IoT Conference 2016

TELCO TECH NETWORK SECURITY
ENGINEERED IN GERMANY

AXIOMTEK

May 12, 2016, IoT Nuremberg

IT-Security in industrial Environments

Scenarios of integrated IT-Security
to protect networks

Agenda

1. Case Studies of Attacks
2. Wording and Concept
3. Design of a UTM/Firewall
4. Examples of Attacks on Infrastructure
5. Zusammenfassung/Summary
6. LISS
7. TELCO TECH GmbH

Case Studies of Attacks 1

Example 1

A fake train-controlsystem was set up with real hardware and recorded videos from supervision cameras in order to attract hacker. The test simulation designed by Sophos called "Honey Train" recorded 2.7 million attacks within six weeks. The majority of access attempts have targeted the firewall and the media server, for which there are standard tools for hackers.However, two of the attacks could have caused potential damage. They have been able to log into a the HMI servers (Human Machine Interface). Through this interface, they could have easily manipulated signals. The attackers used so-called dictionary attacks, in which the passwords is determined on base of a list of popular standard passwords.

(Quelle und Bildmaterial: Heise 09/2015)

Case Studies of Attacks 2

On the Blackhat 2015 a new attack against Siemens Industrial PLCs (Programmable Logic Controller) was shown. Different from Stuxnet which was designed to intrude via an personalized attack from a work station, the attack shown was based on just using the internet connection of the PLC.

In this case the attackers were able to download the program running on the PLC as a MC7 (assembler-like machine code) to manipulate the program and to load their own routines up to the PLC. There, the manipulated program was executed. The researchers could realized a network scanner whose result was sent to the researchers. In addition, they could set up a proxy, which allowed access to the production network over the infected PLC. Most security mechanisms could be by-passed and exposed to the fabrication network a much larger attack surface as expected.

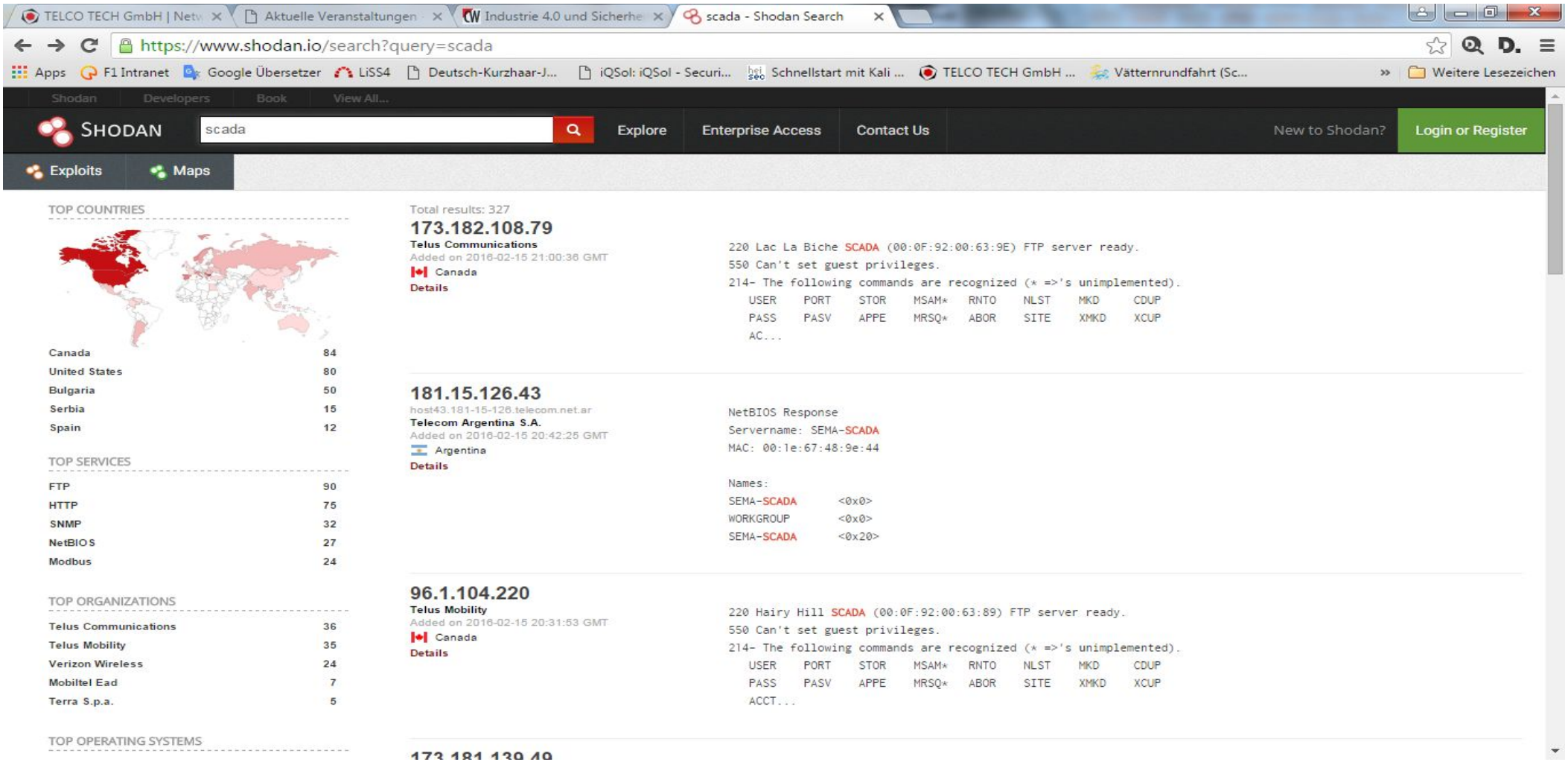
(Quelle und Bildmaterial: datenschutz-notizen 08/2015)

