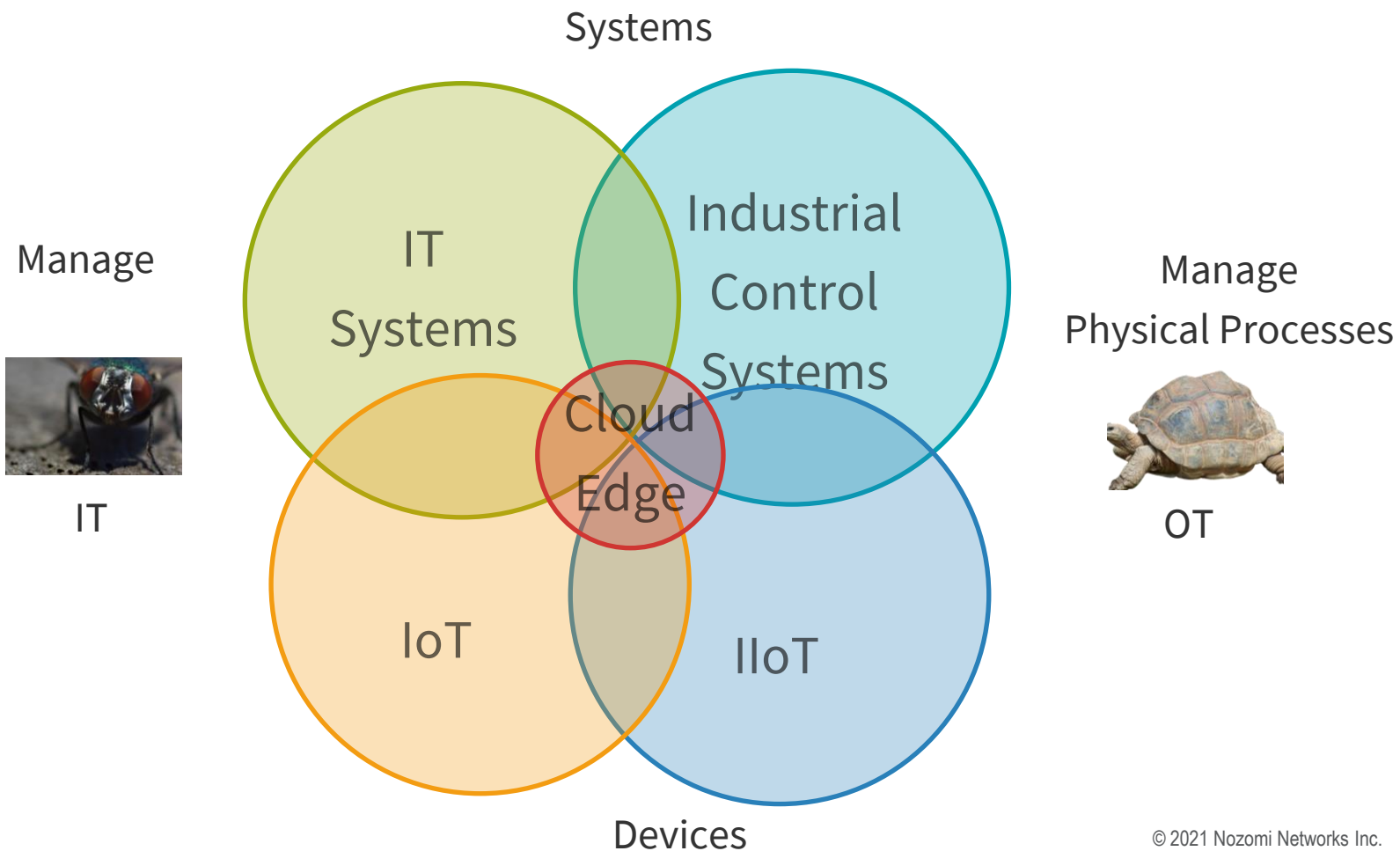


Top 10 Cyber Security Mistakes in Industrial Control Systems

Herbert Dirnberger



IT Bleeding Edge meets OT Legacy



Next Generation IIoT



“Industrial Edge Computing”
with Industrial IoT Controller

**“The Industrial Internet of Things
and service is not an upgrade,
it is a new world of technology.”**

Industrial Cyber Security

Verkürzung von Inbetriebnahmezeiten

- durch Best Practices und Standards
- (ressourcenschonende) Inbetriebnahmen
 - Aufbau von lokalem Know How zu OT/Automatisierungstechnik

