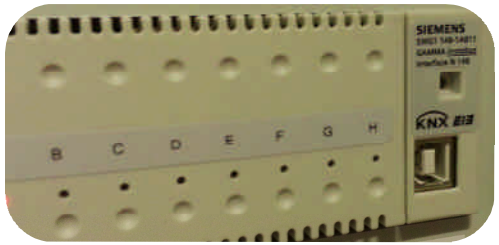


Auswahl denkbarer Angriffe und Schäden



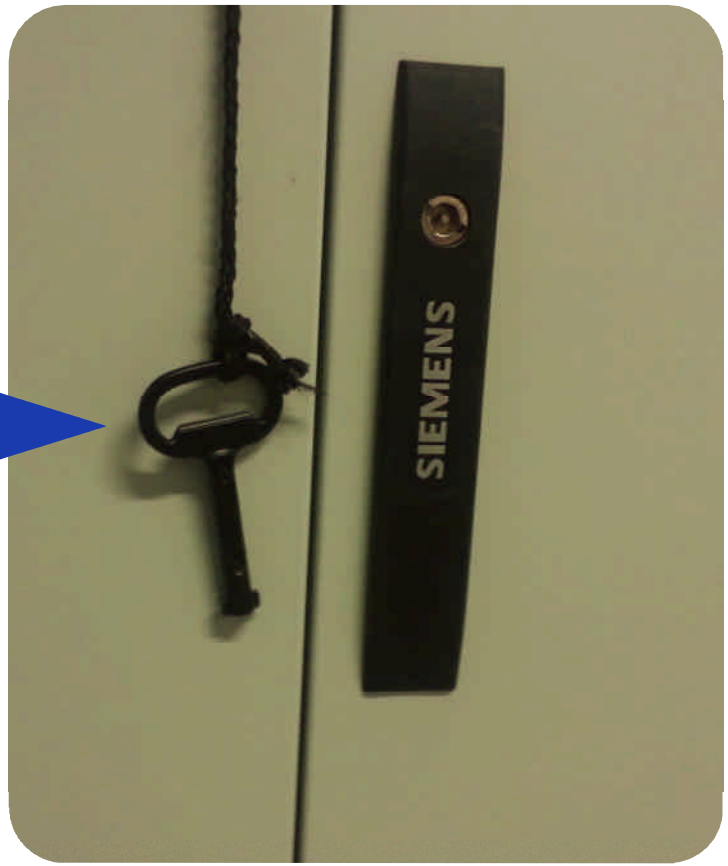
Welcome to hacker's paradise

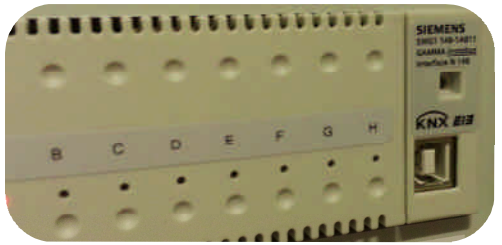
- Grundlegender physischer Zugangsschutz wird vernachlässigt.
- Zugang zum GA-Netzwerk über vorhandene oder mitgebrachte Interfaces.



Welcome to hacker's paradise

- Grundlegender physischer Zugangsschutz wird vernachlässigt.
- Zugang zum GA-Netzwerk über vorhandene oder mitgebrachte Interfaces.





Welcome to hacker's paradise

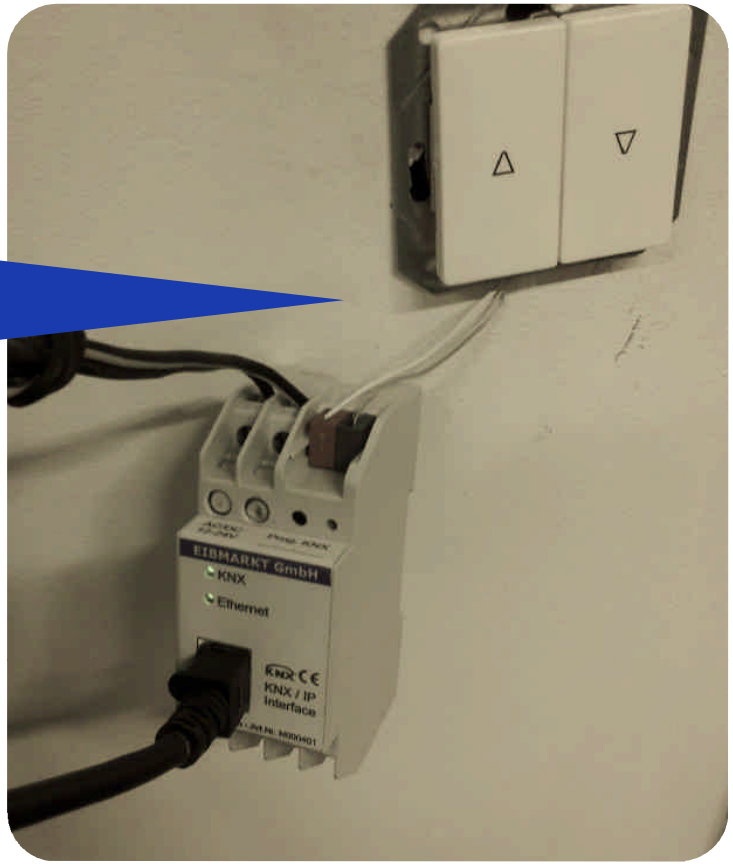
- Grundlegender physischer Zugangsschutz wird vernachlässigt.
- Zugang zum GA-Netzwerk über vorhandene oder mitgebrachte Interfaces.

