Cyberveiligheid in de industrie

howest
university of applied sciences

Wie ben ik?

Security Researcher
& Educator
Laurens Singier

Laurens.singier@howest.be

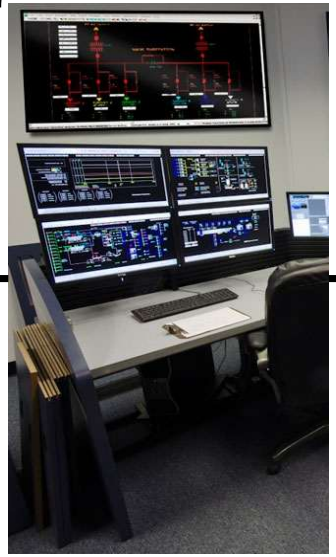
Wat is OT/ICS

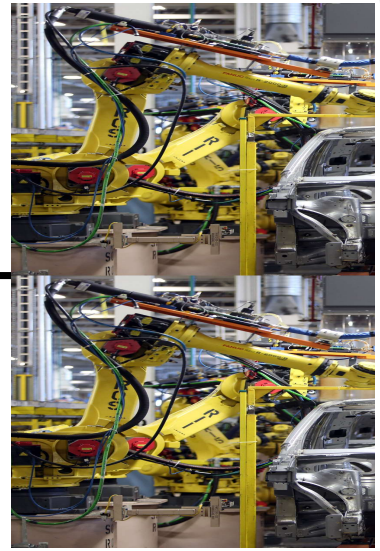
howest
university of applied sciences

Wat is OT?

Office

Industrial Control Systems

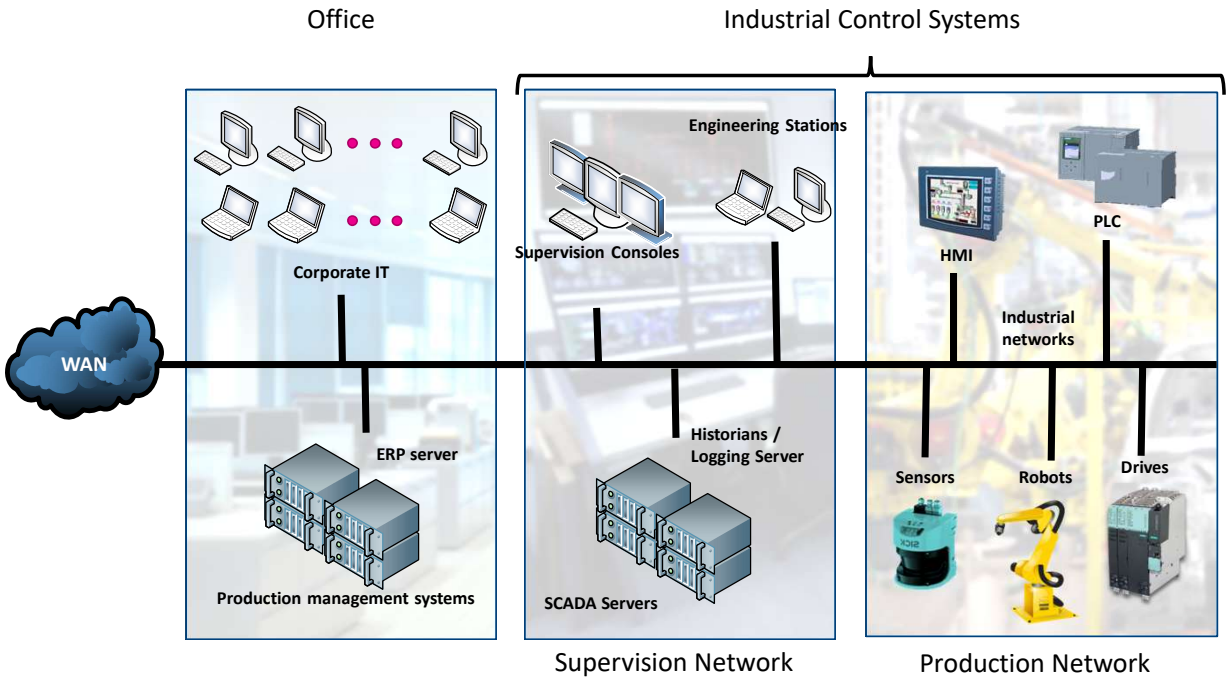




Supervision Network

Production Network

Wat is OT?