Erhöhung der Verfügbarkeit

- Steigerung von Robustheit und Resilienz des OT Netzwerkes
- Minimierung von vorhersehbaren Netzwerkausfällen
- Einfachere Fehlersuche
- Schnellere Reaktionszeiten der Servicetechniker
- Vermeidung von Reisezeiten

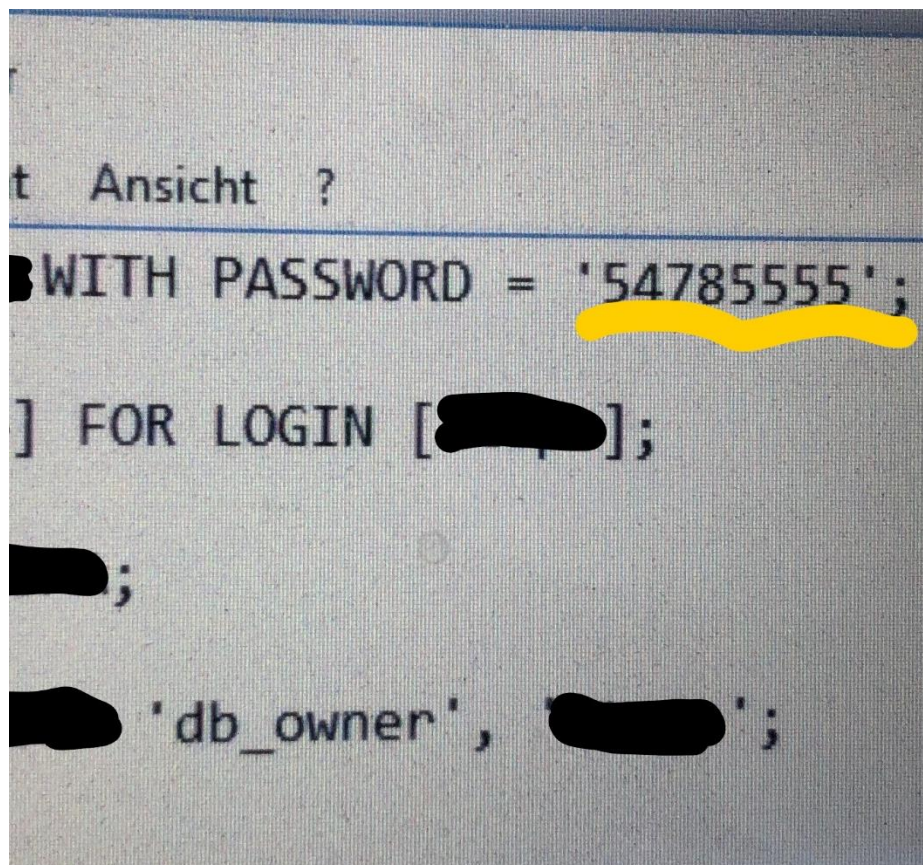
Erhöhung des OT Security Reifegrades

- Netzwerksegmentierung
- Minimierung von Internetzugängen für Maschinen
- Sichere und nachweisbare Fernwartung
- Aktiver Schutz gegen Ransomware