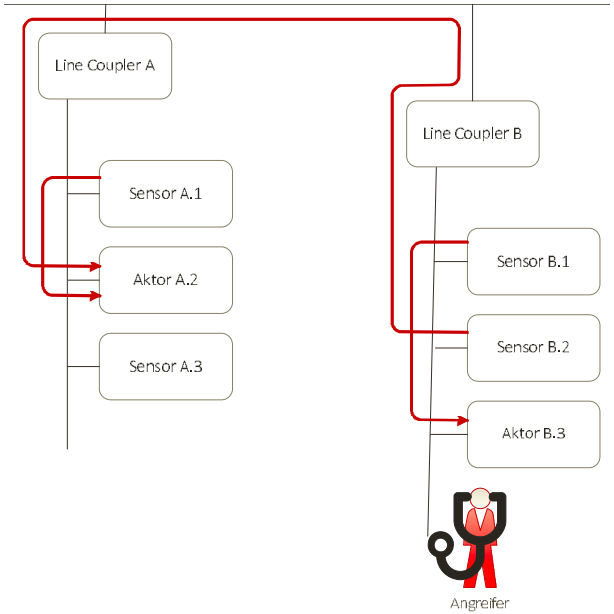
Welcome to hacker's paradise

- Grundlegender physischer Zugangsschutz wird vernachlässigt.
- Zugang zum GA-Netzwerk über vorhandene oder mitgebrachte Interfaces.

Welcome to hacker's paradise

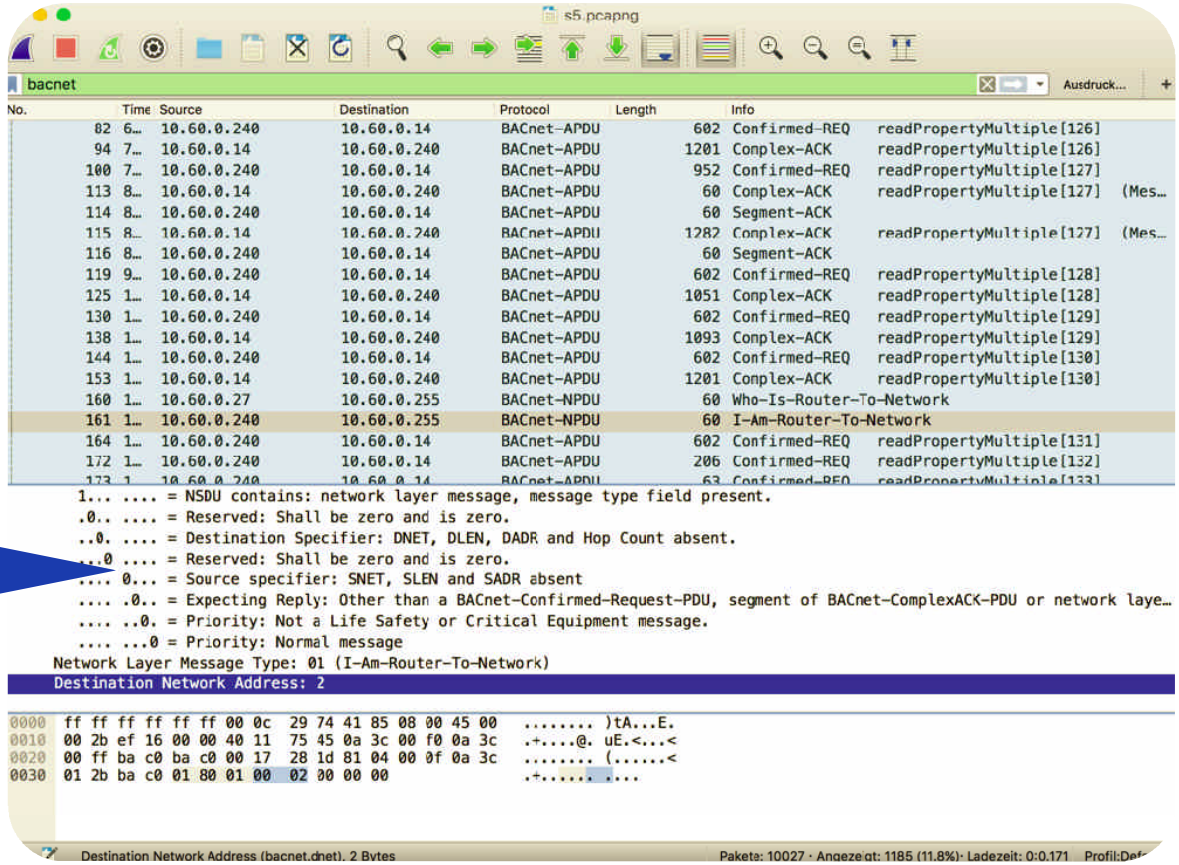
- Nachrichten nahezu überall unverschlüsselt und ohne Authentisierung.
- Zugriff auf Medien zumindest in der Feldebene beliebig möglich, auch versteckt.





