FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Sicherheit und Forensik einer Beckhoff SPS

B.Sc. Gregor Bonney

B.Sc. Benedikt Paffen

Lehrgebiet Datennetze, IT-Sicherheit und IT-Forensik

IT Forensik
FH Aachen

Agenda

- **Einführung (kurz)**
  - SPS
  - Beckhoff's CX5020 SPS
- Welche Schwachstellen haben wir 2014 entdeckt?
- Was hat sich seit dem geändert?
- Welche forensischen Möglichkeiten bieten sich?
- Fazit

Motivation

Buzzword: „Internet of Things“

- Interesse an intelligenten Geräten
- Industrieanlagen sollen „smart“ werden
  - z. B. automatisch Farbe nachbestellen
  - individuelle Kundenwünsche berücksichtigen

Cyber-Physical Systems:

- stark vernetzte, technische Anlagen

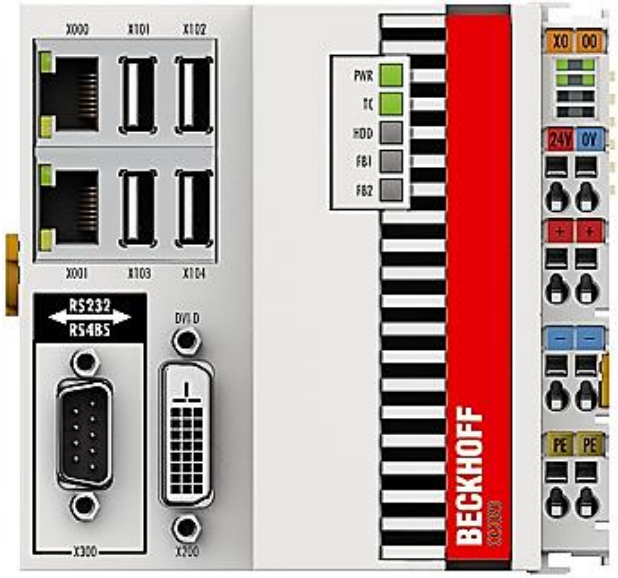
CX5020:

- repräsentativ für aktuell genutzte Hardware

Einführung: Beckhoff's CX5020 SPS

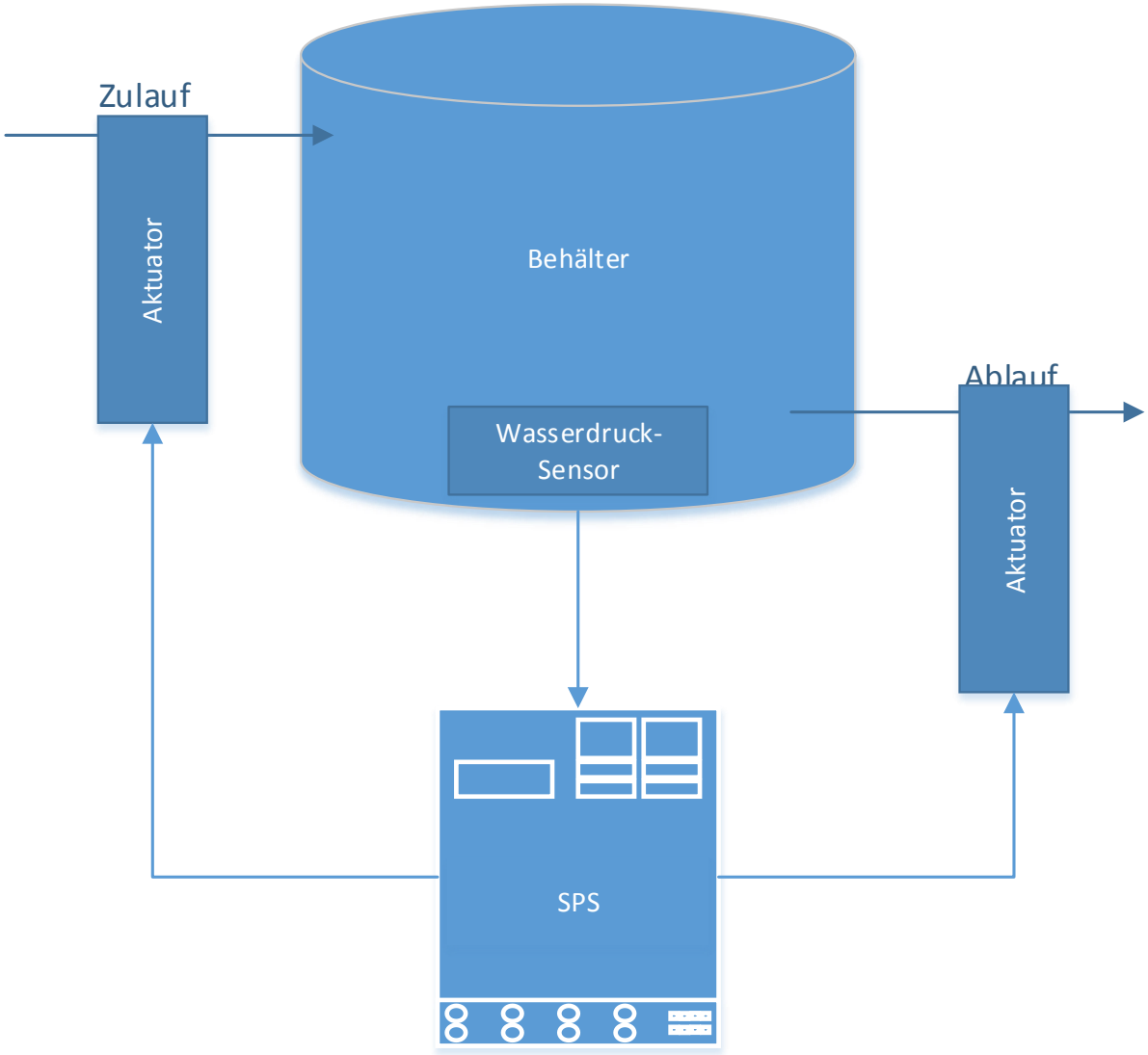
Beckhoff CX5020:

