What do we mean exactly with cyber security ?

It is time to secure your factory...

Why is it time to secure your factory ?

Industry 4.0 is about…

- ✓ Optimizing processes & productivity
- ✓ Developing services
- ✓ Seamless data flow
- ✓ Network convergence

…and this calls naturally for a secured network infrastructure

…in an industry perspective !

Why is it time to secure your factory ?

Industrial Control Systems like PLC‘s, HMI, SCADA and Drives with their reliance on proprietary networks and hardware, have long been considered immune to any kind of attacks from network or other interfaces.

But since these Control Systems are inter-connected together, connected to office networks and Internet, there is a new challenge :

Cyber Security !

“Would you imagine driving a car without safety belts on the streets today ?

Useless, uneasy, not so nice, we heard everything about them when they were introduced. Today, you wouldn’t feel safe on the road without them.

On today’s data highways, your traffic needs the same care for security : whether for support & maintenance, for data analytics, for production operations, your machines and your networks need protection.

So, because accidents happen, buckle up and drive your business safely…”

What do we mean exactly with Cyber Security :

- ✓ Security against what ? How am I affected ?
- ✓ What are the threats ? What should we do ?
- ✓ What is a firewall ? How does it work ?
- ✓ How about remote access and cyber security ?

Security against what ?

- Cyber crime :

  Offences committed to intentionally harm the reputation, to perpetrate financial theft, to gain unauthorized access to a computer in order to commit another crime (cracking, copyright infringement, threads,…)

- Cyber warfare :

  Actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption (bring down the power grid or paralyze the financial system)

- Cyber spying :

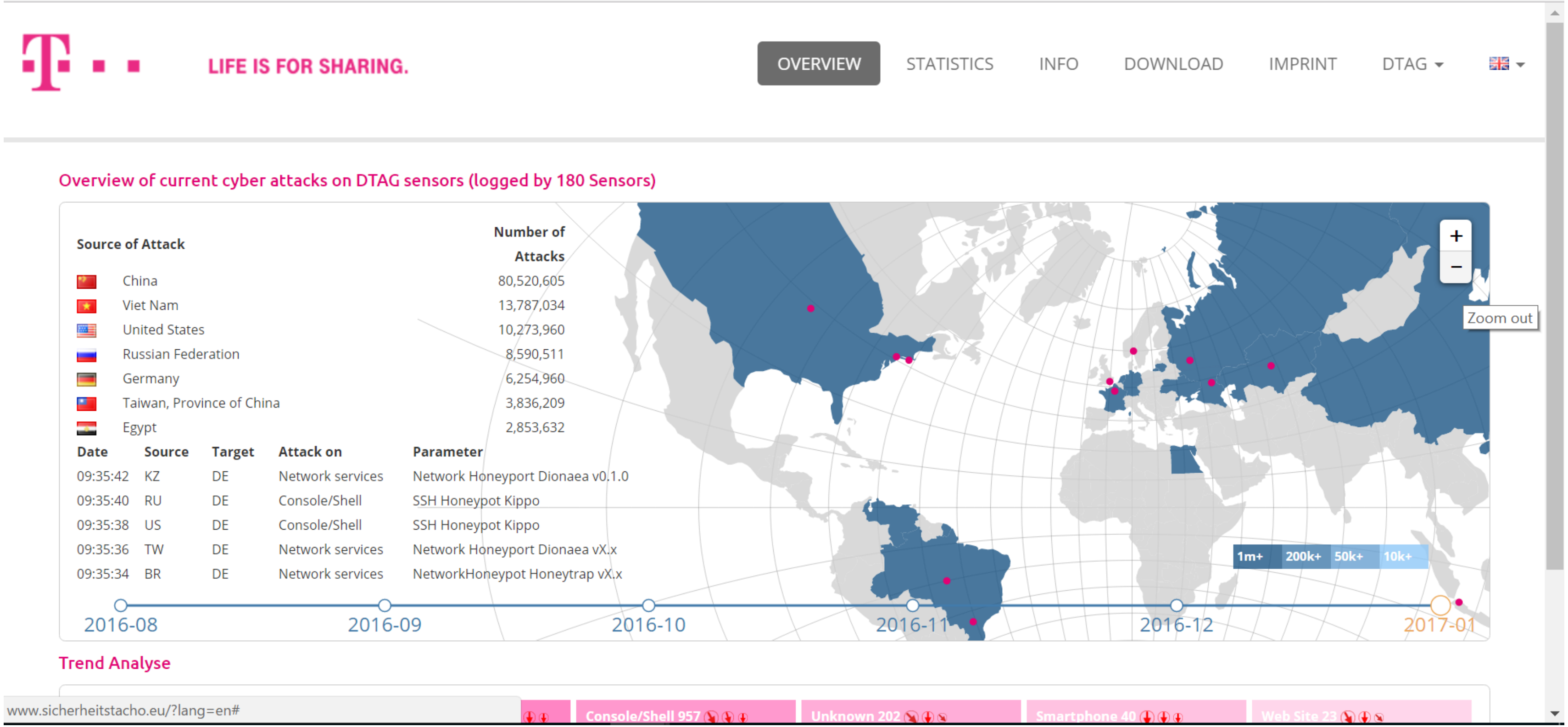
  The act of obtaining secrets or classified information from individuals, competitors or governments for economic, political or military advantage

