IKARUS security software

Top 10 Cyber Security Mistakes in Industrial Control Systems

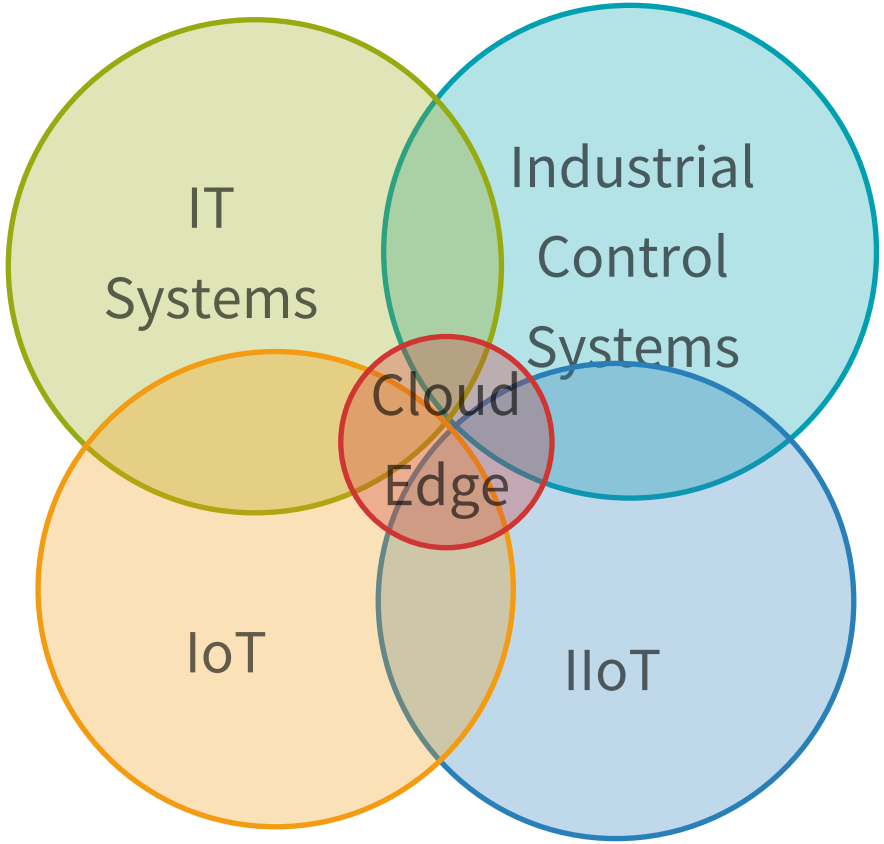
Herbert Dirnberger

IT Bleeding Edge meets OT Legacy

Systems

Manage

IT



Devices

Manage
Physical Processes

OT

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

- (resssoutcenschonende) Inbetriebnahmen
- Aufbau von lokalen Know How zu OT/Automatisierungstechnik

