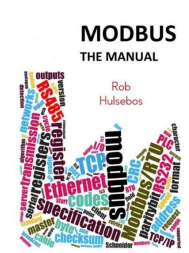
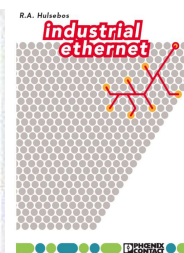
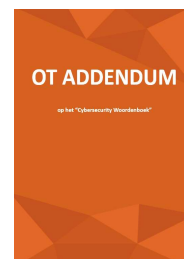


CYBERSECURITY CHALLENGES IN OT



WHO AM I

- Rob Hulsebos, 1961
- 30 years experience industrial networks as sw engineer, end-user, vendor, troubleshooter, teacher
- Working at Philips, ASML, Kulicke & Soffa, Delem, SecurityMatters / **Forescout (Eindhoven)**
- Freelance journalist
- Author
 - Various books on industrial networking and cybersecurity



WHAT IS OT ?

(FORMERLY KNOWN AS: SCADA)

3

WHAT IS "OT" ?

- OT = **Operations Technology**
IT = **Information Technology**
- Monitoring and control of industrial equipment
(the exact definition of what "industrial" is may vary)
- Two different worlds!




OT





IT



4



OT IS EVERYWHERE (BUT INVISIBLE)

In the morning, when you wake up and turn on , it works because of OT

You take a , water supply thanks to OT  gas supply

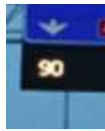


Sewage  done via OT, electrical network infrastructure too 

Car made in factory  fuel from refinery  all made with OT

Traffic light control,  highway management, bridge control 

Etc....



And this shows: OT is there in the first hour of your day! (23 to go)

AND THEN: OT IN THE OFFICE

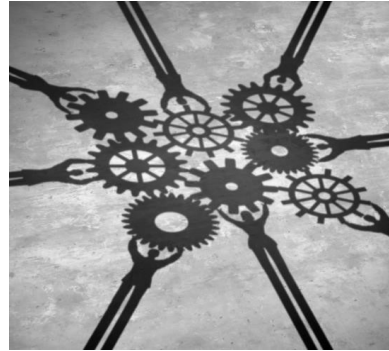


- Advanced Metering Infrastructure
- Building Automation System
- Building Management Control System
- CCTV Surveillance System
- CO2 Monitoring
- Digital Signage Systems
- Electronic Security System
- Emergency Management System
- Energy Management System
- Exterior Lighting Control Systems
- Fire Alarm System
- Fire Sprinkler System
- Interior Lighting Control System
- Intrusion Detection Systems
- Physical Access Control System
- Public Safety/Land Mobile Radios
- Renewable Energy Geothermal Systems
- Renewable Energy Photo Voltaic Systems
- Shade Control System
- Smoke and Purge Systems
- Vertical Transport System (Elevators and Escalators)

6

THREATS FOR OT

- Systems originally designed to run standalone (and hacking didn't exist at the time)
- Now connected to rest of company, and company itself connected to Internet
- Old OT protocols designed without authentication / encryption
- Owners often have no idea about what equipment is on their network
- Systems open to internet ("so easy for our vendors", "work from home")
- Long life-span 20+ years, still in use



7

A FEW OT HACKS

8

THE VERY FIRST OT HACK: MAROOCHY

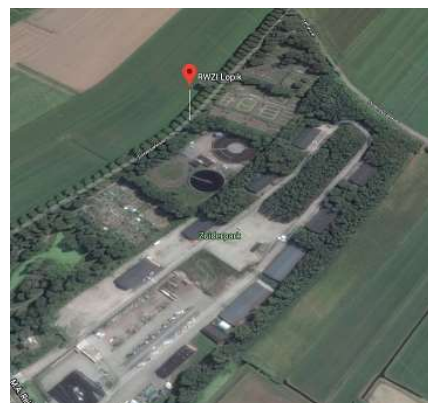
- What happened:
 - Maroochy (Australia) sewage processing
 - Conflict with employee, is fired
 - Follow strange disturbances, flow of million litres of sewage in all places in the city multiple times
- Root cause: unprotected wireless network, allowed access to pumps and valves from outside control network
- Starting point for industrial cybersecurity