How am I affected ?

Reality check :

- Time to have an overview : http://www.sicherheitstacho.eu/
- Time to see examples : http://www.shodanhq.com/

How am I affected ?



Overview of current cyber attacks on DTAG sensors (logged by 180 Sensors)

Source of Attack	Number of Attacks
China	80,520,605
Viet Nam	13,787,034
United States	10,273,960
Russian Federation	8,590,511
Germany	6,254,960
Taiwan, Province of China	3,836,209
Egypt	2,853,632

Date	Source	Target	Attack on	Parameter
09:35:42	KZ	DE	Network services	Network Honeyport Dionaea v0.1.0
09:35:40	RU	DE	Console/Shell	SSH Honeypot Kippo
09:35:38	US	DE	Console/Shell	SSH Honeypot Kippo
09:35:36	TW	DE	Network services	Network Honeypoort Dionaea vX.x
09:35:34	BR	DE	Network services	NetworkHoneypot Honeytrap vX.x

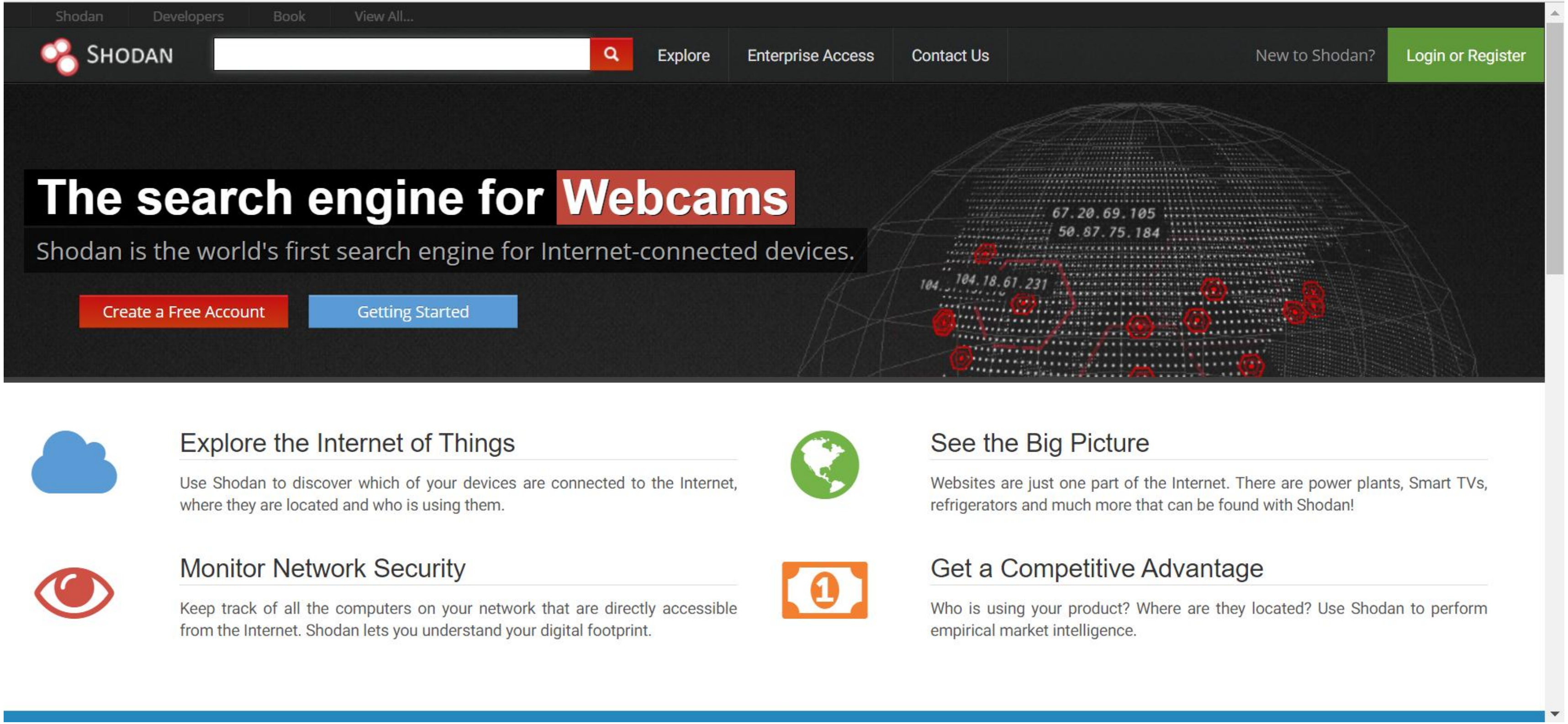
2016-08 2016-09 2016-10 2016-11 2016-12 2017-01