Förderung der sicheren IT/OT Konvergenz

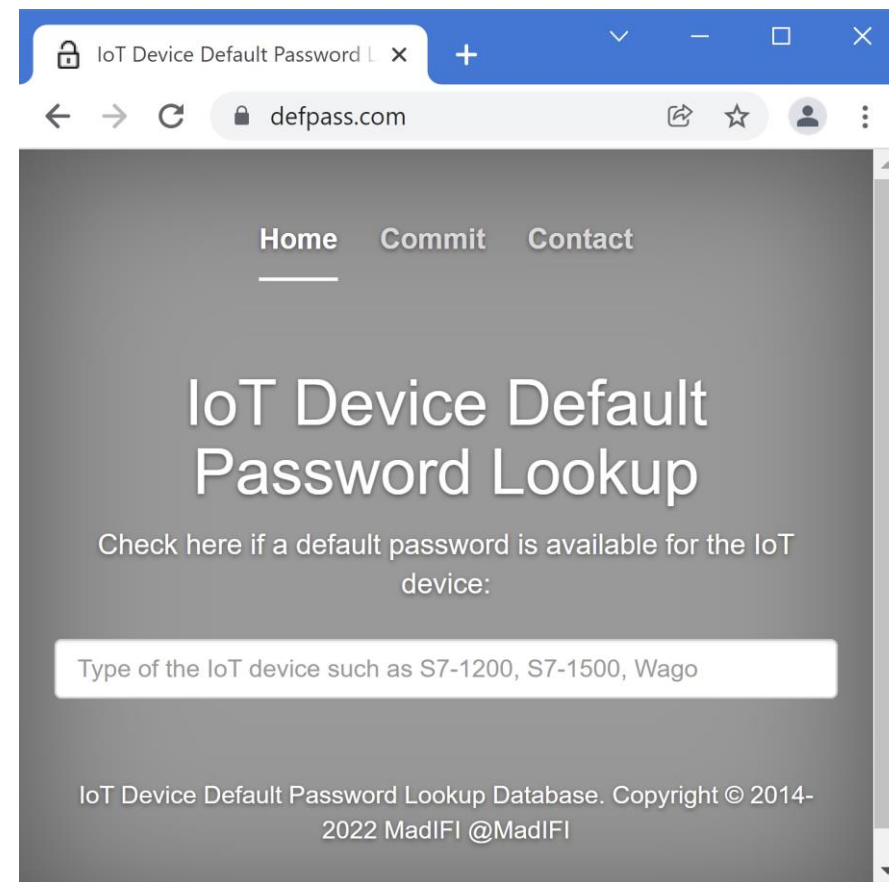
#10 Hardcoded Weak Password for Default User/Admin



```
int CheckLogin(char
*password) {

    if (strcmp(password,
„54785555!") {
        printf("Incorrect
Password!\n");
        return 0;
    }

    printf("Entering
Diagnostic Mode\n");
    return 1;
}
```



#9 Unsecure Protocols

```
telnet
smbv1
pop3
smtp
ldap
tls1.0
ntlm
llmnr
http
snmpv1/v2 ...
```

weak - cleartext
 no use of any crypto
 outdated cryptographic
 legacy
 data accessible without any
 authorisation

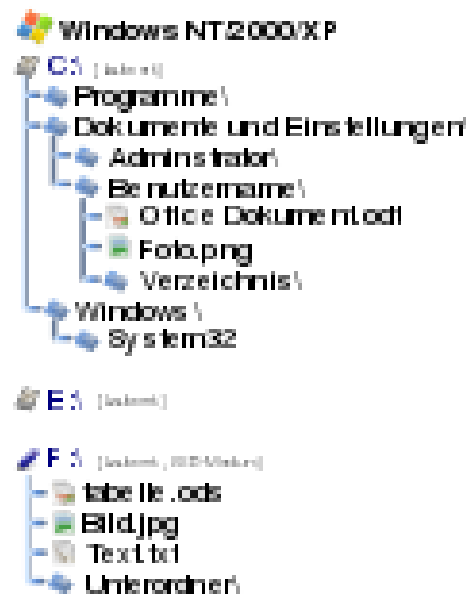
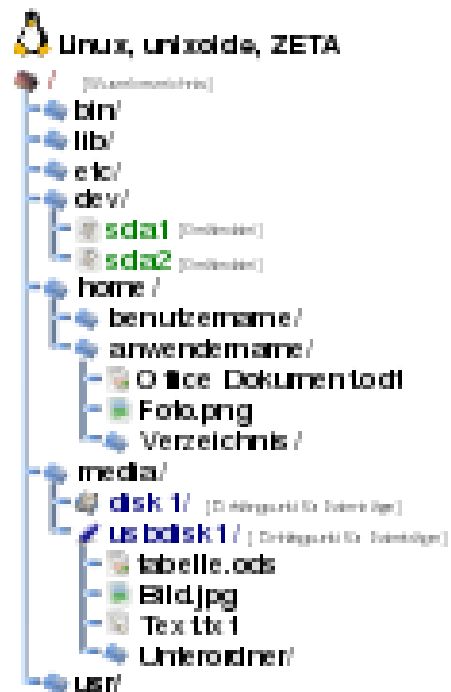
 Alert **Cleartext password** [55a

...
 Detected plain text password authentication for ftp protocol.