Case Studies of Attacks 3

In the past, industrial control systems were isolated and therefore considered safe. A mistake, because an infected USB stick is enough to infect most critical infrastructure. The the virus system of BlackEnergy2 showed that security incidents are in complex, regulated SCADA software environments not uncommon. The Kaspersky Security Network identified by the end of 2014 about 13,000 incidents per month in which computers with automatic process control systems - could be infected with a malicious code – which then is true for Siemens, Rockwell, Wonderware, General Electric, Emerson and other companies. An average industrial control system had already end of 2012, eleven direct connections to the Internet.

(Quelle und Bildmaterial: computerwoche 10/2015)

… search for yourself

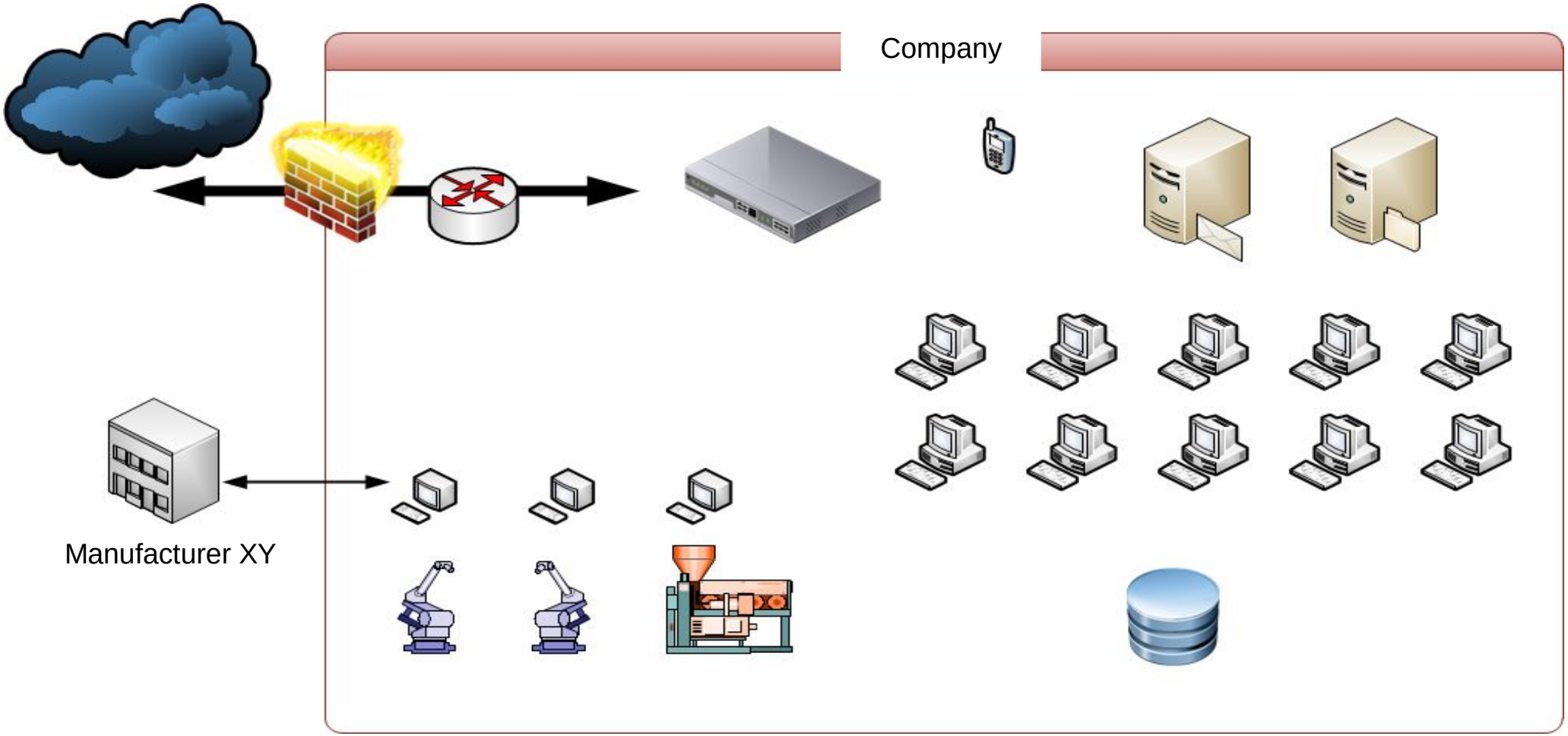


Of course: You can easily search with the new search engine Shodan for examples of unprotected industrial devices and systems worldwide !!!