Trend Analyse

Console/Shell 957 | Unknown 202 | Smartphone 40 | Web Site 23

www.sicherheitstacho.eu/?lang=en#

How am I affected ?



The search engine for Webcams

Shodan is the world's first search engine for Internet-connected devices.

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

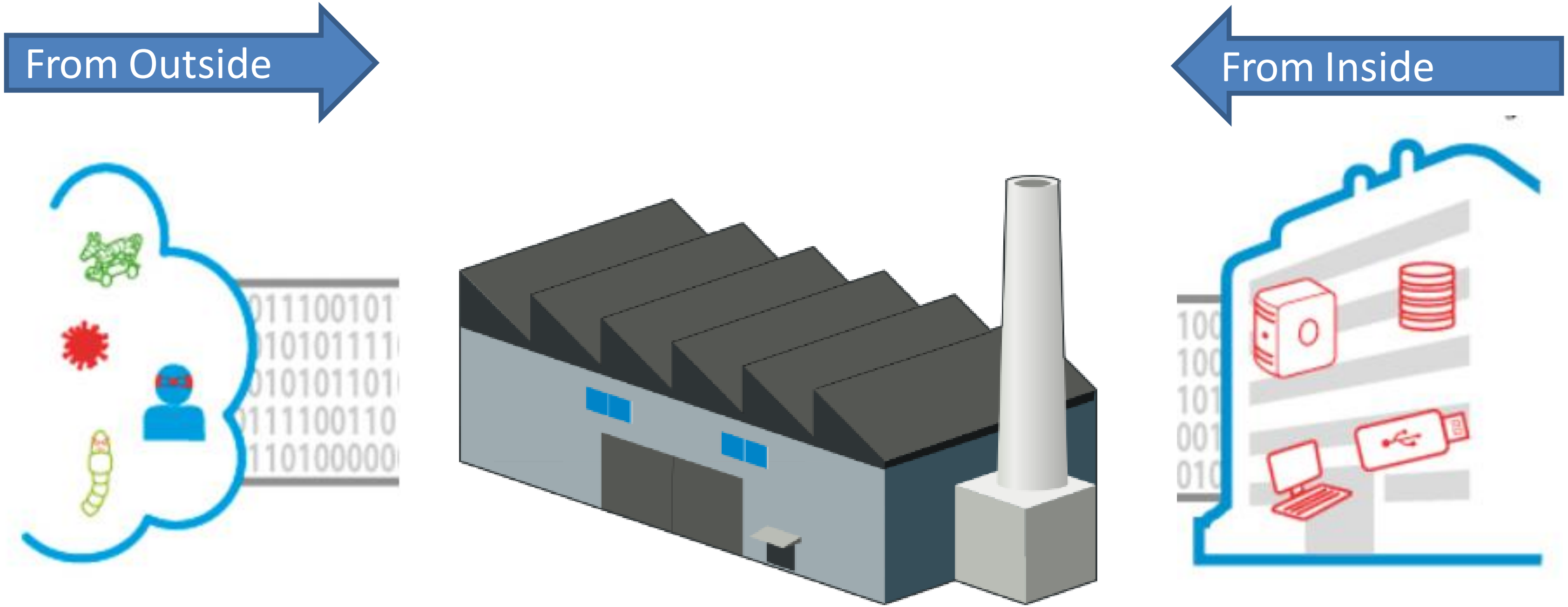
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

Governments react to the threat on industrial assets

National agencies :

- USA : Department of Homeland Security
  http://www.dhs.gov/topic/cybersecurity
- France : Agence Nationale pour la Sécurité des Systèmes d’Information
  http://www.ssi.gouv.fr/
- Germany : Bundesamt für der Sicherheit in der Informationstechnik
  http://www.bsi.bund.de/
- Europe : European Union Agency for Network and Information Security
  https://www.enisa.europa.eu/