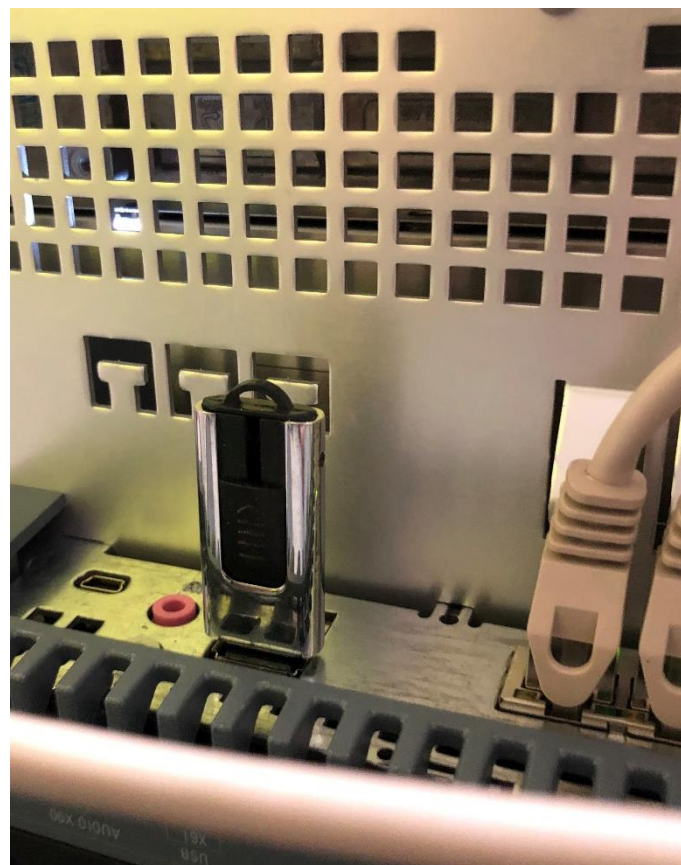
#8 Insufficient File Service Authorization

A suspicious packet was sent [sid:9000009] -- OS-WINDOWS Microsoft Windows SMB a Access Denied. Detected an attempt to establish an anonymous session IPC\$ share with scan attempt for MS17-010.