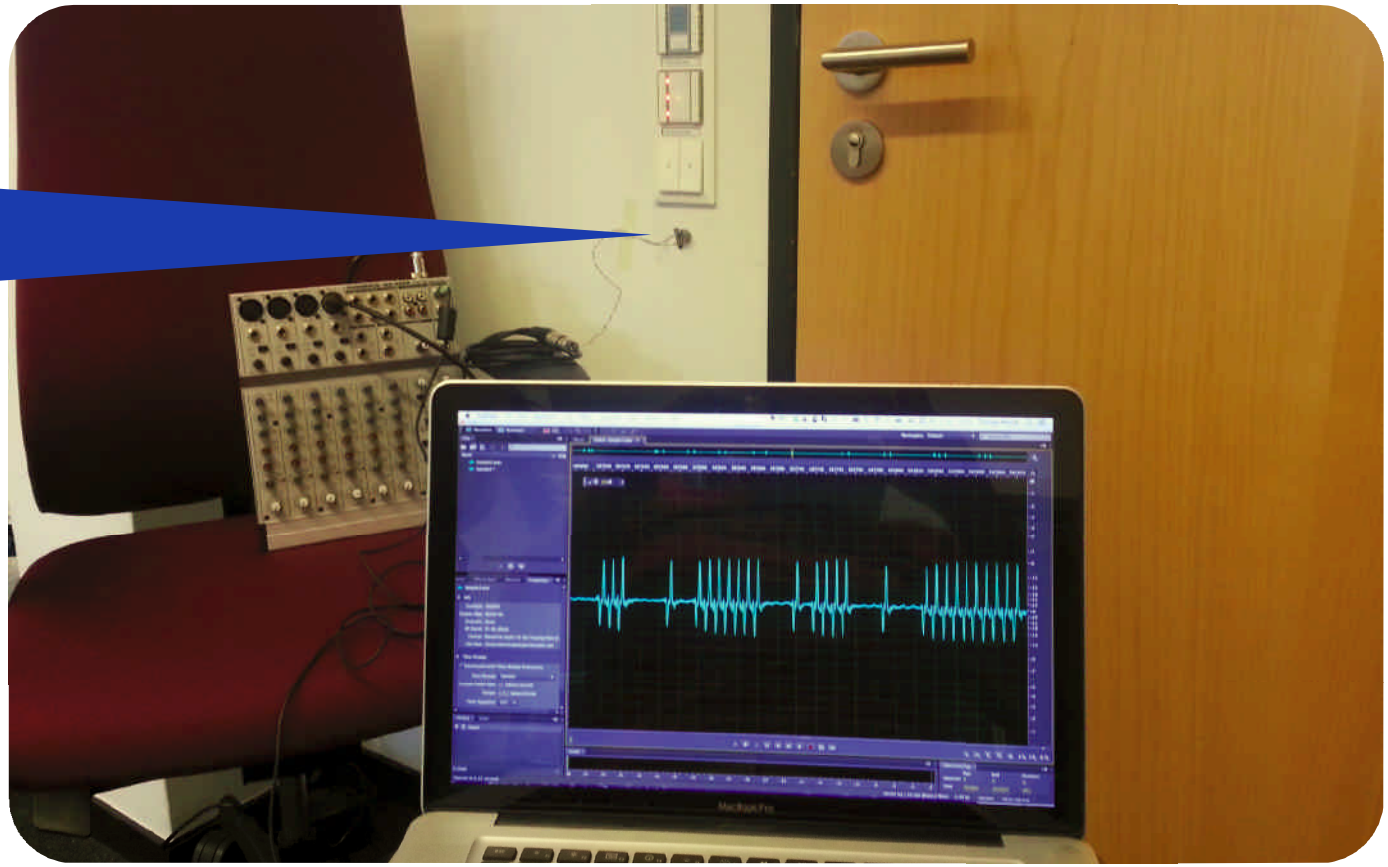
Welcome to hacker's paradise

- Nachrichten nahezu überall unverschlüsselt und ohne Authentisierung.
- Viele Broadcasts.



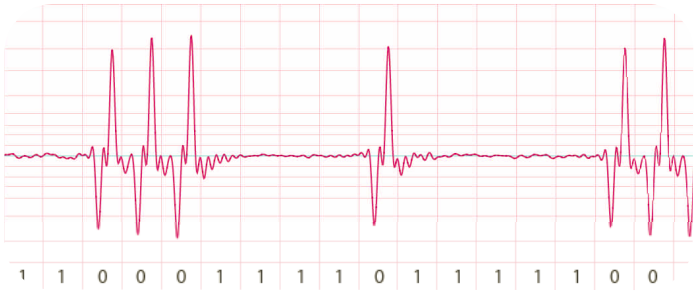
Welcome to hacker's paradise

- Selbst echter physischer Zugang ist entbehrlich.