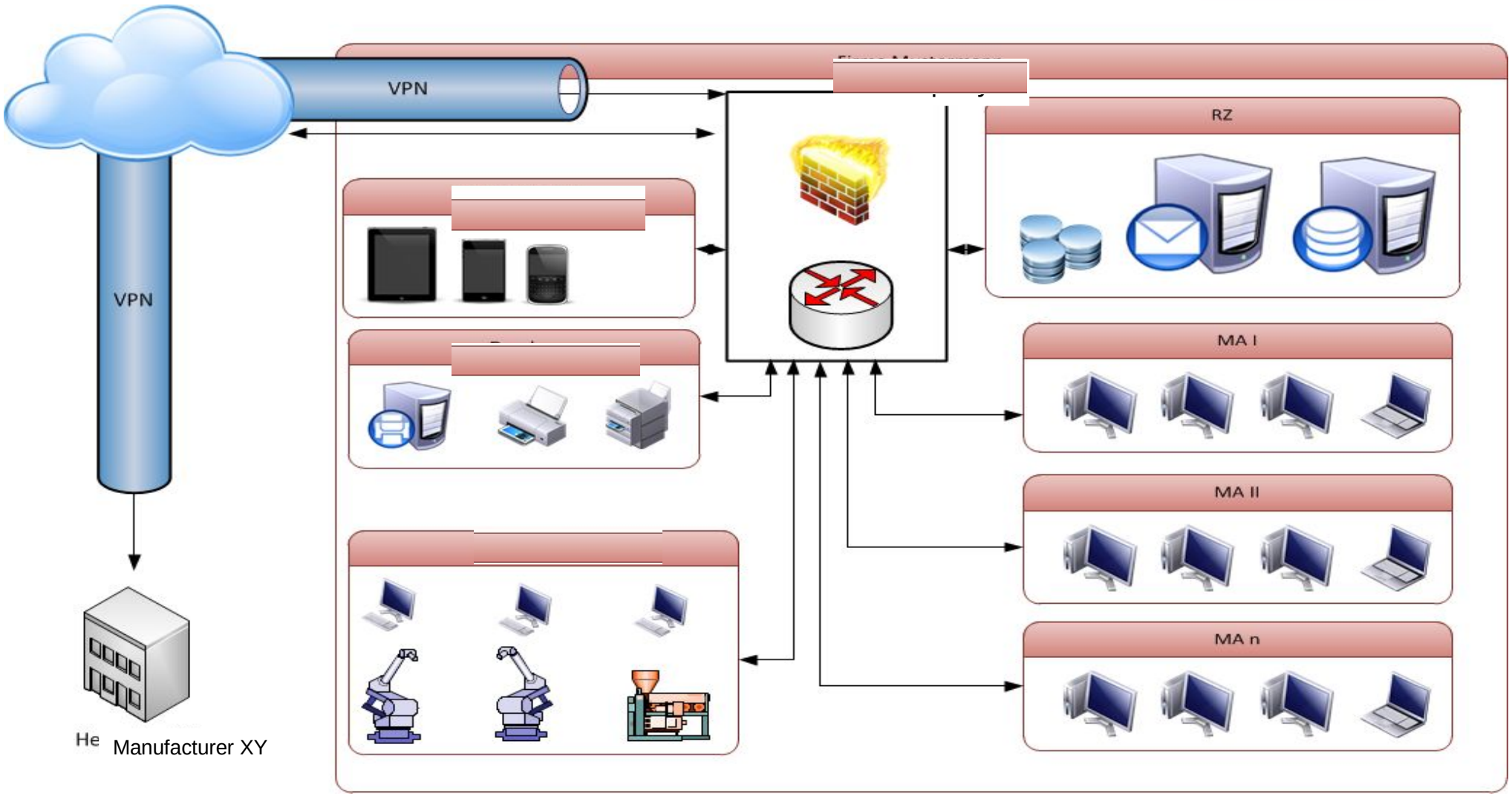
Concept of UTM / Firewall

- „Firewall”
- Immunization of different networks
  - Internet, Intranet, coupling networks
  - Different trust settings
  - Creating managed transitions
- Central components
  - Filtering of the data flow (rules)
- Interaction of hardware and software
  - Security Gateway Hardware or FW
  - Personal or Desktop FW