Incident **Suspicious Activity**

#7 No Restricted USB Media Usage



#6 Discover Unknown Devices with Network Scans



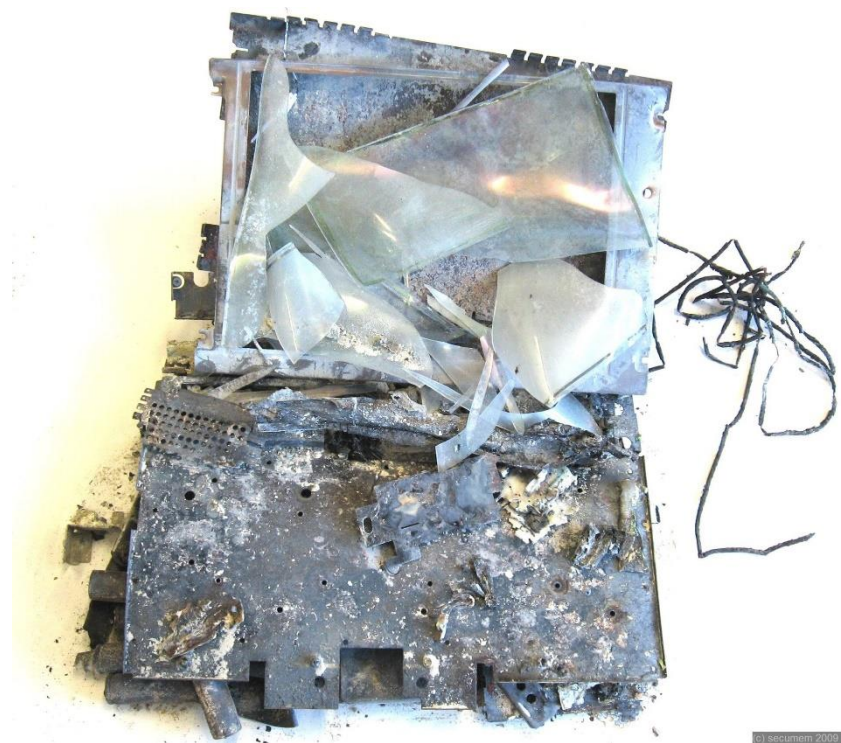
```
root@pensrv: ~ - Befehlsfenster - Konsole
Sitzung Bearbeiten Ansicht Lesezeichen Einstellungen Hilfe

root@pensrv:~#
root@pensrv:~# nmap -T5 wikipedia.de

Starting Nmap 4.20 ( http://insecure.org ) at 2007-12-12 13:26 CET
Interesting ports on m20s26da.ispgateway.de (80.67.25.148):
Not shown: 1673 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
6000/tcp  closed X11
6001/tcp  closed X11:1
6002/tcp  closed X11:2
6003/tcp  closed X11:3