- Mini-Computer
  - Tastatur und Maus über USB
  - Monitoranschluss (DVI)
  - 2 Netzwerkanschlüsse
- Auslieferungszustand
  - Windows CE
  - ohne Kennwort (Administrator)
  - keine Firewall aktiv

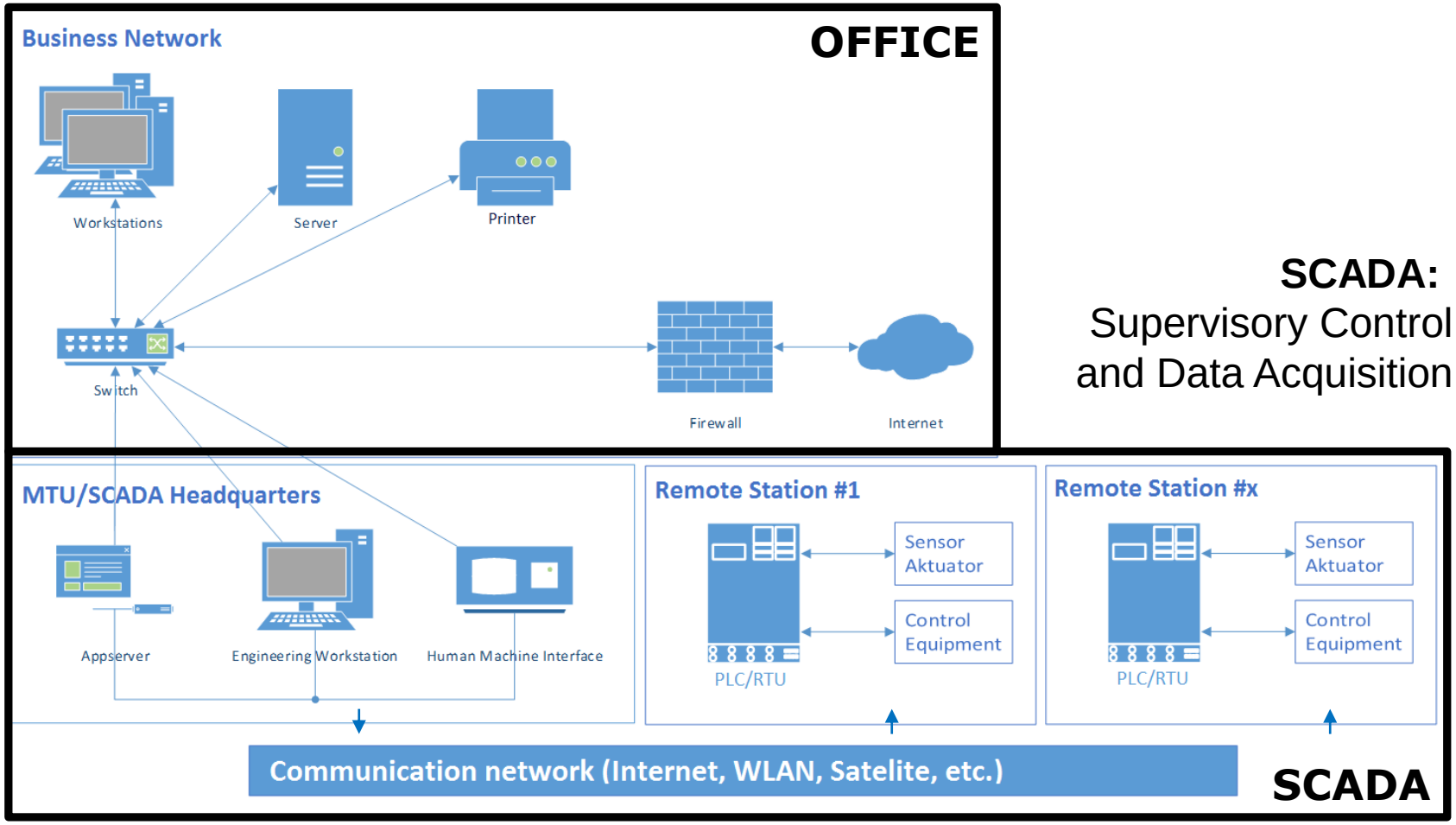


Quelle: Beckhoff.com

Einführung: Was macht eine SPS?