9

MAROOCHY IN NL: LOPIK

- Almost identical “Maroochy” hack here in NL
- What happened ?
 - Lopik, 2016
 - Manager sewer systems: job conflict, got fired
 - Months later: strange problems with pumps, valves opened & closed (but no damage inflicted)
 - 8000 files removed
 - System three days inoperable
- How did it happen ?
 - IT accounts were blocked, OT accounts not (were unknown to department)



10

STUXNET

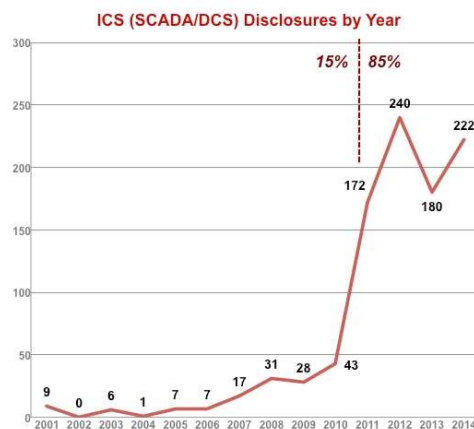
- The hack that started OT cyber for real
- What happened:
 - Iran, uranium enrichment factory, 2010
 - Special malware for Siemens PLC's (first industrial malware ever!)
 - Disrupted control of ultracentrifuges (without Iran having a clue), ~ 30% destroyed
- Stuxnet escaped from the factory and went around the world (reportedly even in the ISS) so we found out



11

AFTER STUXNET

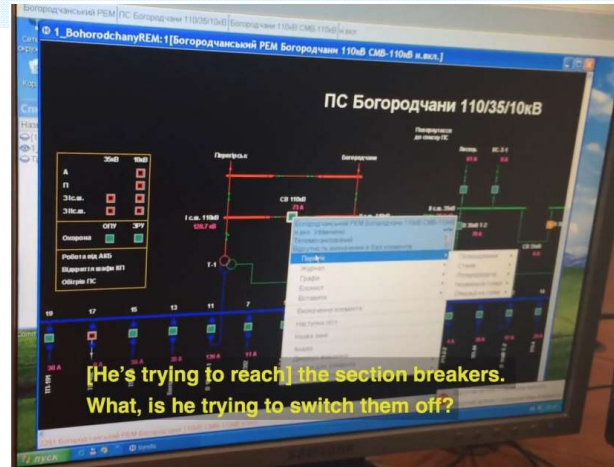
- After Stuxnet the interest in OT vulnerabilities exploded
- Interest from hackers because:
 - Easy to find
 - Old software
 - Easy to hack
 - Little interest from suppliers
- Interest from countries as well:
 - Attack enemy infrastructure without being attributable (see next page)



12

INDUSTROYER

- Cyberattack on Ukraine
- What happened:
 - Kiev, December 2015, power loss
 - Malware took over operator stations and switched off 30 substations
 - Windows registry on PC's erased
 - Firmware erased
- Operators reacted quickly
 - Put plant on “manual” control
 - It was an old power plant
- Who did it? Your guess...



Actual moment photographed by an operator at a workstation when he realized he lost the view and control of a power grid during a cyber-attack on a regional power utility in Ukraine on December 23, 2015. For a while he thought the IT department was playing a funny trick on him as he watched how the mouse moved by itself and clicked open the breakers at 30 substations under his control and in front of his eyes. The investigation after the attack revealed that the system was penetrated and compromised months before the actual attack.

TRITON / TRISYS

- Hack of controller in oil refinery
- What happened:
 - Saudi-Arabia, 2017
 - Bug in firmware of triple-redundant Schneider “Triconex” controller
 - Hacker tries to install malware
 - Due to user error (switch wrong setting, see picture) this was allowed
 - Because of bug in malware, it was detected, and controller shut down refinery (to make it “safe”)
- Who did it? Your guess...