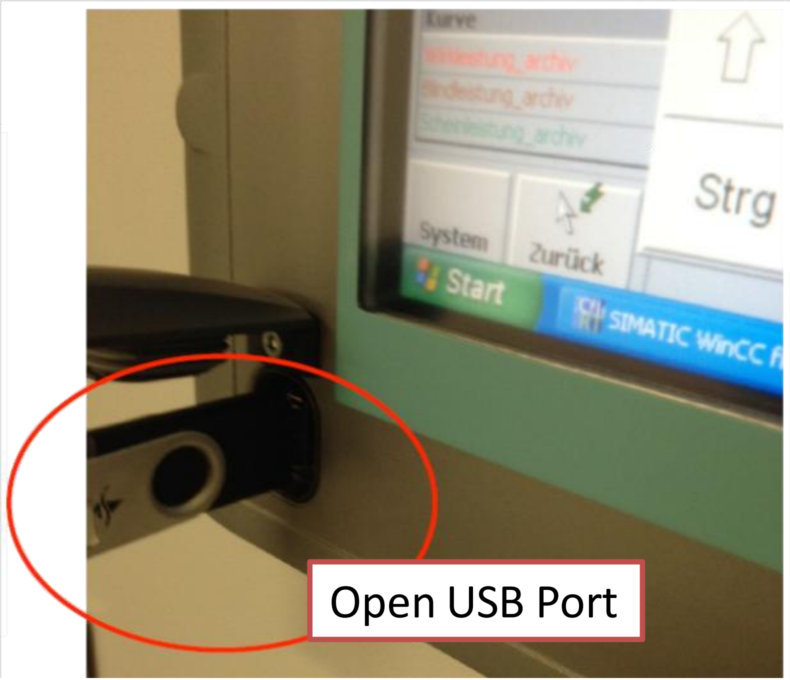
Where is the threat coming from ?



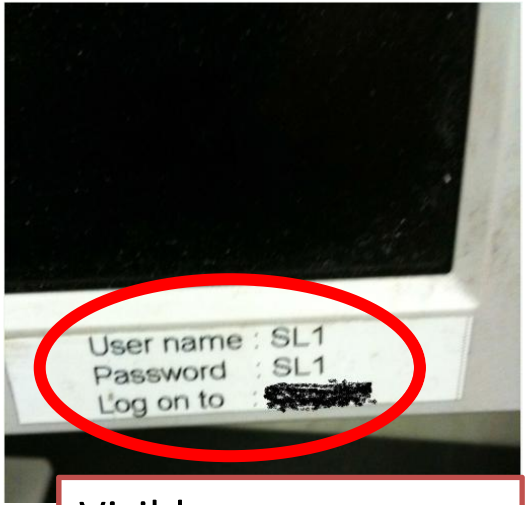
From Outside

From Inside

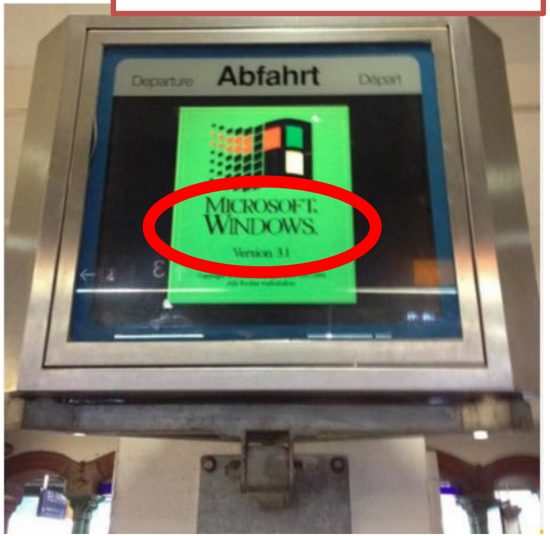
The vulnerabilities from inside...



Open USB Port



Visible server name & login credentials



Old & unsecured Operating Systems

What can we do ?

Technical Measures :

Restricted access, encryption, backups, network segmentation

Organizational Measures :

Control user access, set procedures, raise awareness

Surveillance Measures :