Erhöhung der Verfügbareit

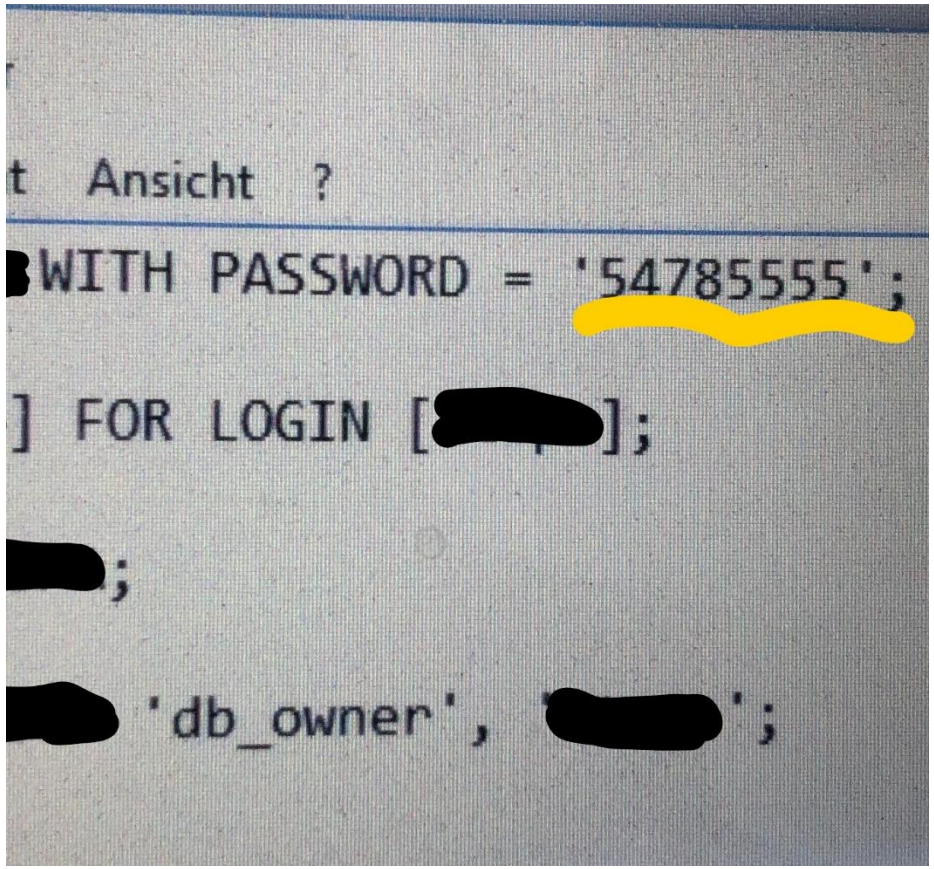
- Steigerung von Robustheit und Resililenz des OT Netzwerkes
- Minimierung von vorhersehbaren Netzwerausfällen
- Einfachere Fehlersuche
- Schnellere Reationszeiten der Servicetechniker
- Vermeidung von Reisezeiten