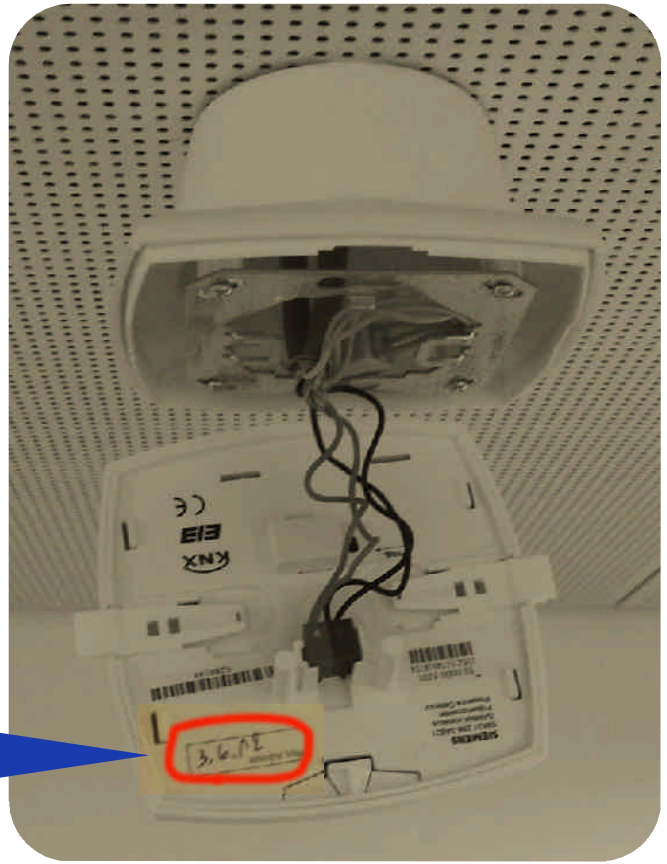
Welcome to hacker's paradise

- Selbst echter physischer Zugang ist entbehrlich.



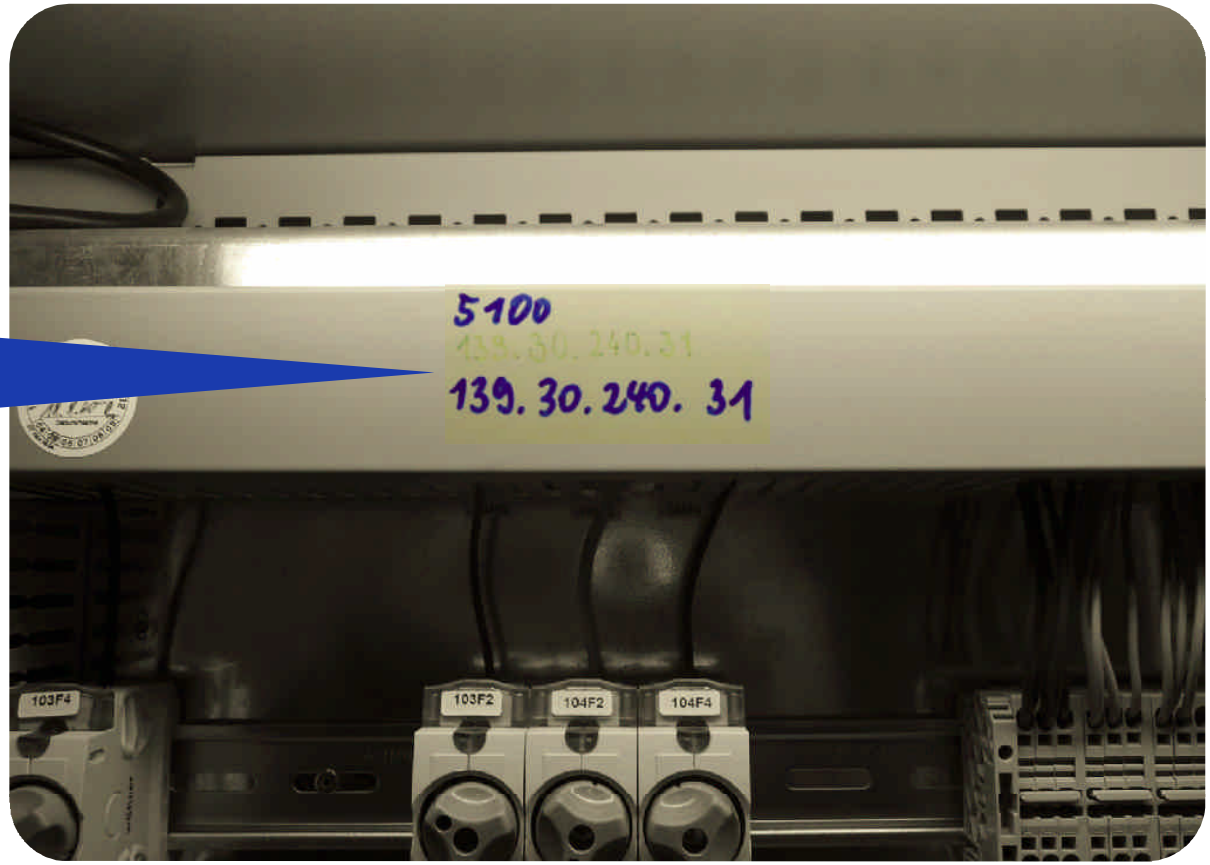
Welcome to hacker's paradise

- Informationen zur Konfiguration sind nahezu beliebig einfach zu beschaffen.



Welcome to hacker's paradise

- Informationen zur Konfiguration sind nahezu beliebig einfach zu beschaffen.