Corporate IS handle data
≠
ICS handle interfaces data with physical world

howest
university of applied sciences

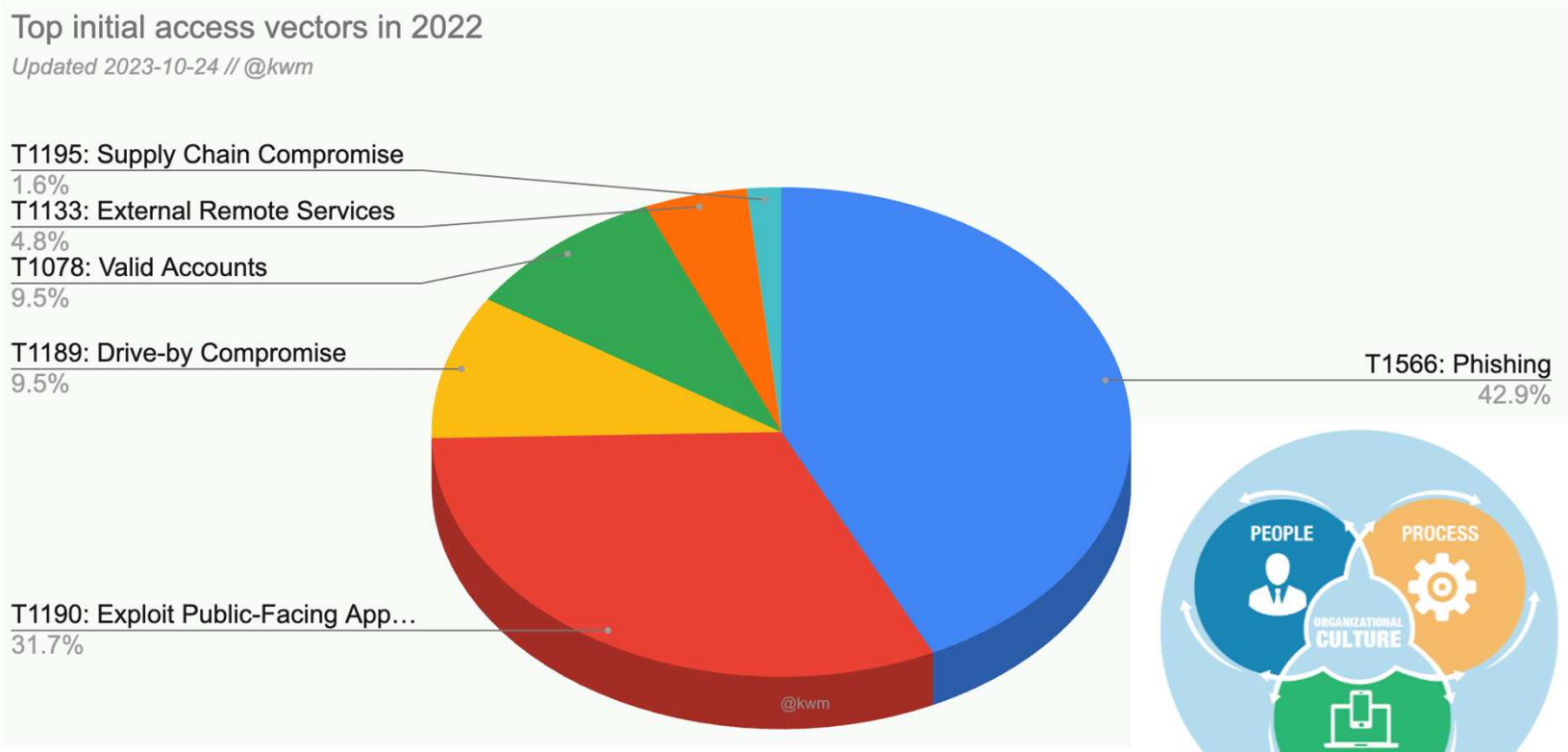
Andere denkwijze

IT Security		OT Security* * Often referred to as Industrial Security
Confidentiality Integrity Availability	Protection goals & priorities	Safety Availability Integrity Confidentiality
3-5 years	Asset lifecycle	20-40 years
Forced migration (e.g. PCs, smart phone)	Software lifecycle	Usage as long as spare parts available
High (> 10 “agents” on office PCs)	Options to add security SW	Low (old systems w/o “free” performance)
Low (~2 generations, Windows 7 and 10)	Heterogeneity	High (from Windows 95 up to 10)
Standards based (agents & forced patching)	Main protection concept	Case and risk based (transparency needed)

Hoe geraken hackers binnen?