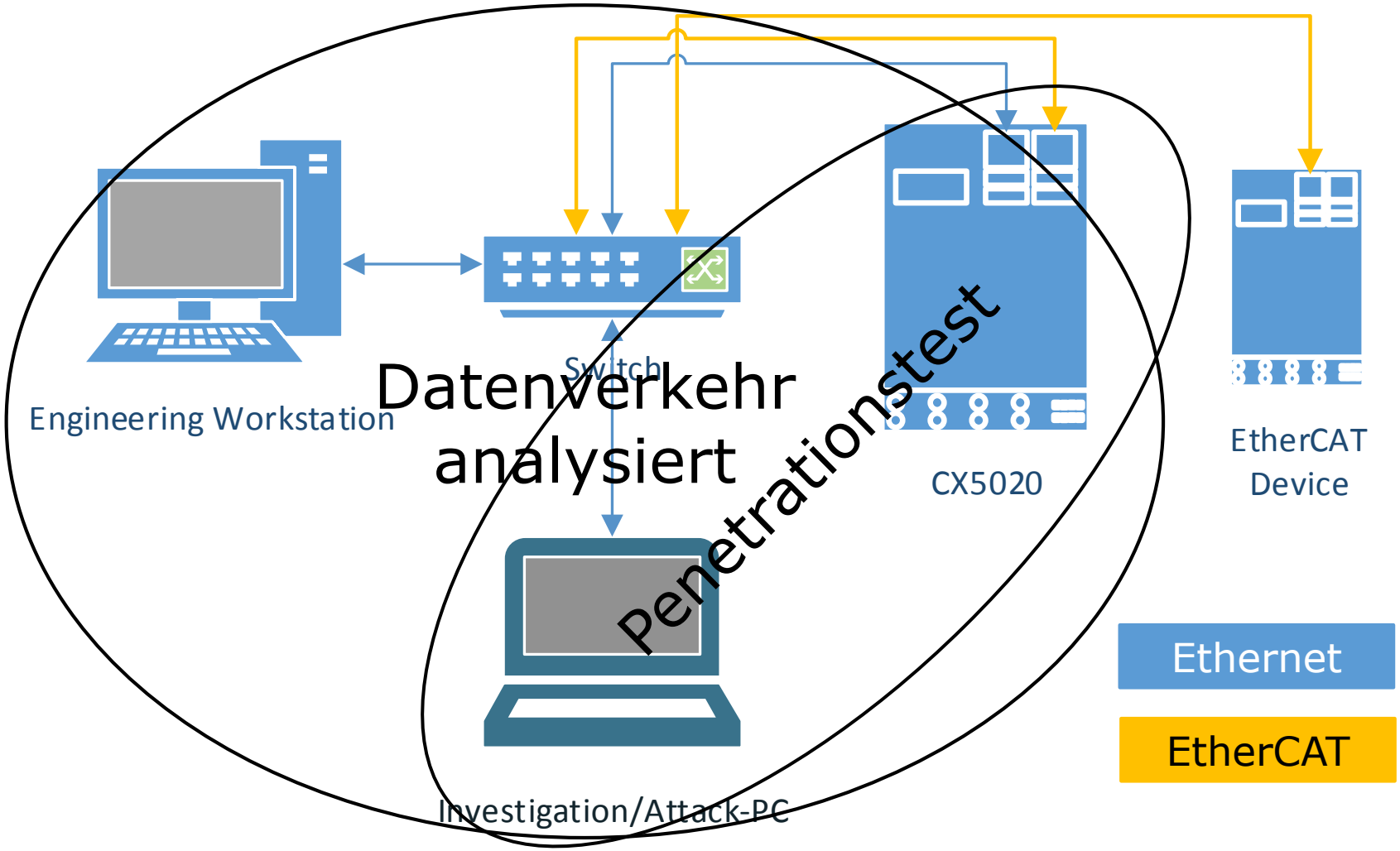


Einführung: SCADA System



SCADA:
Supervisory Control and Data Acquisition

Einführung: Untersuchungs-Setup



Agenda

- Einführung (kurz)
  - SPS
  - Beckhoff's CX5020 SPS
- **Welche Schwachstellen haben wir 2014 entdeckt?**
- Was hat sich seit dem geändert?
- Welche forensischen Möglichkeiten bieten sich?
- Fazit

CX5020: Port Scan

PORT	STATE	SERVICE	VERSION
23/tcp	open	telnet	Pocket CMD telnetd
80/tcp	open	http	ChipPC Extreme httpd (WinCE 6.00)
139/tcp	open	netbios-ssn?	
443/tcp	open	tcpwrapped	
445/tcp	open	netbios-ssn	
987/tcp	open	unknown	
5120/tcp	open	http	ChipPC Extreme httpd (WinCE 6.00)
5357/tcp	open	http	ChipPC Extreme httpd (WinCE 6.00)
8080/tcp	open	http-proxy	
48898/tcp	open	tcpwrapped	
123/udp	open	ntp?	
137/udp	open	netbios-ns	Samba nmbd (workgroup: d)
138/udp	open|filtered	netbios-dgm	
161/udp	open	snmp	SNMPv1 server (public)
1900/udp	open|filtered	upnp	
48899/udp	open|filtered	unknown	