Install tools to detect viruses, changes, manipulations

Two worlds, big differences

Business Network

1.) Confidentiality
2.) Integrity
3.) Availability

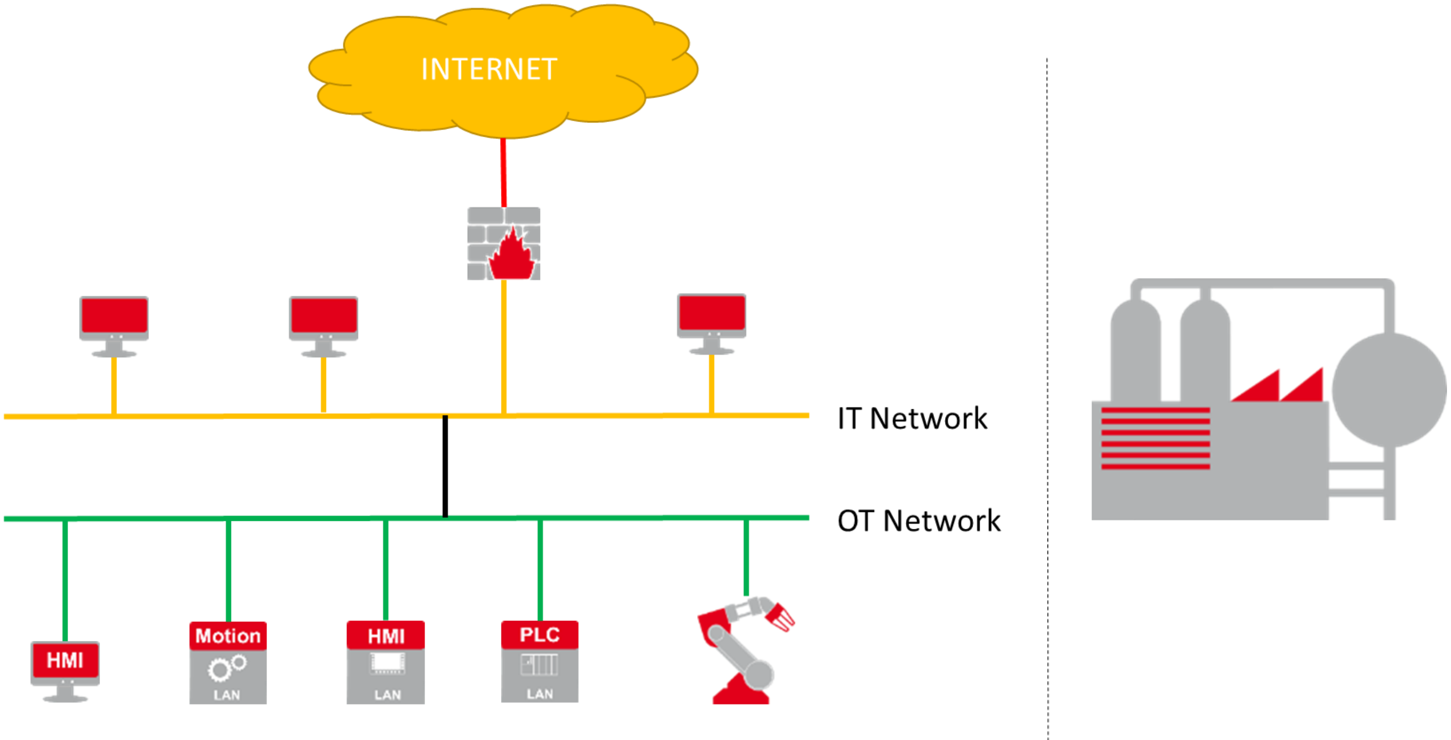
Production Network

1.) Availability
2.) Integrity
3.) Confidentiality

Two worlds, big differences

	Business IT	Industrial IT
Latency	Limited relevance	Highly critical
Patch Management	Often, up to daily	Rarely, needs often additional approval from 3rd party vendor
Management	Centralized	Often standalone
Life time	3 – 5 years	5-20 years (unsupported OS like NT and older)
System changes	Often	Rarely
Availability	Reboot is acceptable	24x7x365
Virusprotection	Standard	Complex, often not possible
Awareness	Good	Poor
Vulnerability checks	Standard	Rarely and complex (availability)
Outsourcing	Usually	Rarely
Physically Security	Safeguarded and closed areas	Unmanned and white areas