JUST AFTER STUXNET: ALARM IN NL

Sluizen slecht beveiligd



De sluizen in de gemeente Veere zijn slecht beveiligd
drhenkenstein / Flickr / Creative Commons 2.0 by-nc-sa

Toegevoegd: dinsdag 14 feb 2012, 17:46

Het is slecht gesteld met de digitale beveiliging van sluizen, bruggen en gemalen. Beveiligingsexperts luiden in het tv-programma [EenVandaag](#) de noodklok.

Volgens de experts is het kinderlijk eenvoudig voor hackers om de sluizen thuis via internet te bedienen. In sommige gevallen is het wachtwoord gemakkelijk te

kraken, in andere gevallen is er helemaal geen wachtwoord nodig om de systemen binnen te dringen.

De rioleringspompen en gemalen van de gemeente Veere zijn gemakkelijk van een afstand te bedienen, zo blijkt uit de uitzending. Volgens de experts ligt dat aan het SCADA-systeem dat wordt gebruikt. Het zou veel te kwetsbaar zijn.

INTERNET CONNECTED "SCADA"

- NOS didn't dare to touch systems in Zeeland
- So sought other 'victim'
- Shutdown the central heating of NL office of Salvation Army
- How: via internet access to their building mgmt

Last week... o yes, it was so cold here...



IT VULNERABILITY COULD AFFECT OT

- A hack in IT can also become a problem for OT
- Examples:
 - Drinking water system Florida via RDP take over control of addition of dangerous chemicals to water
 - Colonial Pipeline US east coast (ransomware after leaked password) Deliveries stopped because financial accounting no longer possible
- IT and OT are intertwined !

Report: Oldsmar water hack came after city computer visited compromised website

Investigation finds watering-hole attack discovered targeting water utilities



The Colonial Pipeline Crisis Is a Taste of Things to Come

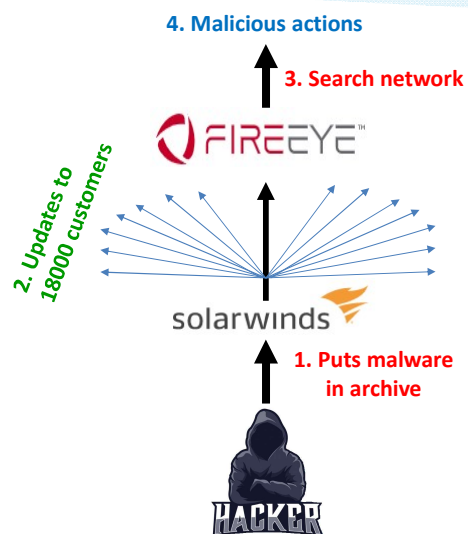
Biden must act now to protect the energy system from the rising threat of cyberattacks and natural disasters.



17

SOLARWINDS HACK

- Supply chain attack
 - Modification of source code
 - Malware comes with updates
- Detected after 8 months (...)
- Inside FireEye network
- 18000 customers in danger
- Also huge usage in OT products



18

WHAT IS DIFFERENT IN OT ?

19

SOME TECHNICAL DIFFERENCES IT / OT

- Newer Windows versions
- TCP/IP and family
- Managed switches
- Dynamic addressing (DHCP)
- Shutdown one PC not fatal
- Virus scanner (or similar)
- Patching regularly
- Multi-factor authentication
- Account lockout after many tries
- Higher cyber awareness
- *Many more...*
- Still Windows NT, XP, ...
- Hundreds of dedicated protocols
- Unmanaged switches (at lower layers)
- Static IP addressing
- Everything *must* work to produce
- Virus scanner not possible or unwanted
- Patching irregularly or not at all
- MFA often impossible
- Account lockout not allowed
- Production goes 1st, 2nd, 3rd. Cyber later.
- *Many more...*