CX5020: Telnet

```
23/tcp    open          telnet       Pocket CMD telnetd
```

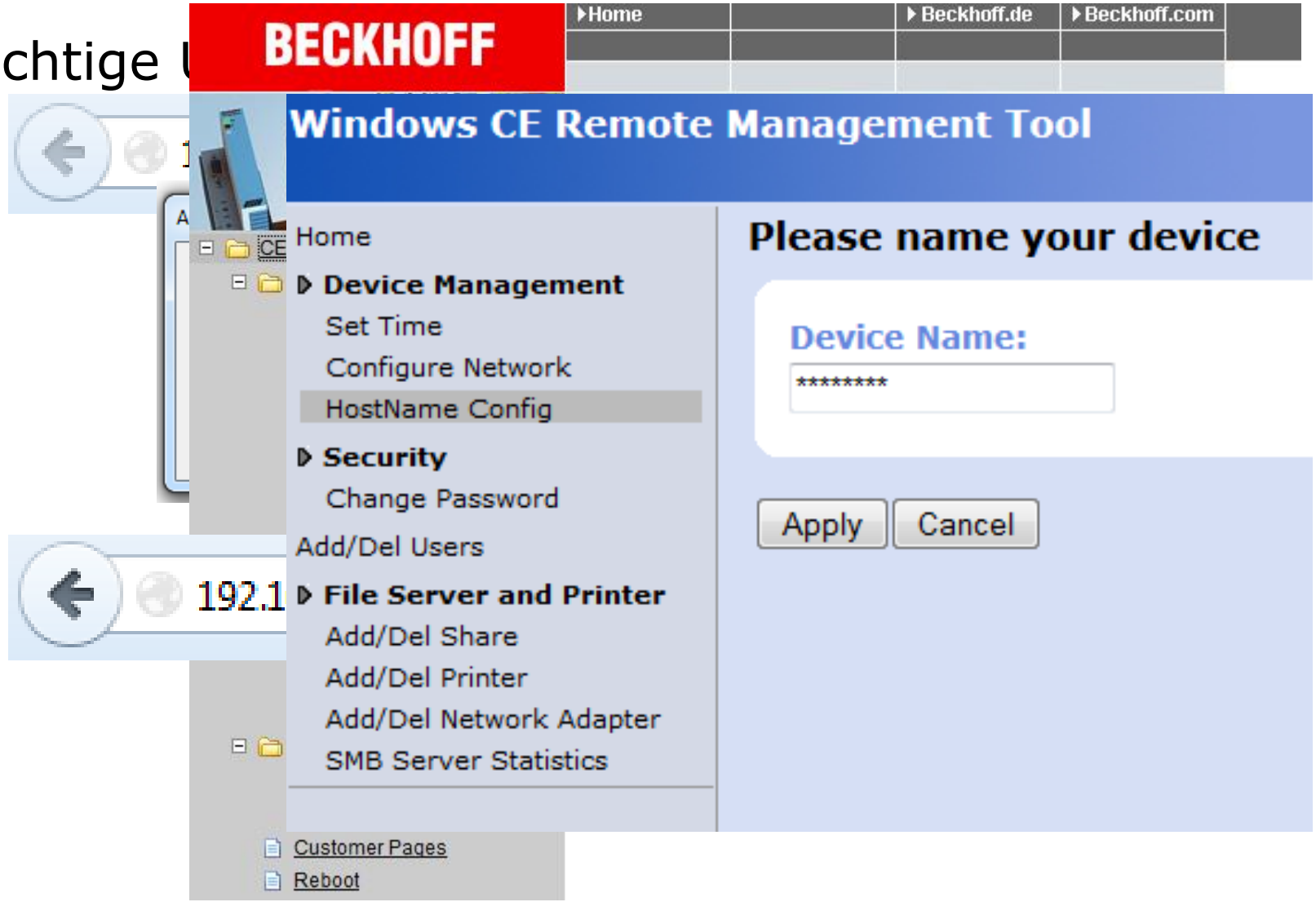
```
Trying 192.168.1.20...
Connected to 192.168.1.20.
Escape character is '^]'.




Welcome to the Windows CE Telnet Service on CX-ABCDEF

login:
```

- per Default aktiviert
- default username/password: webguest/1
- Windows CE 6.0 ist ein single user system
  - alle Nutzer haben Admin-Rechte
    - *weitere Accounts anlegen*
    - *CxAddUser*

CX5020: Webserver

```
80/tcp    open          http          ChipPC Extreme httpd (WinCE 6.00)
```