A typical factory network…

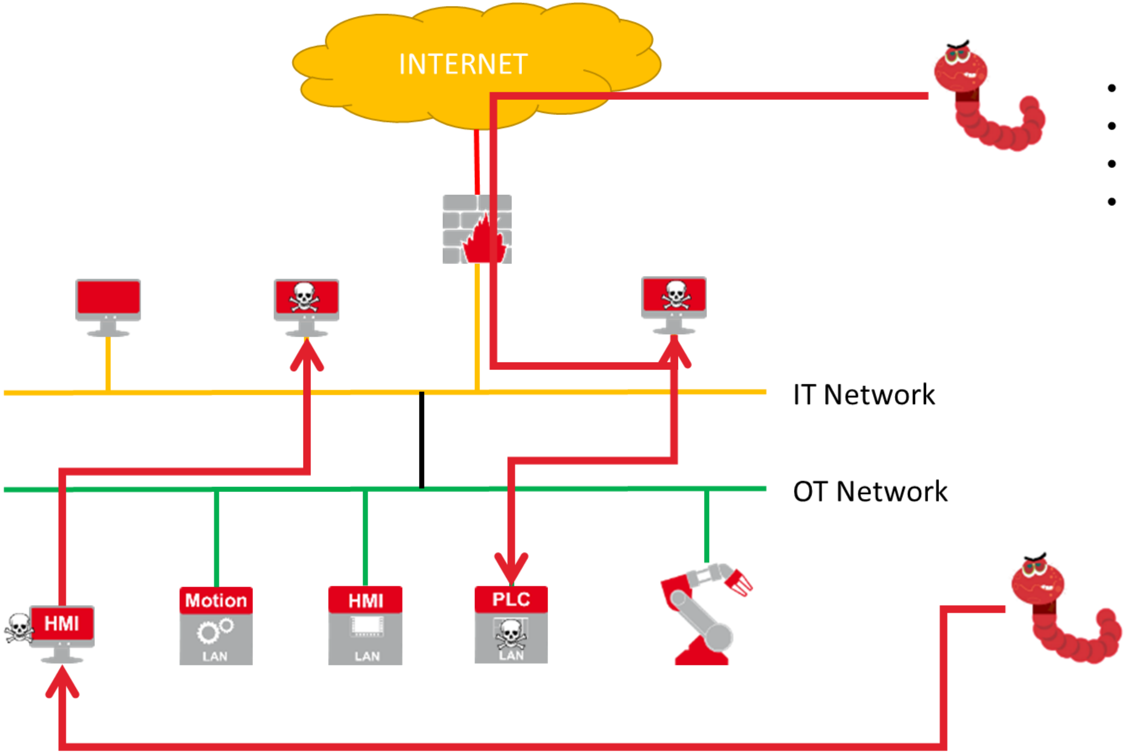


INTERNET

IT Network

OT Network

A typical factory network... under attack



- Spear Phishing
- Remote Access
- Firewall configuration
- ....

- Unsupported Operating System
- USB memory with virus
- Virus on PC
- ....

What do we mean exactly with Cyber Security :

- ✓ ~~Security against what ? How am I affected ?~~
- ✓ ~~What are the threats ? What should we do ?~~
- ✓ What is a firewall ? How does it work ?
- ✓ How about remote access and cyber security ?

A firewall : how does it work ?

Incoming protocols :

- Phone
- Post
- Courrier
- Visitors

Firewall

Destination processes :

- R&D
- Finance
- Production
- QA
- Support
- Service
- Marketing
- Sales

A firewall : how does it work ?

Incoming protocols :

- Phone
- Post
- Courrier
- Visitors

Firewall

Destination processes :

- R&D
- Finance
- Production
- QA
- Support
- Service
- Marketing
- Sales

A firewall : how does it work ?

Incoming protocols :

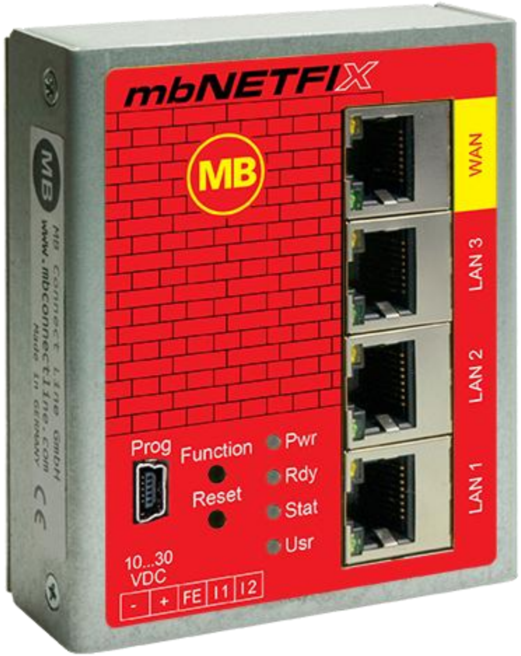
- Phone
- Post
- Courrier
- Visitors

Firewall

Destination processes :

-
-
-
-
-
-
- Marketing
- Sales

How does an automation firewall look like ?