6004/tcp  closed X11:4
6005/tcp  closed X11:5
6006/tcp  closed X11:6
6007/tcp  closed X11:7
6008/tcp  closed X11:8
6009/tcp  closed X11:9
6017/tcp  closed xmail-ctrl
6050/tcp  closed arcserve
49400/tcp closed compaqdiag
50000/tcp closed iiimfsf
50002/tcp closed iiimfsf
54320/tcp closed bo2k
61439/tcp closed netprowler-manager
61440/tcp closed netprowler-manager2
61441/tcp closed netprowler-sensor
65301/tcp closed pcanalyzer

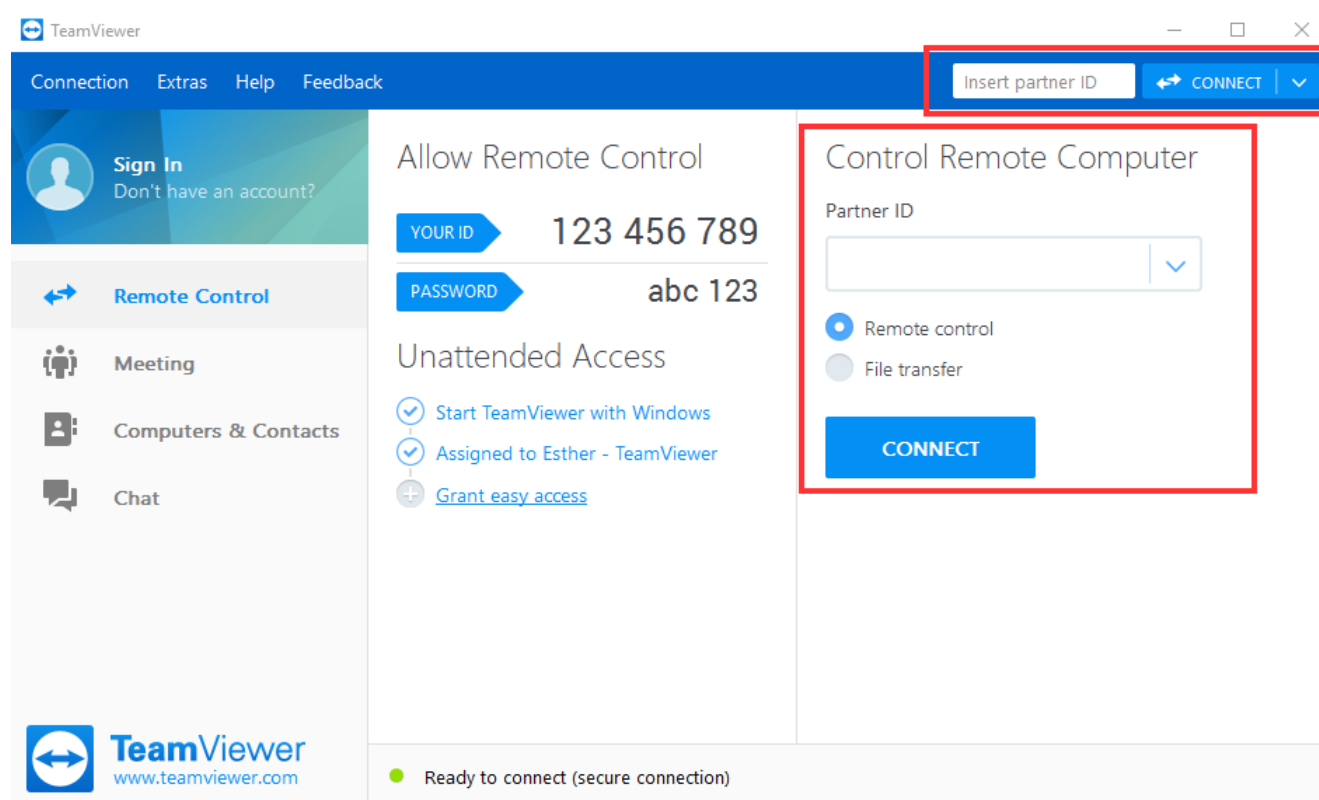
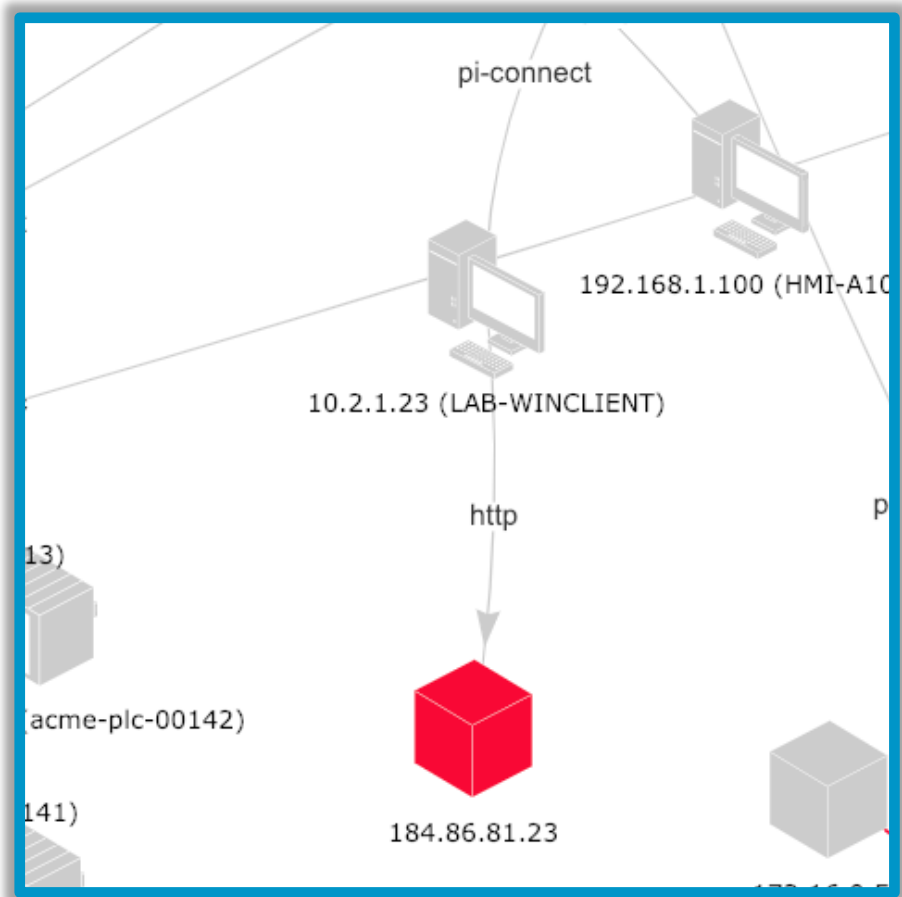
Nmap finished: 1 IP address (1 host up) scanned in 7.274 seconds
root@pensrv:~#
```