Wichtige U



CX5020: CE Remote Display

```
987/tcp    open          unknown
```

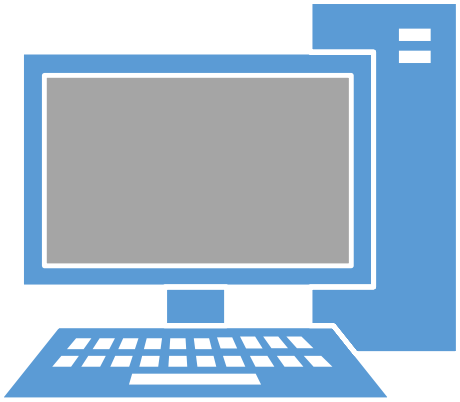
> remote desktop service für Windows CE

> Kennwort ist optional

> User hat vollen Systemzugriff

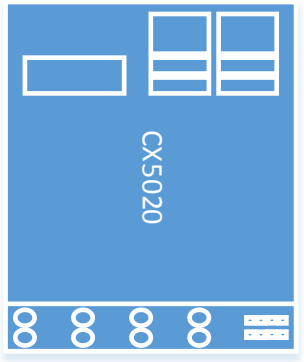
CX5020: Programmier-Port

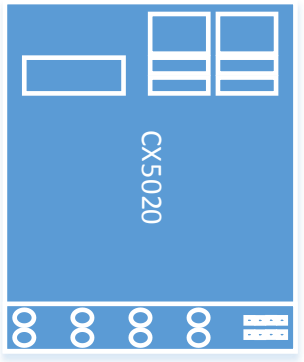
```
48898/tcp open          tcpwrapped
48899/udp open|filtered unknown
```



TwinCAT System Manager

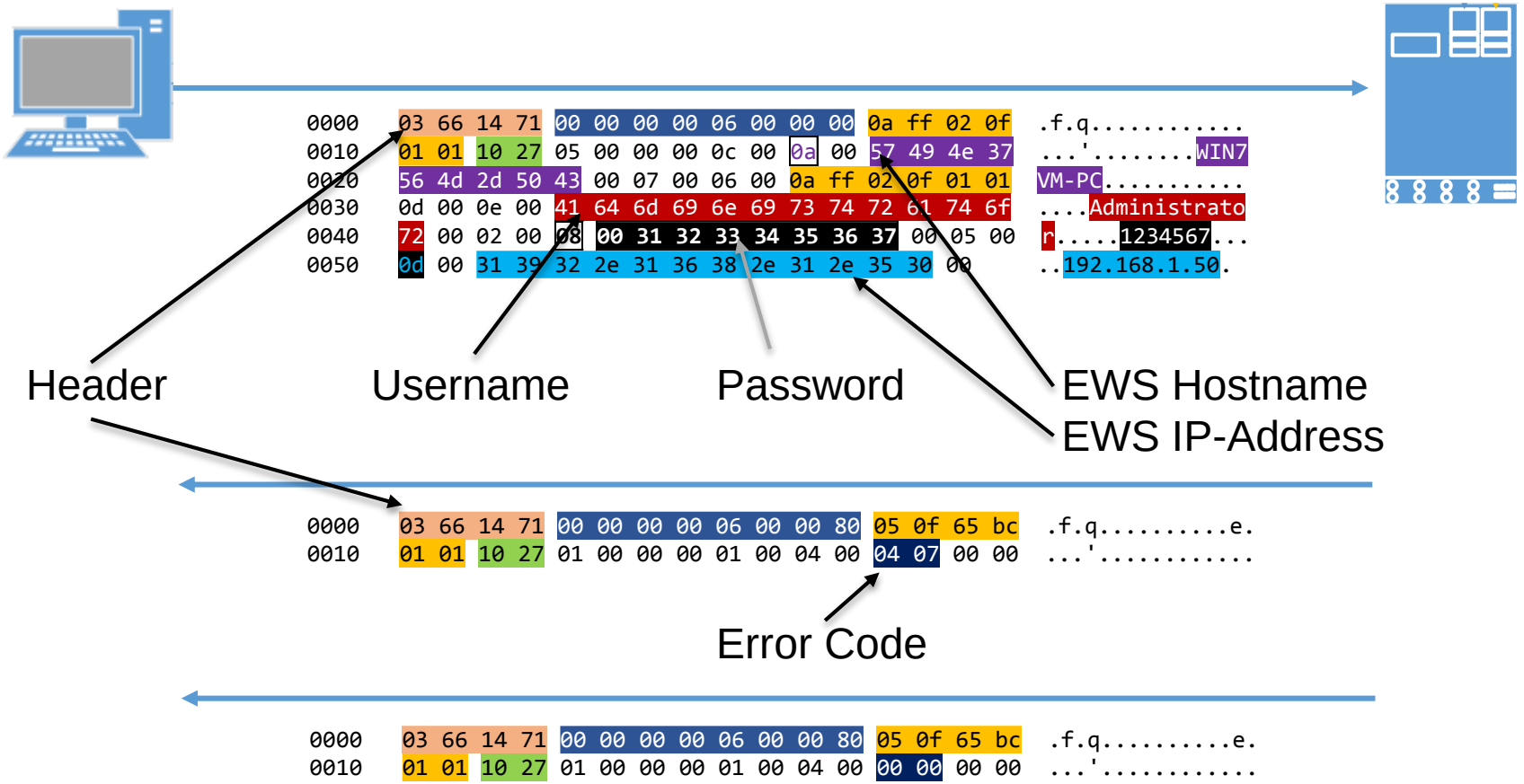
→ Suche nach Geräten
→ Gefundenes Gerät hinzufügen
→ Programme uploaden