A WAN port connects to the "unsafe" network

LAN ports connects to the "protected" network

Remote access routers may also embed firewall capabilities…

There are 3 networks connected to a remote access router : WAN, VPN and LAN

VPN to LAN : all traffic is allowed, user access is controlled from the server

LAN to VPN : all traffic is blocked by the firewall (except in M2M groups)

WAN to LAN : traffic can be controlled through firewall settings

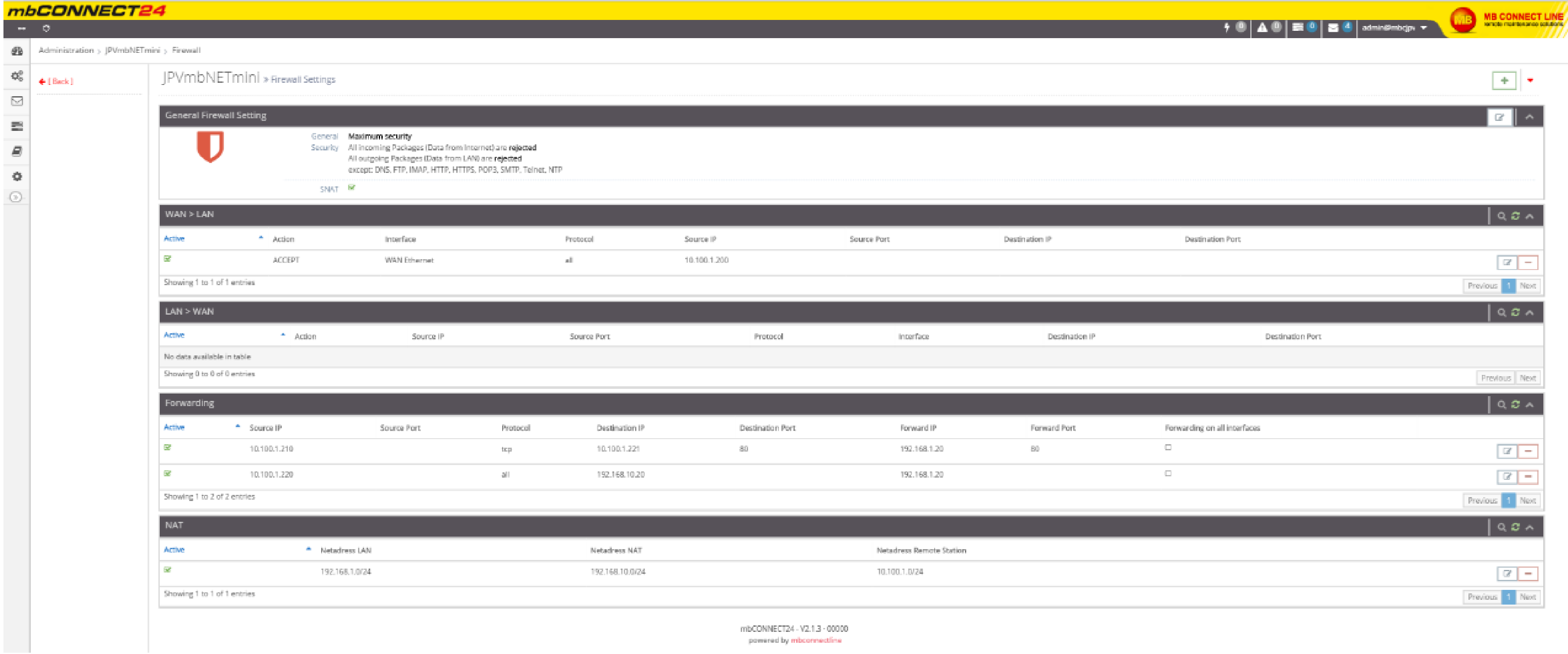
LAN to WAN : traffic can be controlled through firewall settings

WAN to VPN : all traffic is blocked by the firewall

VPN to WAN : all traffic is blocked by the firewall

mbNET is thus also used as a firewall to control WAN network access to the machine

Controlling traffic with the firewall



Administration › JPVmbNETmini › Firewall

JPVmbNETmini » Firewall Settings

General Firewall Setting

General Security: Maximum security
All incoming Packages (Data from Internet) are rejected
All outgoing Packages (Data from LAN) are rejected
except: DNS, FTP, IMAP, HTTP, HTTPS, POP3, SMTP, Telnet, NTP

SNAT ☑

WAN > LAN

Active	Action	Interface	Protocol	Source IP	Source Port	Destination IP	Destination Port
☑	ACCEPT	WAN Ethernet	all	10.100.1.200			

Showing 1 to 1 of 1 entries

LAN > WAN

Active	Action	Source IP	Source Port	Protocol	Interface	Destination IP	Destination Port
No data available in table							

Showing 0 to 0 of 0 entries

Forwarding

Active	Source IP	Source Port	Protocol	Destination IP	Destination Port	Forward IP	Forward Port	Forwarding on all interfaces
☑	10.100.1.210		tcp	10.100.1.221	80	192.168.1.20	80	☐
☑	10.100.1.220		all	192.168.10.20		192.168.1.20		☐