#5 Not existent Backups



Von secumem - secumem, CC BY-SA 3.0,
<https://commons.wikimedia.org/w/index.php?curid=5878159>

#4 No Restricted Access to Internet – unknown backdoor remote control



Quelle: Teamviewer

#3 Unsecure Engineering Station



Zugriff zum Internet

„self management“

Schattengerät

Keine Endpoint Protection

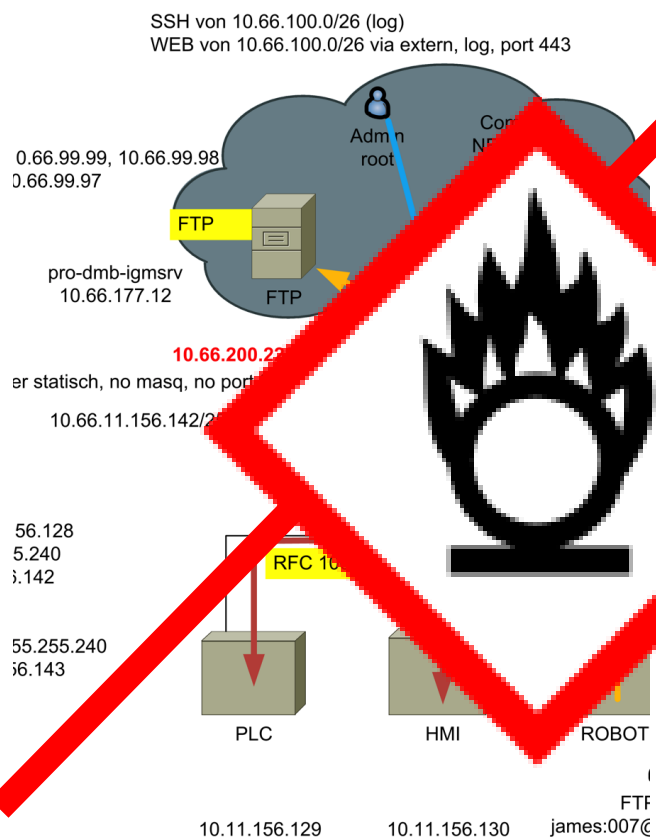
Nicht aktuell gepatcht

Cracked Software

Darf alles, und kommt überall hin!

Von © Raimond Spekking / CC BY-SA 4.0 (via Wikimedia Commons), CC BY-SA 4.0, <https://commons.wikimedia.org/w/index.php?curid=45282376>

#2 Flat Networks – Poor Segmentation



10.0.0.0/8

No Industrial DMZ

No Defined Zones

No Industrial Firewalls

Dual Homed Devices

Profinet meets
Enterprise Core Switch

Lateral Movement

Von Hildegard Markmann – uploader was Hajothu at de.wikipedia
Hildegard Markmann, CC BY-SA 3.0,
<https://commons.wikimedia.org/w/index.php?curid=8823662>



#1 Industrial Control System for Everyone Accessible

Timothy Krause, „Security guard“, CC-Lizenz (BY 2.0)
<http://creativecommons.org/licenses/by/2.0/de/deed.de>
Bild stammt aus der kostenlosen Bilddatenbank www.piqs.de



Herbert Dirnberger, Auszug aus Screenshot der Webseite <http://www.shodanhq.com>





Erste Hilfe

- **Ihr bestehender IT Dienstleister**
- **WKO Cyber-Security-Hotline 0800 888 133**
- **IKARUS Security Software GmbH 01 58995 450**

THANK YOU!

Herbert Dirnberger
Industrial Cyber Security Expert



managed IT/OT Security

You've heard from us.

We want to hear from **you**.



+43 1 58995-500



sales@IKARUS.at



<https://www.IKARUS.at>



<https://www.ikarussecurity.com/ueber-ikarus/karriere/>
Cyber Threat Intelligence Analyst OT Security Engineer