CX5020: Programmier-Port

```
48898/tcp open          tcpwrapped
48899/udp open|filtered unknown
```



Angriffsmöglichkeit 1

Kombination: Webserver + Telnet

> Erzeugt ein neues Benutzerkonto “Admin”

- Login via Telnet
- Services starten/stoppen
- neuen VPN Account anlegen
- pivoten ins Business Netzwerk

Angriffsmöglichkeit 2

Programmier-Port Angriff:

- ☑ brute force/dictionary attack
- ☑ PCLs antworten sehr schnell ☺
- ☑ Accounts werden nicht deaktiviert ☺☺
- ☑ parallele Verbindungen möglich ☺☺☺

> Geschwindigkeit: *ca. 8000 Kennwörter/Sekunde*

- *Vergleich SSH: ca. 3-50 Kennwörter/Sekunde*

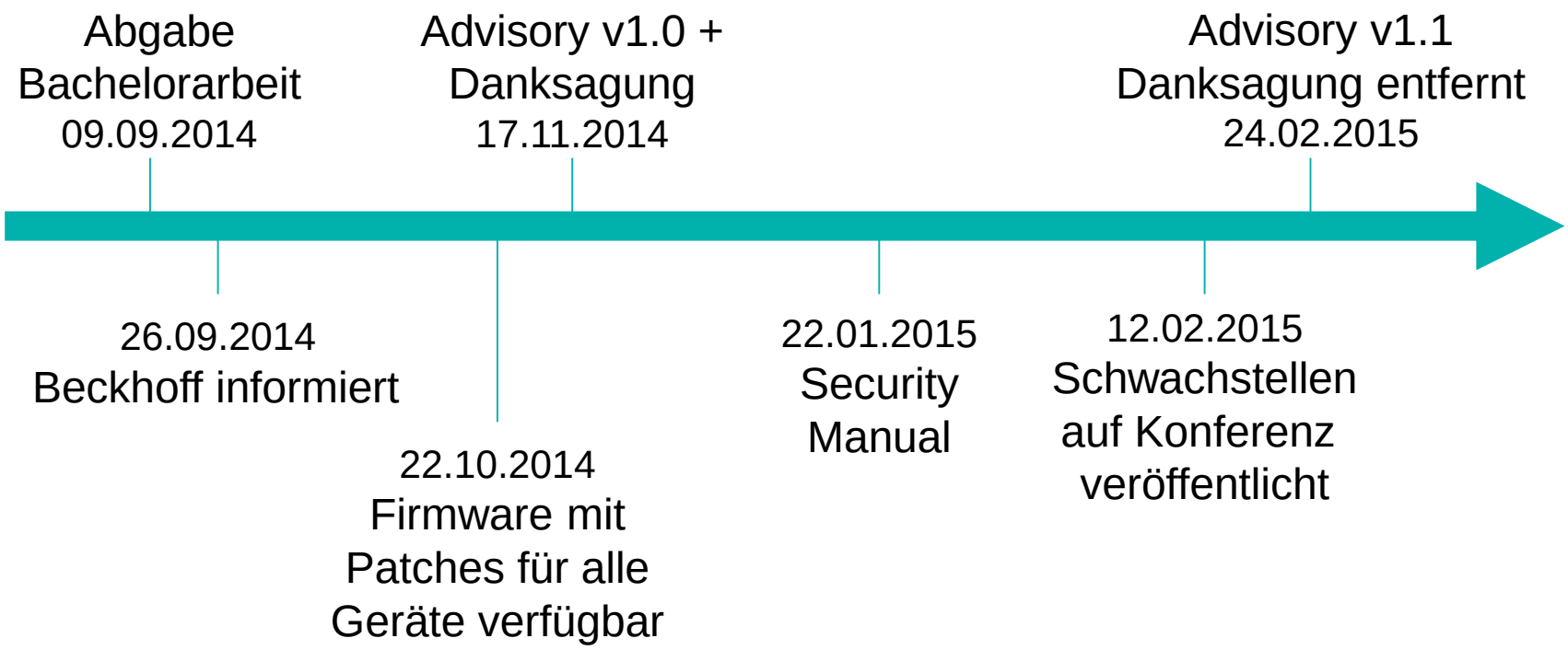
Angriff auf VPN

> **VPN Technik ist PPTP** *mit mschapv2*

```
Creating index file (almost finished) ...Done.
asleap 2.2 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>
        hash bytes:         63cb
        NT hash:            07df657b05ebcd3db637db22017563cb
        password:           0yQB6EiB
[*] Done! =)
```

Kooperation mit Beckhoff

- Verlauf der Zusammenarbeit



Agenda

- Einführung (kurz)
  - SPS
  - Beckhoff's CX5020 SPS
- Welche Schwachstellen haben wir 2014 entdeckt?
- **Was hat sich seit dem geändert?**
- Welche forensischen Möglichkeiten bieten sich?
- Fazit

Was hat sich geändert?

- Telnet
  - Deaktiviert per Default
- Webserver
  - /RemoteAdmin deaktiviert
- Programmier-Ports
  - „kein Patchen notwendig“
  - „so gewollt“
- CE Remote Display: weiterhin möglich
- VPN: weiterhin mschapv2
- Passwörter: webguest/1 und guest/1 noch aktiv

Sicherheit von Steuerungen

- Steuerungen von sich aus können keine Sicherheit bieten.....
- ..... können jedoch ergänzen.