20

DIFFERENT TECHNOLOGY: LOTS OF DEDICATED OTHER PROTOCOLS

IT protocols	Standard OT protocols	Proprietary OT systems/ protocols
<ul style="list-style-type: none"> • AFP • BGP • DHCP • DNS • FTP • HTTP • IMAP • Kerberos • LDAP • LDP • MS-SQL • NTP • NetBIOS • OpenRDA • POP3 • PVSS • Radius • RDP • RFB/VNC • RPC/DCOM • RTSP • SMB / CIFS 	<ul style="list-style-type: none"> • BACnet • DNP3 • EtherCAT • EtherNet/IP + CIP • Foundation Fieldbus HSE • IEC 60870-5-101/104 • IEC 61850 (MMS, GOOSE, SV) • IEC 61850 (MMS, GOOSE, SV) • IEEE C37.118 (Synchrophasor) • Modbus ASCII • Modbus RTU • Modbus/TCP • OPC-DA • OPC-AE • PROFINET (RPC, RTC, RTA, DCP and PTCP) 	<ul style="list-style-type: none"> • CSLib (ABB 800xA) • DMS (ABB AC 800 F) • MMS (ABB AC 800 M) • PN800 (ABB Harmony) • SPLUS (ABB Symphony Plus) • ADS/AMS (Beckhoff) • CygNet SCADA (CygNet) • DeltaV (Emerson) • Ovation (Emerson) • SRTP (GE) • Experion (Honeywell) • ADE (Phoenix Contact) • CIP extensions (Rockwell/AB) • CSP (Rockwell/AB) • COMEX (Schneider Electric Foxboro) • OASyS (Schneider Electric) • Modbus/TCP Unity (Schneider Electric) • Telnet extensions (SEL) • Step7 (Siemens) • S7COMM+/OMS+ (Siemens) • Vnet/IP (Yokogawa)

1000's more...

21

OTHER PROTOCOLS

- Often derived from 80's/90's serial protocols (ported as-is to UDP or TCP)
 - Developed in age where cyber didn't exist
 - Internet didn't exist
 - No authentication needed (or very simple)
 - Complete control over device
 - Important for vendor, cannot easily be migrated
- Migration to Ethernet
 - Older networks connected via "serial converters"
 - Suddenly accessible from outside



22

IT / OT MISUNDERSTANDINGS / CONFLICTS

- OT department
 - Thinks that IT department takes care of OT cybersecurity
- IT department
 - No knowledge of OT, so leaves OT wishes to the OT department
 - Little enthusiasm to work with “Old Technology” (*Oude Troep*) stuff
- OT Staff
 - “It may be forbidden, but production must continue, so I do it anyway” (i.e. USB usage)



23

PATCHING ? PLEASE COME BACK NEXT YEAR

- Production usually cannot be stopped, so ...
 - Many sites never patch
 - Others only once per year
 - Big backlog
- Never automatic (due to reboot)
 - Only during planned production stop
- Problems when patch goes wrong
- Devices in use for 10..20 years or more
 - Vendors have since long stopped support
- Seen a vendor advise to customers: “Patching introduces more downtime than hackers, so don’t”



24

ACTIVE SCANNING FOR OPEN PORTS ?

- Long considered *big* risk in OT
 - Broadcasts affect everyone
 - Crashing devices
 - Disconnected devices
 - Influence on behaviour
 - Disturbance of control cycle
- Is changing
 - More mature protocol stacks
 - Engineering tools use scanning too
 - Different purpose: scan gives more detailed information and quickly (for asset info)



25

WHY CAN'T I JUST BUY A <insert favourite brand> FIREWALL?

- Firewalls:
 - If only they could recognize OT protocols! (DPI)
 - Must adhere to real-time constraints
 - Must be careful with blocking traffic!
- Dedicated OT firewalls *do* exist (scarce)
 - Like "Tofino" (doesn't require firewall guru's to configure)
 - Like "Palo-Alto 220R"
 - OT specific: temperature range, double 24V power supply, fastened connectors, vibration tolerance, no ventilators, etc.



26

RANSOMWARE IS THE MODERN PLAGUE

- Often coincidental
- But: “Conti” hackers group leaked forum shows their interest in OT because “It is easier to breach”

Cyberaanval legde Apollo Vredestein tijdelijk plat – Malware bereikt steeds vaker OT-systemen



Eind juli legde een cyberaanval de bandenfabrikant Apollo Vredestein tijdelijk plat. Door een hack bij het Indiase moederbedrijf Apollo Tyres werden de fabrieken wereldwijd getroffen. Malware besmette de systemen waardoor productie ook in Nederland tijdelijk niet mogelijk was. De oorzaak, zo tekent het FD op, is verouderde software op gebruikte apparatuur die al meer dan tien jaar niet was bijgewerkt. De bandenfabrikant heeft echter niet bevestigd dat de hackers op deze manier zijn binnengekomen. Inmiddels zijn de processen bij Apollo Vredestein geleidelijk weer opgestart.