Erhöhung des OT Security Reifegrades

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

Förderung der sicheren IT/OT Konvergenz

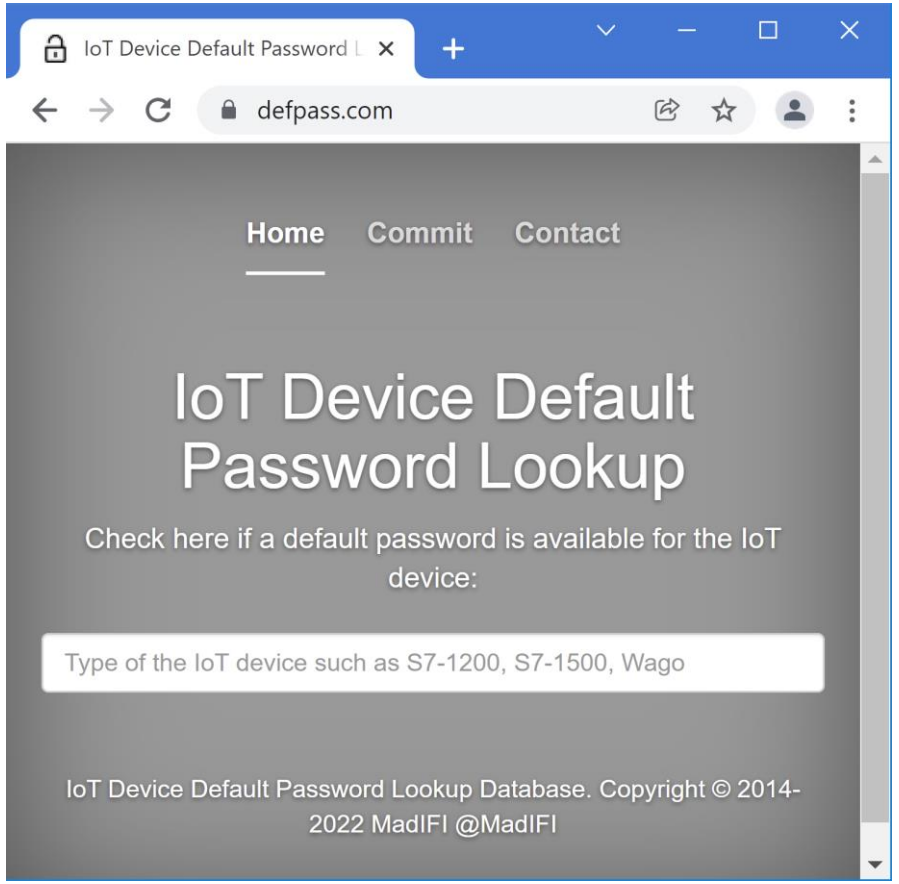
#10 Hardcoded Weak Password for Default User/Admin




```
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outdated cryptograohic