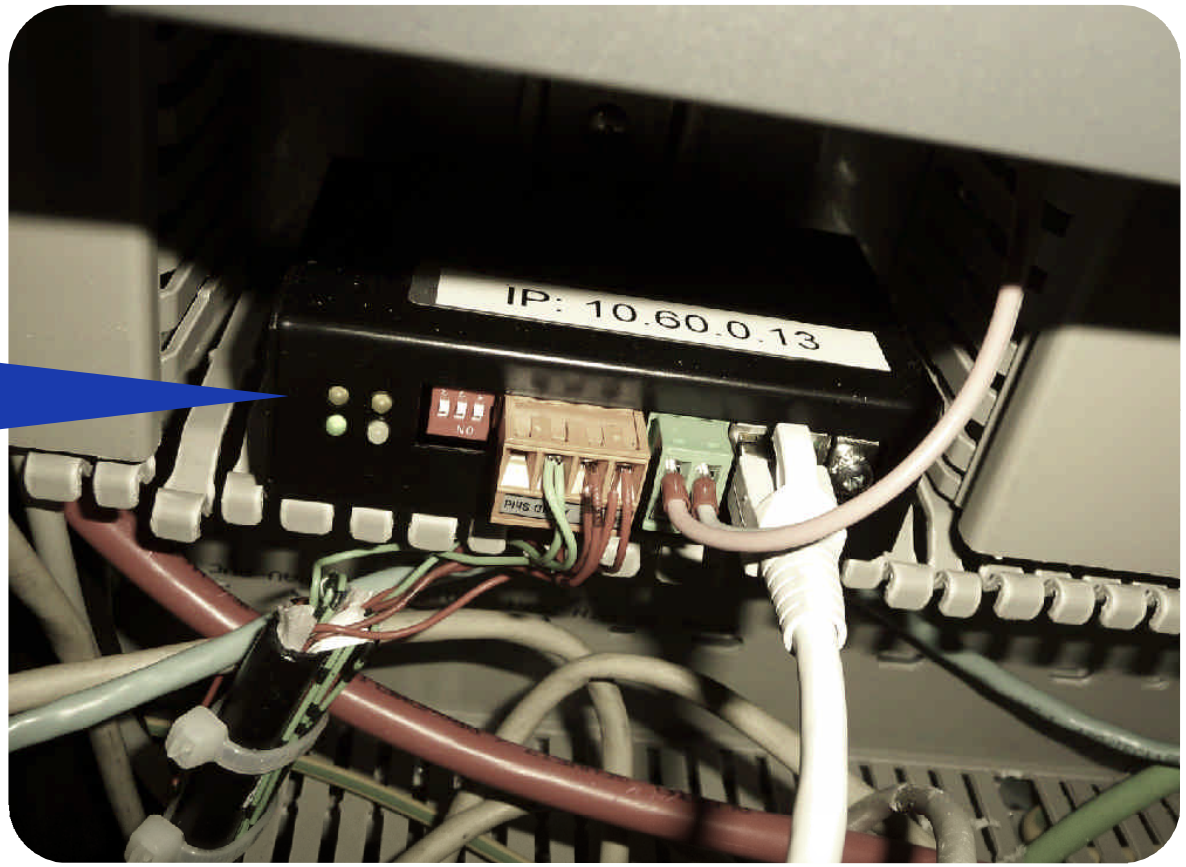


Welcome to hacker's paradise

- Einfach zu überwindende Gateways zwischen den verschiedenen Netzebenen.

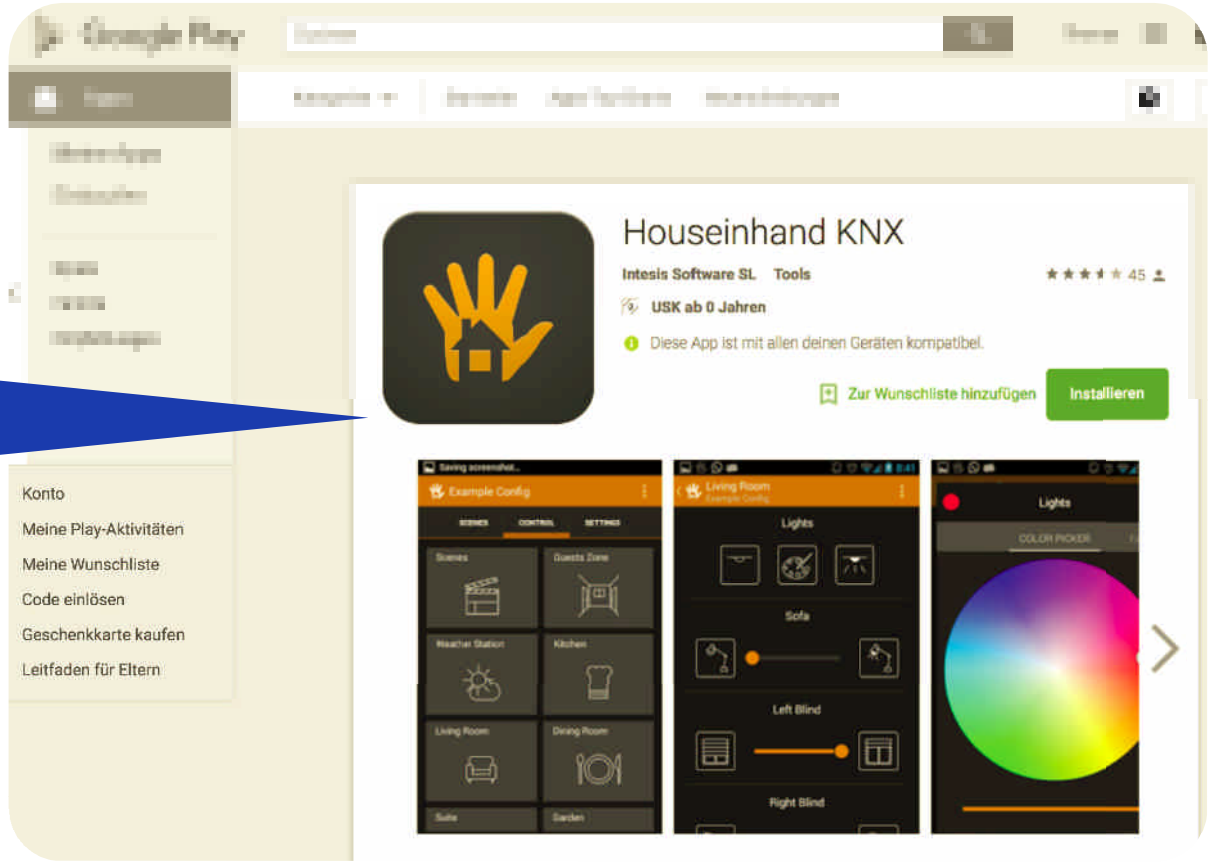
Welcome to hacker's paradise

- Einfach zu überwindende Gateways zwischen den verschiedenen Netzebenen.