NOS Nieuws • Vrijdag 22 oktober 2021, 14:50 •
Aangepast vrijdag 22 oktober 2021, 15:48

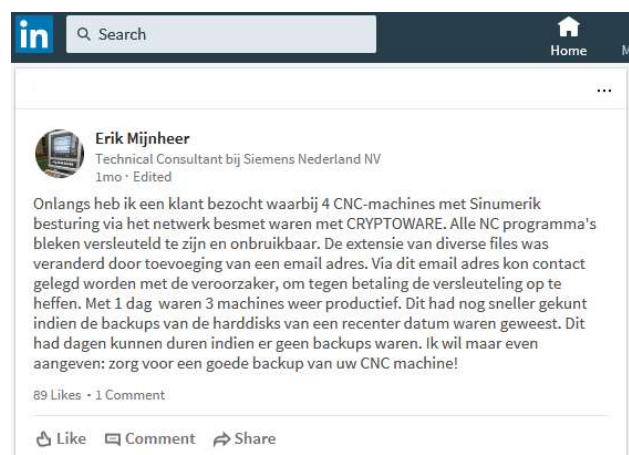
Problemen na hack bij VDL nog niet opgelost, merken ook klanten

De problemen bij industrieconcern VDL Groep zijn nog niet voorbij. [Begin deze maand](#) werd het concern geraakt door een digitale aanval. Alle 105 bedrijven die onder het concern vallen, ook in Azië en Amerika, werden erdoor geraakt.

27

WINDOWS WHERE YOU NOT EXPECT IT

- Even though ransomware is not made for OT, there is still a lot of “Windows” to be found
 - Operator terminals / screen (“HMI”)
 - Embedded controller (WinCE)
 - ...
- Sometimes completely unknown to the users of these devices



28

PROGRESS ?

29

PROGRESS

- There is a 'live' standard IEC-62443 specially for OT
- Many vendors / users treat OT cyber seriously (but could go faster)
- Dedicated OT cyber solution providers (i.e. Forescout, Nozomi, Claroty, Dragos)
- OT cybersecurity companies (i.e. in NL: Hudson Cybertec/DNV, Applied Risk/KIWA)
- Government attention (NL, EU, US) (i.e. NIS2 directive 2024, consumer products)
- NL's largest OT-specific cyber conference (for end-users, not for hackers)
fhi.nl/industrialcybersecurity/
- There's money to be made in OT (suddenly many find themselves OT expert)

30

WHAT CAN YOU DO AS OT OWNER ?

- Train staff (awareness)
- Predictive cybersecurity, not event driven
- Find out what you have (devices)
 - Not uncommon to see 50% is unknown
- Segment, patch, log and backup (and: defend the backups)
- OT Cyber event training →
- No need to reinvent the wheel, some tips:
 - **BIACS** (NL) for beginners
 - **CSIR 3.4** (Cybersecurity Implementatie Richtlijn)
 - **IEC-62443**



Cybergym

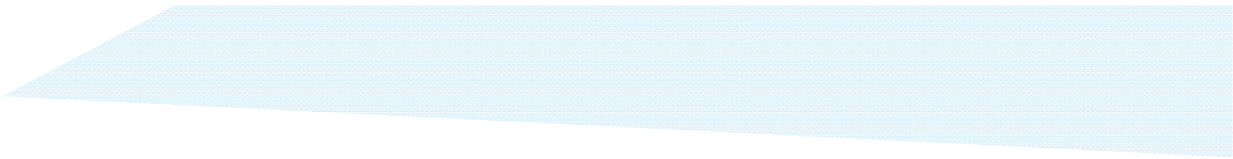
31

WHAT CAN YOU DO AS A PROGRAMMER ?

- PLC programmers can do their part too: program defensively
- Initiative started after talk at “S4” OT cyber conference in Miami
- “Top 20 Secure PLC programming guidelines”

plc-security.com

32



THANK YOU

rh@enodenetworks.com