Planung – Ausgangszustand



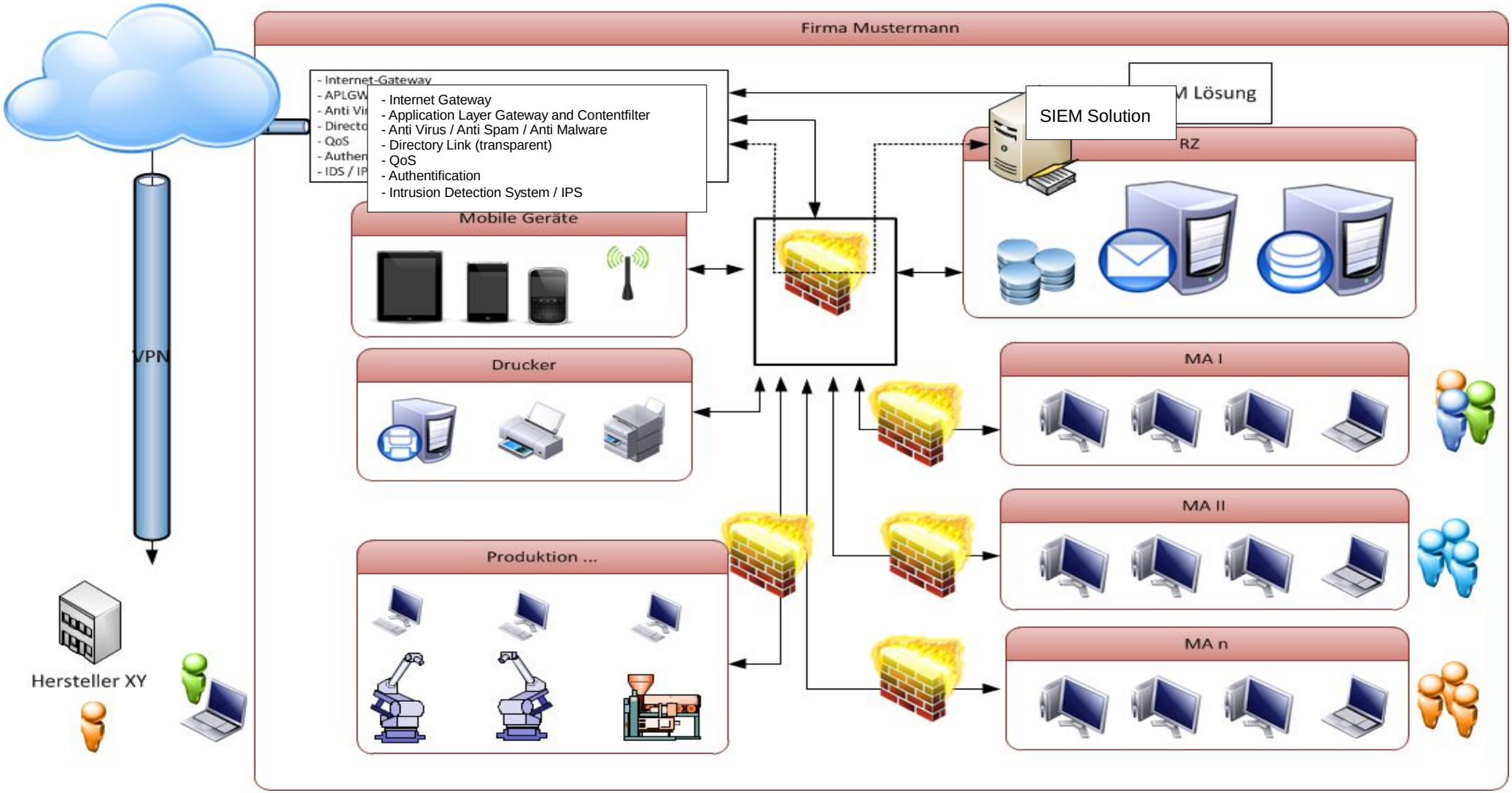
Design – first steps



Further Thoughts

- Which value has your data stock?
- What are the costs of a loss of data?
- Are the data or the know-how of others of interest for you?
- Who can do what in the "network" and why?
- Is your company and your data sufficiently safeguarded?

Design – final Execution



Typical Issues

- Loss of security through ignorance
- Lack of documentation
- Lack of training and / or instruction
- Technical limitations (especially SPI)
- Storage duration (timeout)
- Memory size (sessions)
- Structure and order of the rules
- Outdated firmware, known vulnerabilities
- No (native) attack detection

Professional Firewall

- Extensive rules
- Types: external-external, FW - external, external - FW
- Comments and documentation
- Timing and Timeslots
- Extensive Logging
- Selection of predefined services
- Grouping of IP addresses / Hazardous areas and hostname
- Intercepting misconfigurations
- SPOF (single point of failure) → high availability

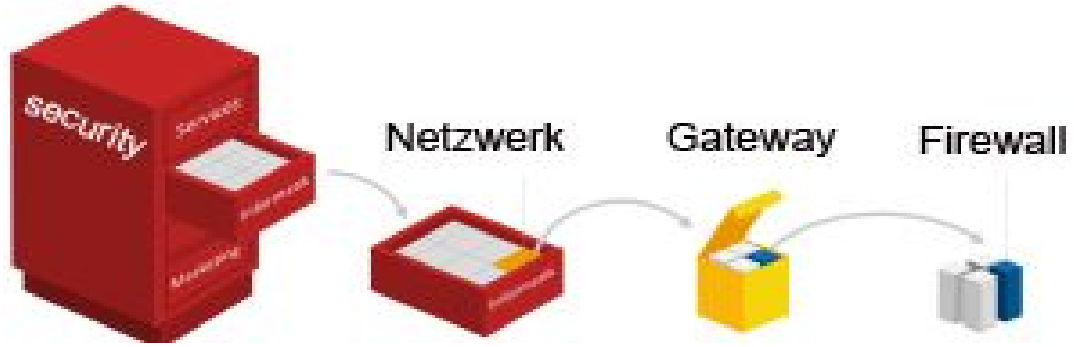
Attack Methodology

- Attackers with various motivations (Hacker, Cracker and Script Kiddies)
- Exploitation of errors in the operating system, in applications and services
- Penetration via "open" ports:
  - Mail and web servers
  - Network shares SMB / CIFS
  - Service Ports → TR-069
  - Discovery Protocols → UPnP