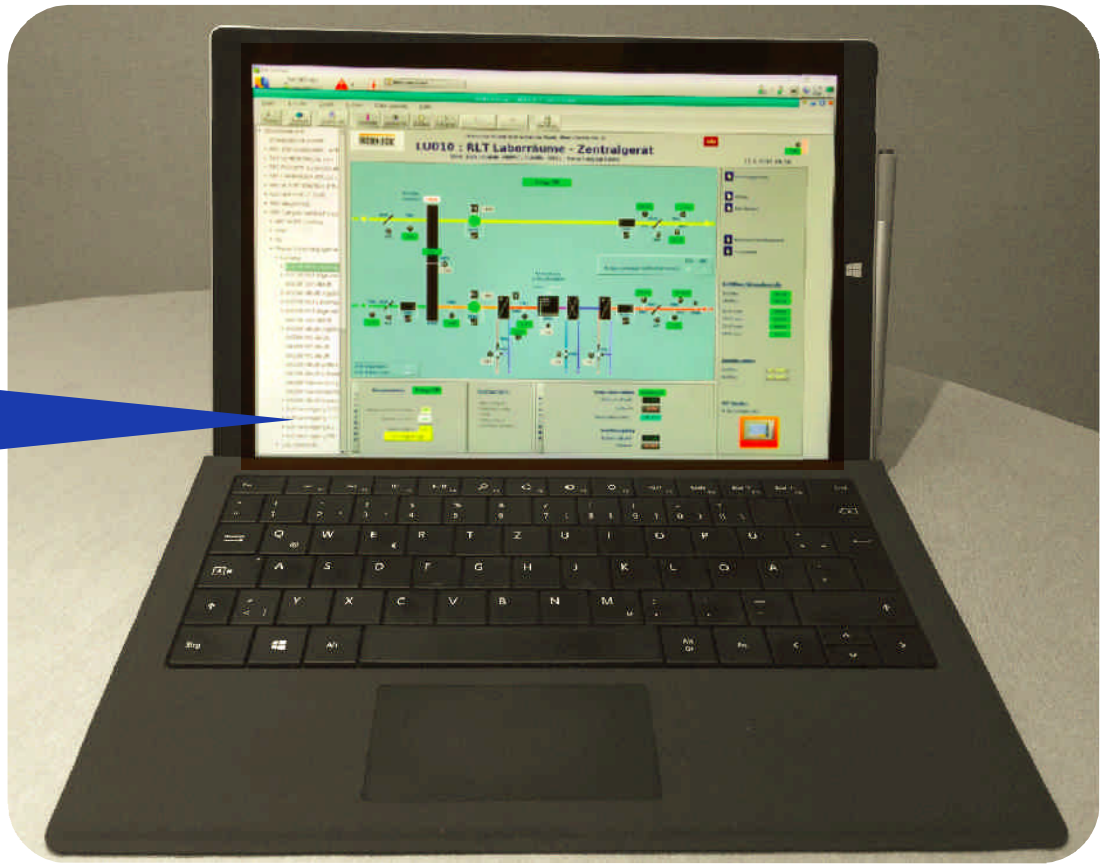
Welcome to hacker's paradise

- Fertige Software und Libraries sind breit verfügbar.



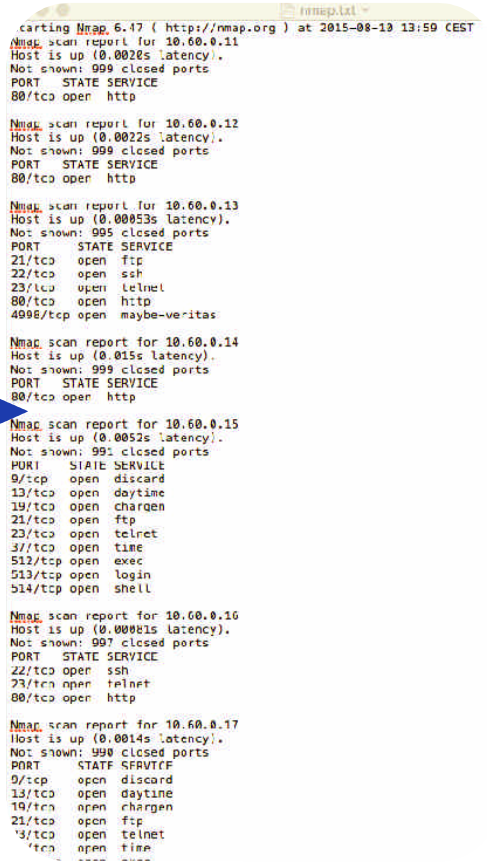
Welcome to hacker's paradise

- Nicht weiter eingeschränkter Remotezugriff über VPN für viele Zulieferer.