legacy
data accessableithout any authorisation

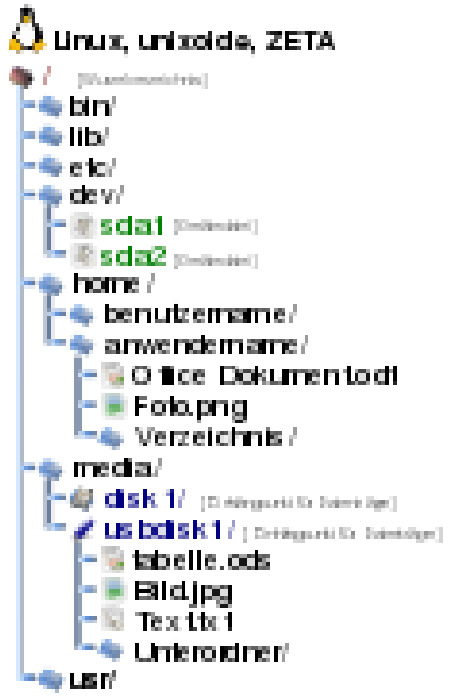
7 Alert **Cleartext password** [55a

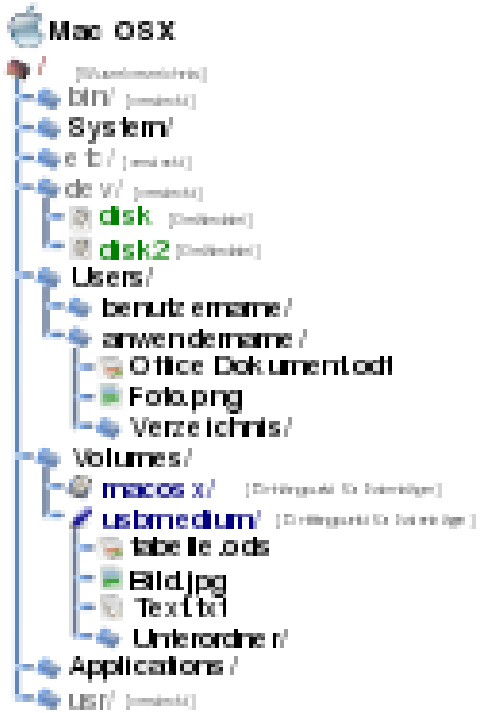
...

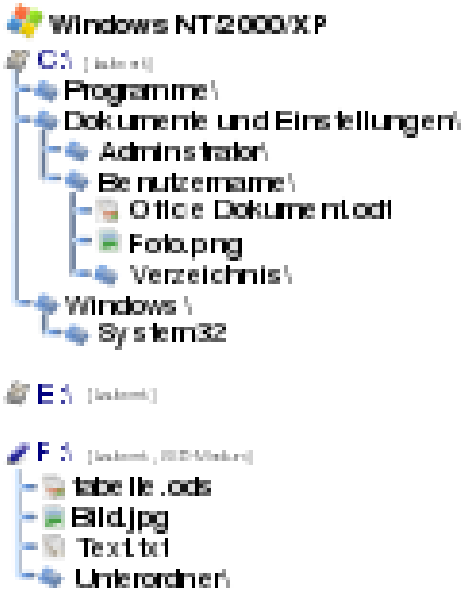
Detected plain text password authentication for ftp protocol.