- Spoofing & Flooding (as DoS)
- Prevention: Penetration Test

DIN-Rail System

Summary

- Firewall is only ONE component
- Alone not sufficient to protect
- Create a concept with different zones
- Consider of the entire IT infrastructure
- Combine products of different manufacturers
- Don't use virtualized solutions where possible
- Aim for a statistical confidence ≠ absolute safety



TELCO TECH GmbH

… has been founded 1993

… Business location in Teltow and since June 2012 second location in Berlin

… developes and produces Security – Solutions under the registered tradename LiSS (LAN Internet Support Station)

… uses only german-based hardware components

Take time for

your IT security,

….otherwise your IT security

will steal your time!

LiSS Appliance bzw. UTM
(Unified Threat Management)

- Internet-Gateway (Router)
- Firewall
- IDS/IPS (Intrusion detection – and prevention))
- VPN-Gateway
- Web- und Mailfilter (Spam) with Antivirus
- Access to directory services (for example, Active Directory)
- Prioritization of services and bandwidth limitation
- Reporting (reports, minutes) Statistics
- Statistics
- Configuration protection

Firewalls

Contentfilter

VPN-Router

Appliances

Security Service

OEM Development

Danke für Ihre Aufmerksamkeit

TELCO TECH GmbH
NETWORK SECURITY

Bernd Schulz
Geschäftsführer

Telefon: +49 (30) 565862681
E-Mail: bschulz@telco-tech.de

Internet: https://www.telco-tech.de