Welcome to hacker's paradise

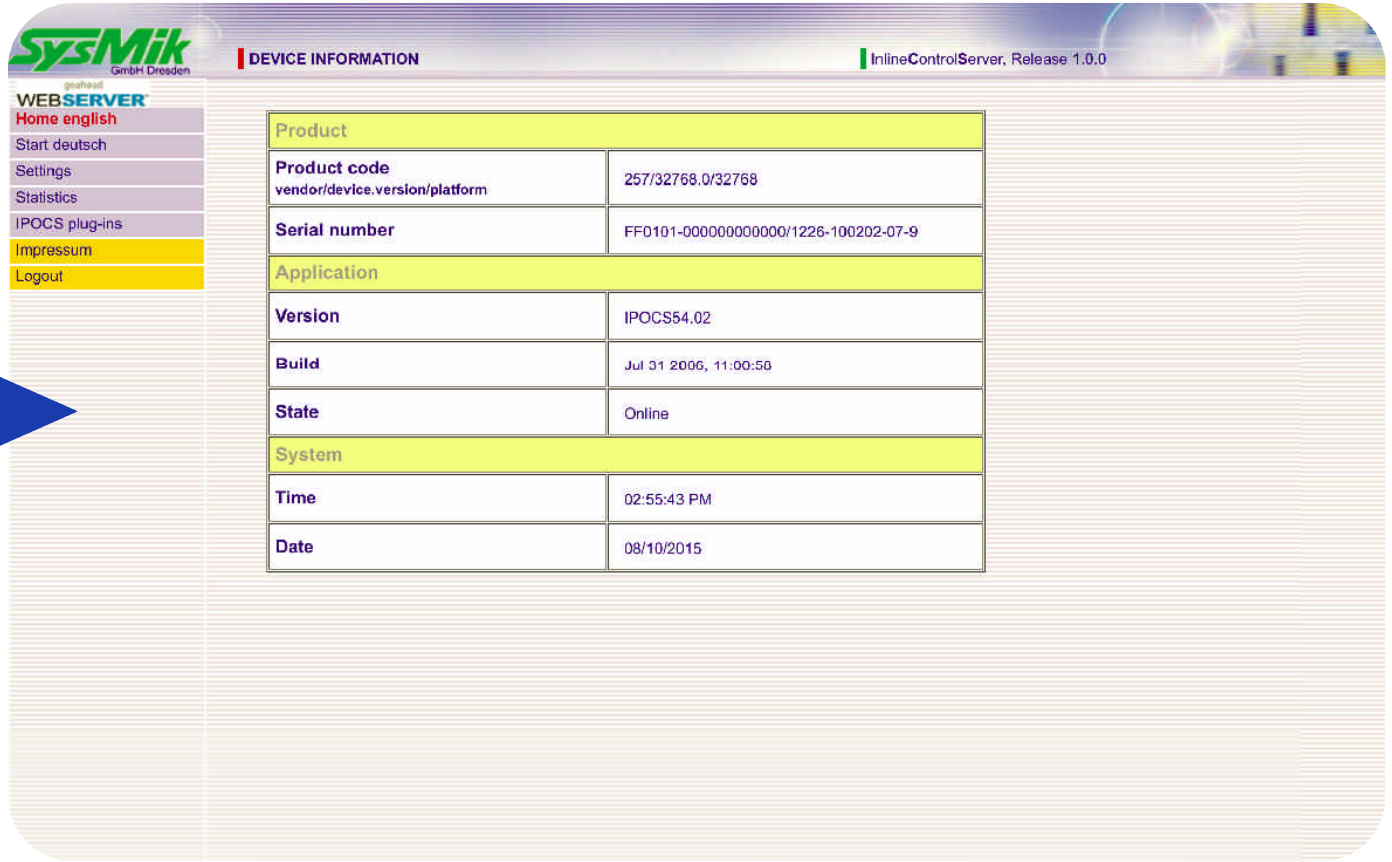
- Offene Zugänge zu Bedienoberflächen.



```
arting Nmap 6.47 ( http://nmap.org ) at 2015-08-13 13:59 CEST
Nmap scan report for 10.60.0.11
Host is up (0.0028s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 10.60.0.12
Host is up (0.0022s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 10.60.0.13
Host is up (0.00053s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
80/tcp   open  http
4998/tcp open  maybe-veritas

Nmap scan report for 10.60.0.14
Host is up (0.015s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 10.60.0.15
Host is up (0.0052s latency).
Not shown: 991 closed ports
PORT    STATE SERVICE
9/tcp   open  discard
13/tcp  open  daytime
19/tcp  open  chargen
21/tcp  open  ftp
23/tcp  open  telnet
37/tcp  open  time
512/tcp open  exec
513/tcp open  login
514/tcp open  shell

Nmap scan report for 10.60.0.16
Host is up (0.00081s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
23/tcp open  telnet
80/tcp open  http

Nmap scan report for 10.60.0.17
Host is up (0.0014s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE
9/tcp    open  discard
13/tcp   open  daytime
19/tcp   open  chargen
21/tcp   open  ftp
23/tcp   open  telnet
37/tcp   open  time
```

Welcome to hacker's paradise

- Offene Zugänge zu Bedienoberflächen.



Welcome to hacker's paradise

- Offene Zugänge zu Bedienoberflächen.


Enter a search query
Search
Total Results: 111
Top Services
BACnet 49
8081 21
HTTP (82) 7
HTTP (81) 7
NetBIOS 5
Top Countries
DE 24
IT 20
GB 12
ES 10
NL 9
Top Organizations
Deutsche Telekom AG 13
Telekom Austria 6
Vodafone Italia 5
Telecom Italia Busin... 4
Wirelesslogic Ltd 3
England
London
Amsterdam
Den Haag
Nederland
Belgique — België
Deutschland
Frankfurt am Main
Paris
France
München
Österreich
Česko
Praha
Zürich
SHODAN MAPS

Penetration testing

Penetration testing

- Drei Studenten ohne einschlägiges Vorwissen.
- Circa zwei Wochen Arbeitsaufwand.