#8 Insufficent 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 wit scan attempt for MS17-010.

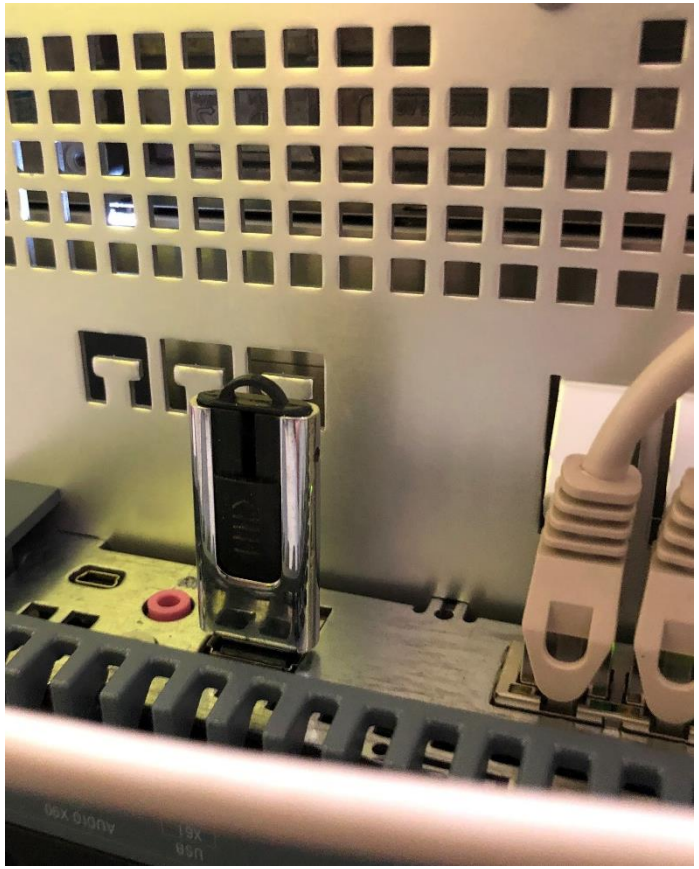




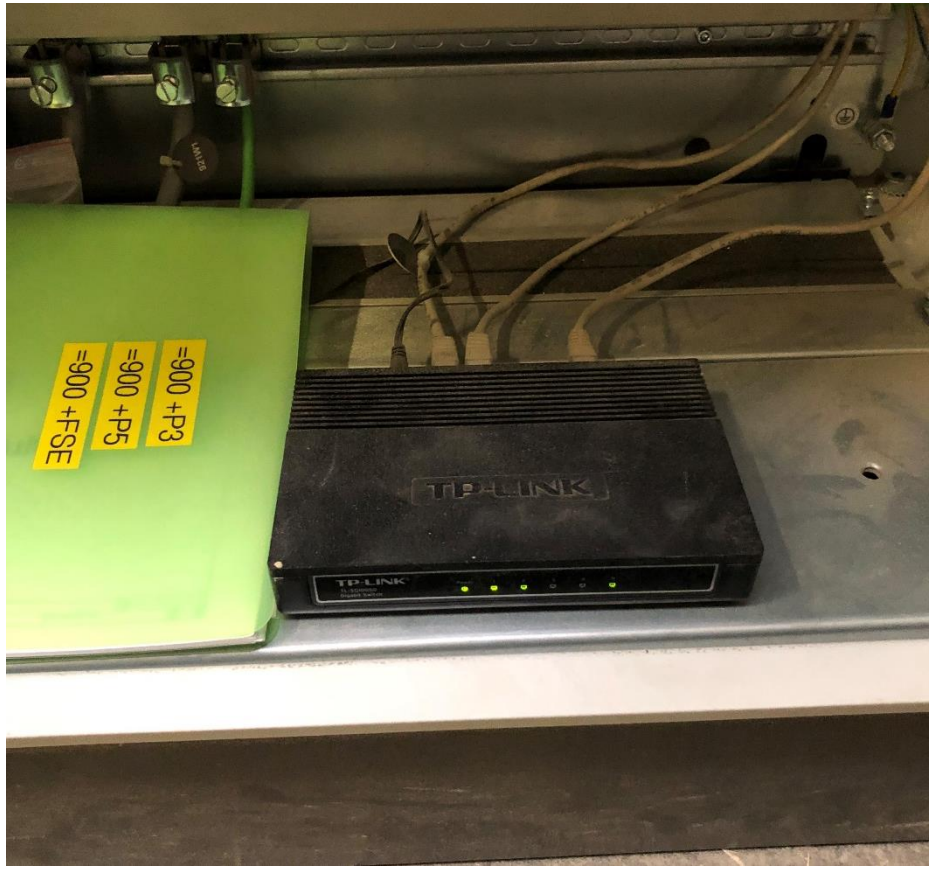


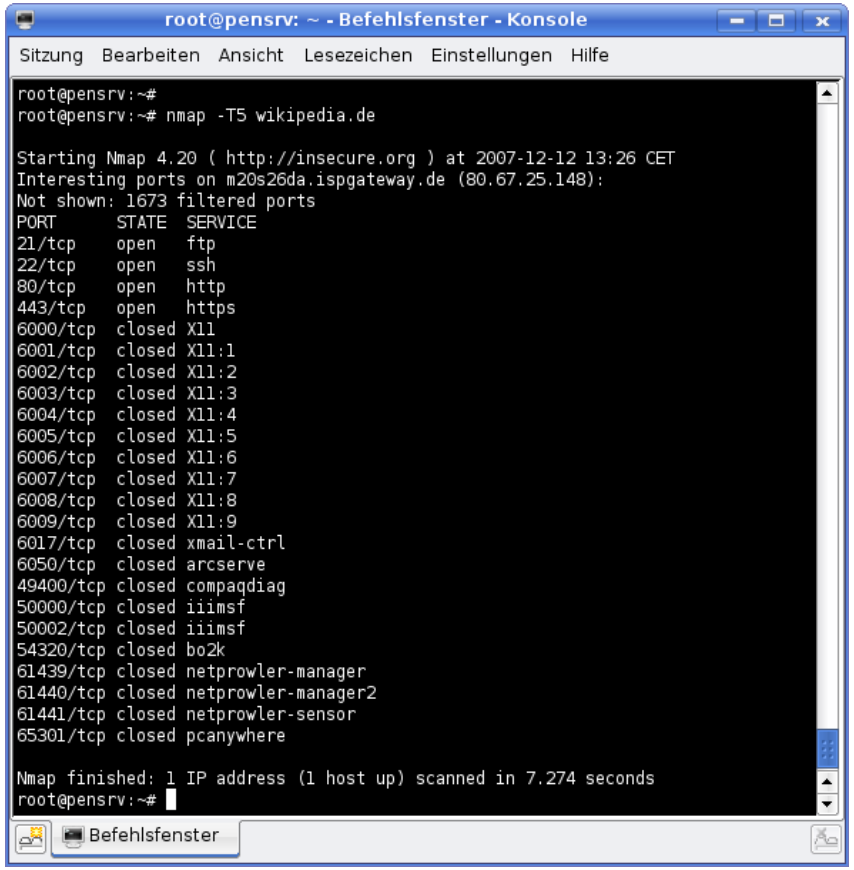
9 Incident **Suspicious Activity**

#7 No Restricted USB Media Usage