- Nicht den eingebauten Sicherheitsmaßnahmen vertrauen
- ICSsysteme unterscheiden sich kaum von normalen Netzwerken
  - !!Sie müssen nur besser geschützt werden!!
- Nur geschultes Sicherheitspersonal für die Einrichtung von Netzwerken einsetzen
- Relevante Komponenten sollten nicht aus dem Internet erreichbar sein

Agenda

- Einführung (kurz)
  - SPS
  - Beckhoff's CX5020 SPS
- Welche Schwachstellen haben wir 2014 entdeckt?
- Was hat sich seit dem geändert?
- **Welche forensischen Möglichkeiten bieten sich?**
- Fazit

Forensiche (Un)Möglichkeiten

- x86 Windows CE auf einer SPS
  - 64MB Flash
  - 1 GB Ram
  - Abgespecktes System
  - Alles in einer NK.bin
- Keine Logdateien
- Registry vorhanden
- Live-Response uns nicht möglich

Forensiche (Un)Möglichkeiten

- .EXE-Dateien auf der SPS
  - x86 Windows CE
    - Keine Windows Mobile Binaries
    - Nur Cross-Compile
      - bisher ohne Erfolg
      - Programmen fehlen DLLs
- NK.bin (Windows CE Firmware)
  - „Nkbintools“ auf XDA
    - Extrahieren
    - Modifizieren
- Registry
  - Fehlende Tools erschweren die Analyse

Forensiche (Un)Möglichkeiten

- Post Mortem Analyse
  - Registry
  - Dateien

Hilfestellungen für Forensik

- Netzwerkforensik ist essentiell

- Daten aus Logdateien notwendig
  - Firewall
  - IPS (?!)

- Verwendung von Terminaldiensten erlaubt Identifizierung von Usern

Fazit

- Live Response eingeschränkt möglich
  - Ce-Remote Display
- Kein RAM-Dump
- Verlass auf bestehende Infrastruktur notwendig

Vielen Dank für Ihre Aufmerksamkeit

Gibt es Fragen?

Kontaktmöglichkeit:

benedikt.paffen@alumni.fh-aachen.de
gregor.bonney@alumni.fh-aachen.de