Penetration testing: Boot-log

```
15:36:06 user.notice ddc4000: Sat Jan 18 02:08:52 CET 2014
15:36:06 user.info kernel: [    1.231812] fp4000 90000000.fp4000:
fp4000_probe: base=0xc70be000 irq=28
15:36:06 user.notice ddc4000: erstellt durch
XXXX@linux-bzdak-build-2 ( )
15:36:06 user.debug kernel: [    1.232720] irq: irq 2 on host
/soc@fff00000/pic@0 mapped to virtual irq 29
15:36:06 user.notice ddc4000: in:
/home/XXXX/build/targets/Target-Rel.1.11.x
15:36:06 user.warn kernel: [    1.232968] OLD or4/br4: 0xffff8926 0x90000401
15:36:06 user.notice ddc4000: ws:
/home/XXXX/build/workspace/ddc4000_head
15:36:06 user.warn kernel: [    1.233070] FP4000 Init ChipSelect #4
at 0x90000000
15:36:06 user.notice ddc4000: ################################
15:36:08 local6.info ddc4000: d4run starte Daemon: cmd='/usr/bin/uiclient-4200
/etc/uiclient-4200.cfg', registerFile=/tmp/d4run_605.register
15:36:09 authpriv.warn dropbear[609]: Failed reading
'/etc/dropbear/dropbear_dss_host_key', disabling DSS
15:36:56 syslog.info syslogd started: BusyBox v1.18.4
```

Ergebnisse

- Voller root-Zugang durch Passwort-Raten.
- Uralte Kernel-Version.
- Selbst "gestrickter" Webserver von 2007.
- Sensibel für Brute-Force - 4-stelliges numerisches Passwort und beliebig viele Versuche.
- Sensibel für DoS (ICMP u.a. Protokolle) - stürzt ab.


Enter a search query
Search
Total Results: 111
Top Services
BACnet 49
8081 21
HTTP (82) 7
HTTP (81) 7
NetBIOS 5
Top Countries
DE 24
IT 20
GB 12
ES 10
NL 9
Top Organizations
Deutsche Telekom AG 13
Telekom Austria 6
Vodafone Italia 5
Telecom Italia Busin... 4
Wirelesslogic Ltd 3
England
London
Amsterdam
Den Haag
Nederland
Belgique — België
Deutschland
Frankfurt am Main
Paris
France
München
Österreich
Česko
Praha
Zürich
SHODAN MAPS

Rob Joyce, Chief of Tailored Access Operations, National Security Agency, spricht über seine Tätigkeit als staatlicher Hacker

Ergebnisse - Sicherheit der verwendeten Protokolle

- Bei den am häufigsten auf der Feldebene eingesetzten Protokollen KNX und LON verheerend.
  - Verschlüsselung und Authentisierung sind in den entsprechenden Standards überhaupt nicht vorgesehen oder praktisch nicht von Nutzen.
  - Lebensdauer über 30 Jahren üblich. Ein Umstieg auf Protokolle mit besserem Schutz scheidet kurz- und mittelfristig aus, da dazu große Teil der Haustechnik ersetzt werden müssten.
- Auch in den IP- basierten Netzwerken wird das Potential bekannter Schutzmaßnahmen nur selten genutzt. Hier sind ebenfalls ungesicherte Protokolle eher die Regel als die Ausnahme.

Ergebnisse - Zugriffsmöglichkeiten

- Angreifern gelingt es nach Erlangung des physischen Zugangs, z.B. durch Installation eines Zwischensteckers hinter der Deckenverkleidung, beliebige Aktionen auf der Feldebene auszulösen.

- Generell wurden einige - nicht alle - der untersuchten Zugänge auf Programme, Geräte und Gerätefunktionen mit Nutzernamen und Passwörtern gesichert (sonst nichts).

- In IP-basierten Netzbereichen (VLAN) schützt man sich vor physischem Zugang durch Abschließen der entsprechenden Räume. Die Vielzahl der Räume an sich mit vielen Berechtigten und die Vielzahl der möglichen Netzzugänge und Möglichkeiten zur Fehlkonfiguration lassen das als gültigen Schutz fraglich erscheinen.

Ergebnisse - Mögliche Auswirkungen

- Sehr hohes Risiko für beträchtliche Schäden.
- Angriffe mit dem Ziel von Chaos und Aufmerksamkeit sind in den untersuchten Gebäuden besonders leicht durchführbar.
- Beliebige Aktoren können auf der Feldebene angesteuert werden.
- Aufzeichnung von Sensordaten einfach. Auswertungen ermöglichen komplexe Rückschlüsse.

Planung - Weitere Analysen

- Intensivierung der Zusammenarbeit zwischen Haustechnikern und Netzwerktechnikern.
- Übernahme vieler Konzepte aus der Netzwerkwelt möglich und sinnvoll.
- Dokumentation und Fortführung der Dokumentation müssen verbessert werden.

Zusammenfassung

- Wer sein Netzwerk schützen möchte, muss seine Struktur, seine Geräte, seine Schnittstellen kennen.
- Lösungen für Sicherheitsprozesse liegen auf der Hand.
- Erfahrungen sind vorhanden.
- Bewusstsein muss wachsen.