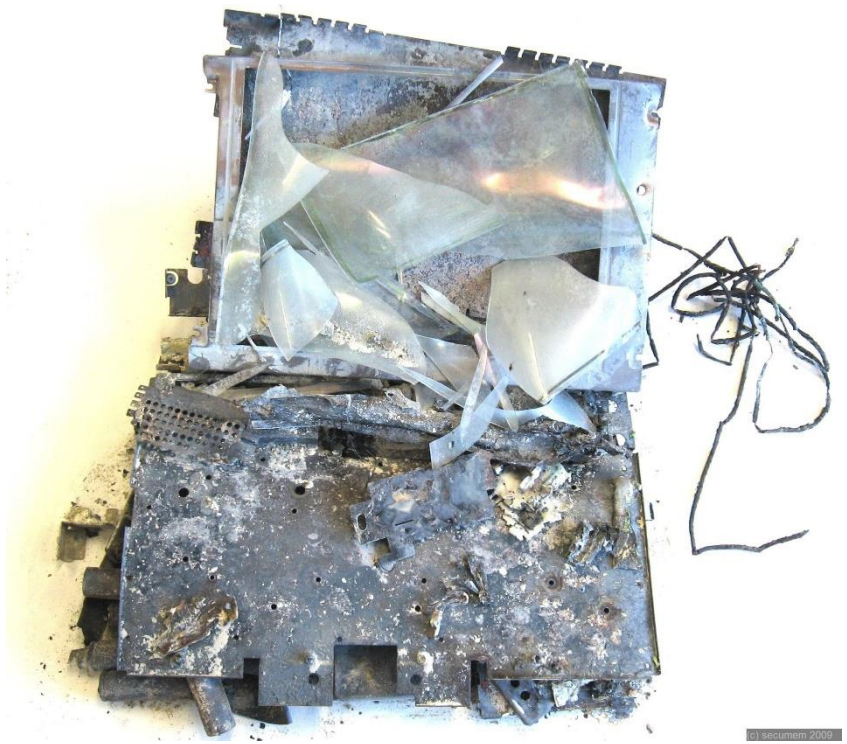


#6 Discover Unknown Devices with Network Scans



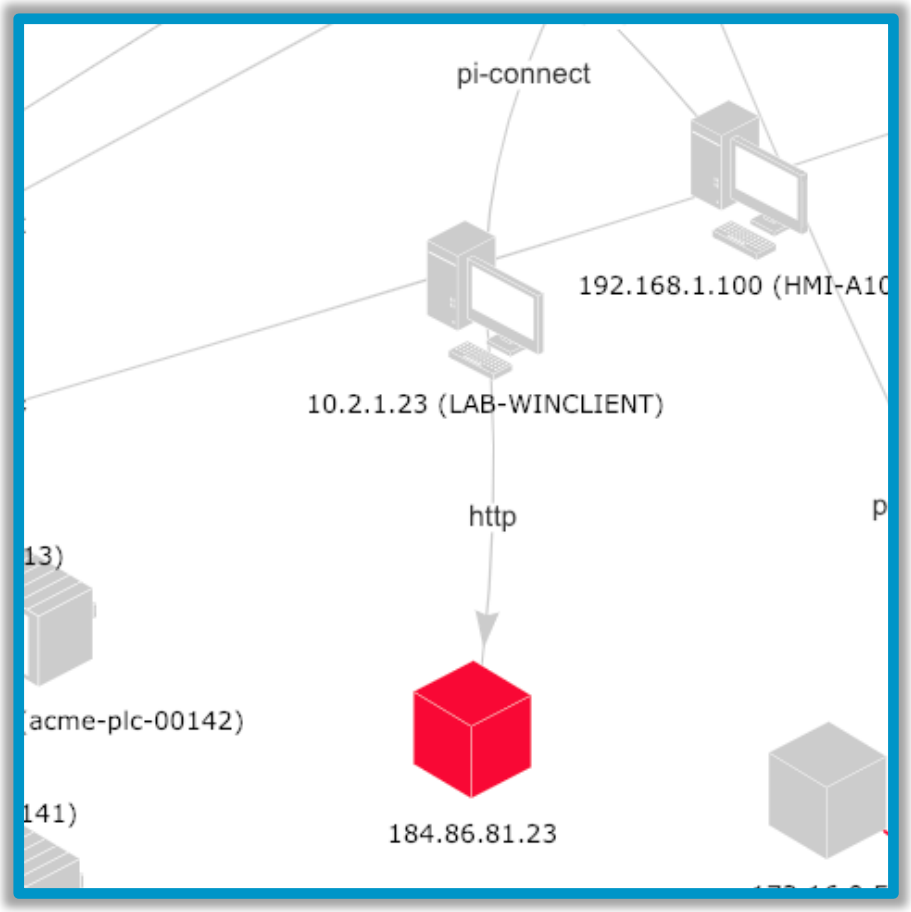


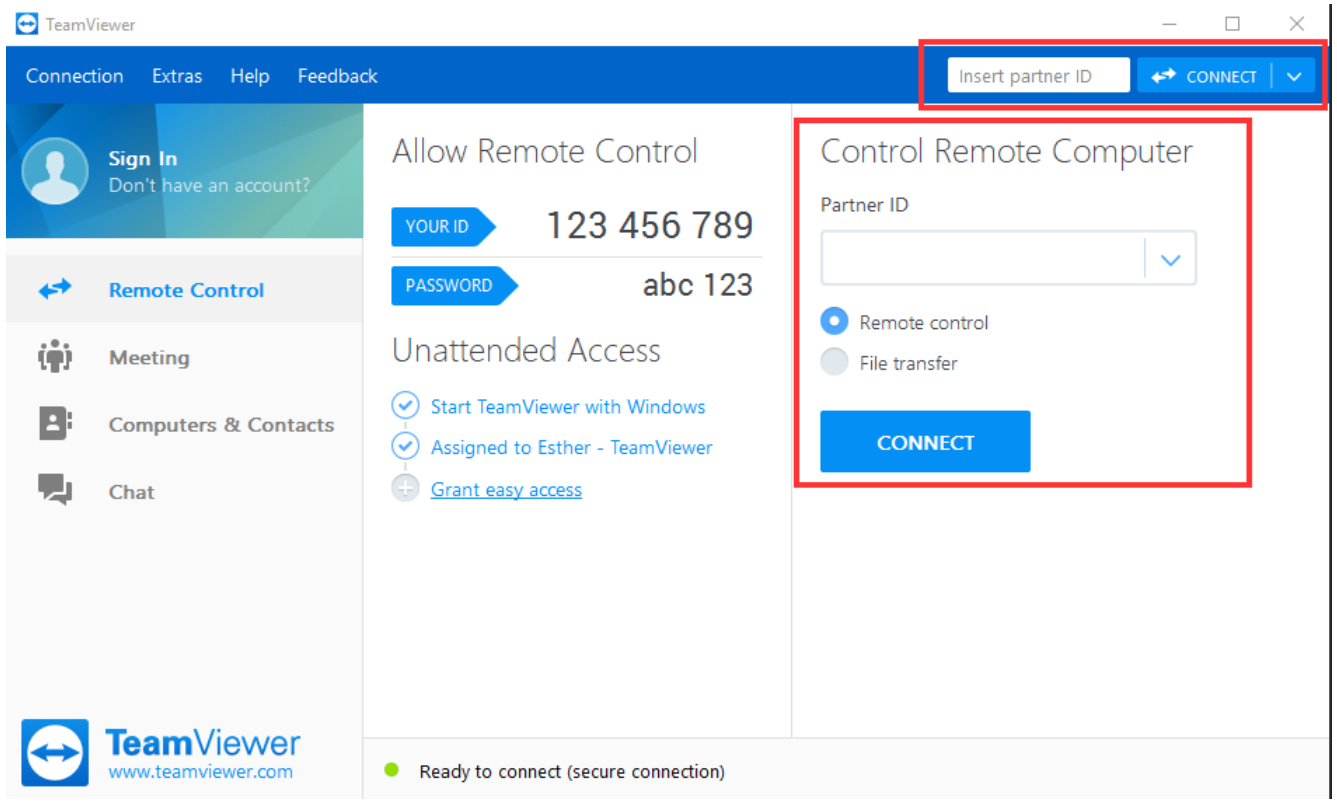
#5 Not existent Backups



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

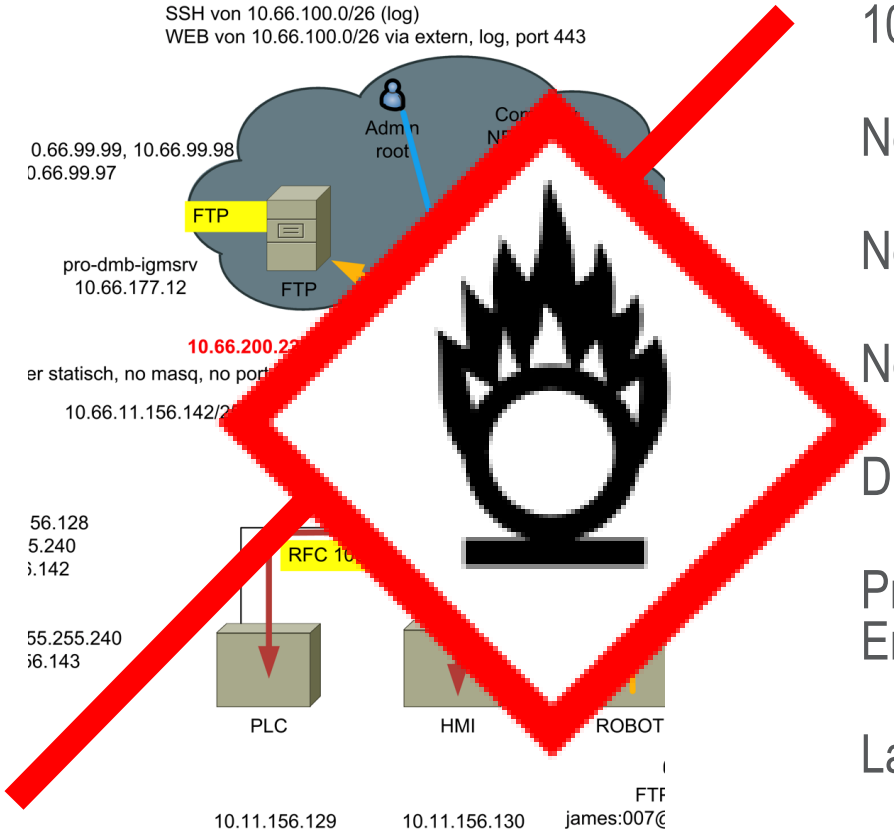
Keine Entpoint Protection

Nicht aktuell gepacht

Cracked Software

Darf alles, und kommt überall hin!

#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 Hajotthu 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

FIREEYE MANDIANT NOZOMI NETWORKS

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