Showing 1 to 2 of 2 entries

NAT

Active	Netadress LAN	Netadress NAT	Netadress Remote Station
☑	192.168.1.0/24	192.168.10.0/24	10.100.1.0/24

Showing 1 to 1 of 1 entries

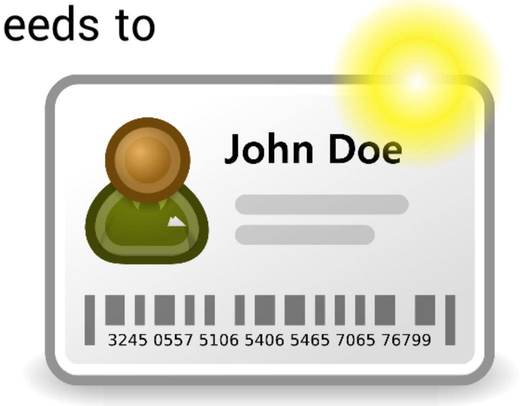
mbCONNECT24 - V2.1.3 - 00000
powered by mbconnectline

How about remote access and cyber security ?

There was a time when the technician from your machine supplier could walk in and out freely in the company…

Today, he is still very welcome at your site, yet, he now needs to

- ✓ register at reception,
- ✓ badge in & out,
- ✓ notify a supervisor of his presence,
- ✓ get approval for any intervention and
- ✓ report when done.



A quite natural course of action today indeed and you keep in control.

How about remote access and cyber security ?

Today…

How many machines do you have on your factory foor ?

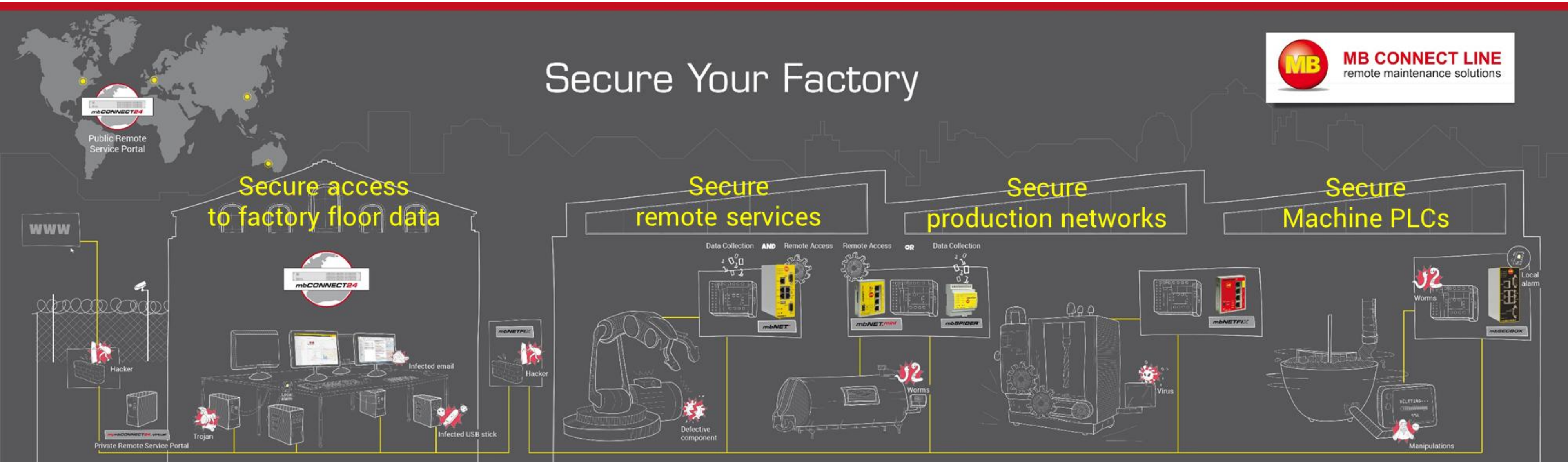
How many of them are "connected" ?

How many of them are equipped for remote support & maintenance ?

Those supplier's remote services are quite valuable for your production…

Yet, wouldn't it be time to make production optimization and common security guidelines meet, …just like anywhere else ?

This is what we mean with cyber security…



Secure Your Factory

Secure access to factory floor data

Secure remote services

Secure production networks

Secure Machine PLCs

4S INDUSTRIE
Industrial Internet of Things

MB CONNECT LINE
remote maintenance solutions

Your next MB Connect Line solution is a close as can be...

✉ info@4Sindustrie.nl

sales@mbconnectline.com

☎ www.4sindustrie.nl

055 542 4228

Let's talk about your project !