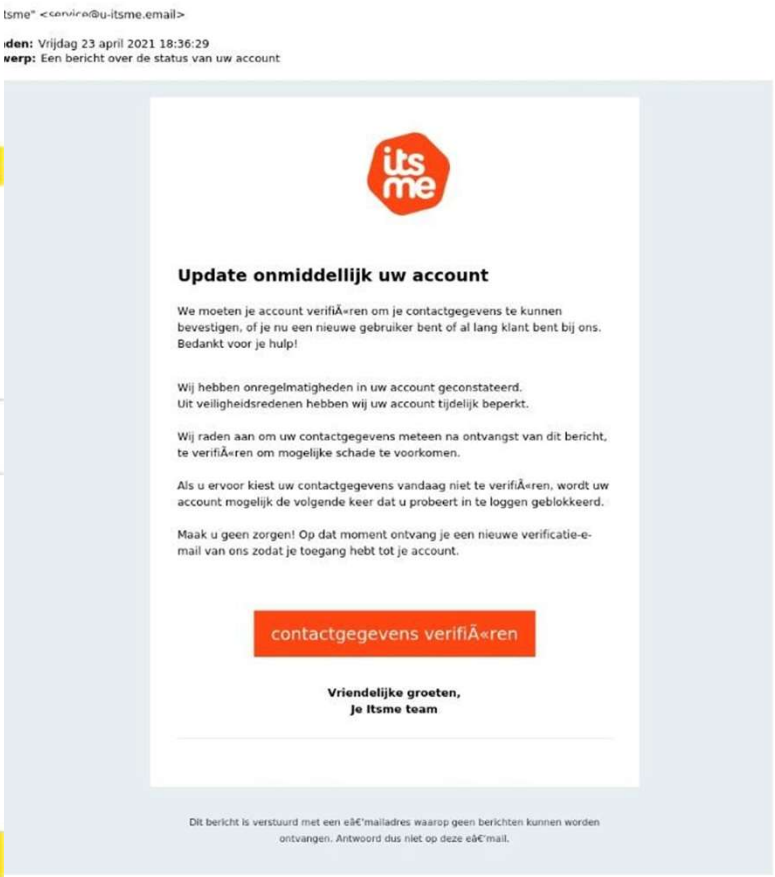
howest
university of applied sciences

De grootste gevaren



howest university of applied sciences

Voorbeeld phishing herkennen



howest university of applied sciences

Toenemende dreiging

VLAIO

Nieuwsblad

Hackers gebruikten ransomware om cybe uit te voeren: grote hinder op Brussels Ai ook luchthavens Heathrow en Berlijn getr

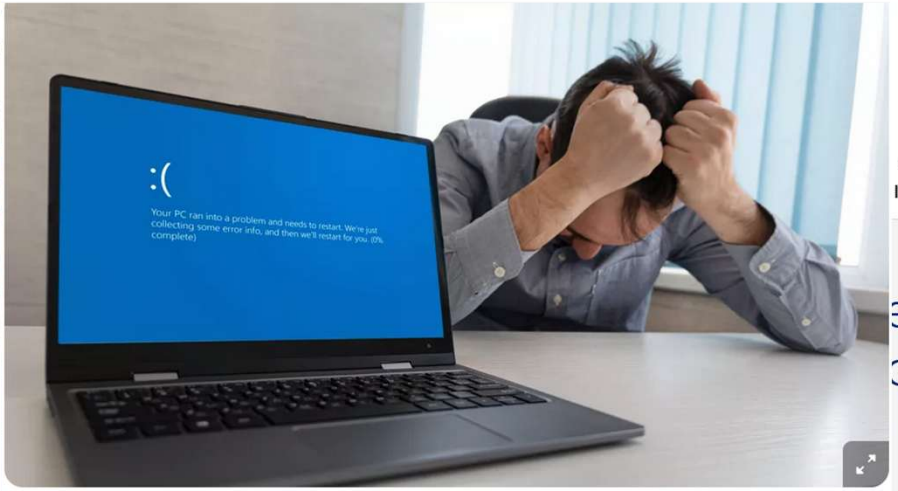
Door een cyberaanval op een partner van Brussels Airport moet de check-in en boar passagiers daar zaterdag manueel gebeuren. Dat meldt de luchthaven. Er werden al geannuleerd, vijftien vluchten lopen vertragingen op van een uur of meer.

Nieuws Duvel Moortgat

Duvel-ha

e vraag

vrt nws



Technologie & Wetenschap

"Blauw scherm des doods" brengt talloze bedrijven in de problemen: wat is er nu eigenlijk aan de hand?

Computersystemen die plots herstarten, inclusief het fameuze "blauwe scherm des doods": duizenden bedrijven met Windows-pc's wereldwijd ondervinden pannes en problemen. Maar het probleem ligt eigenlijk helemaal niet bij Windows. Waar dan wel? En hoe valt dit op te lossen?

Nieuws Events Ondernemersverhalen Blog Publ

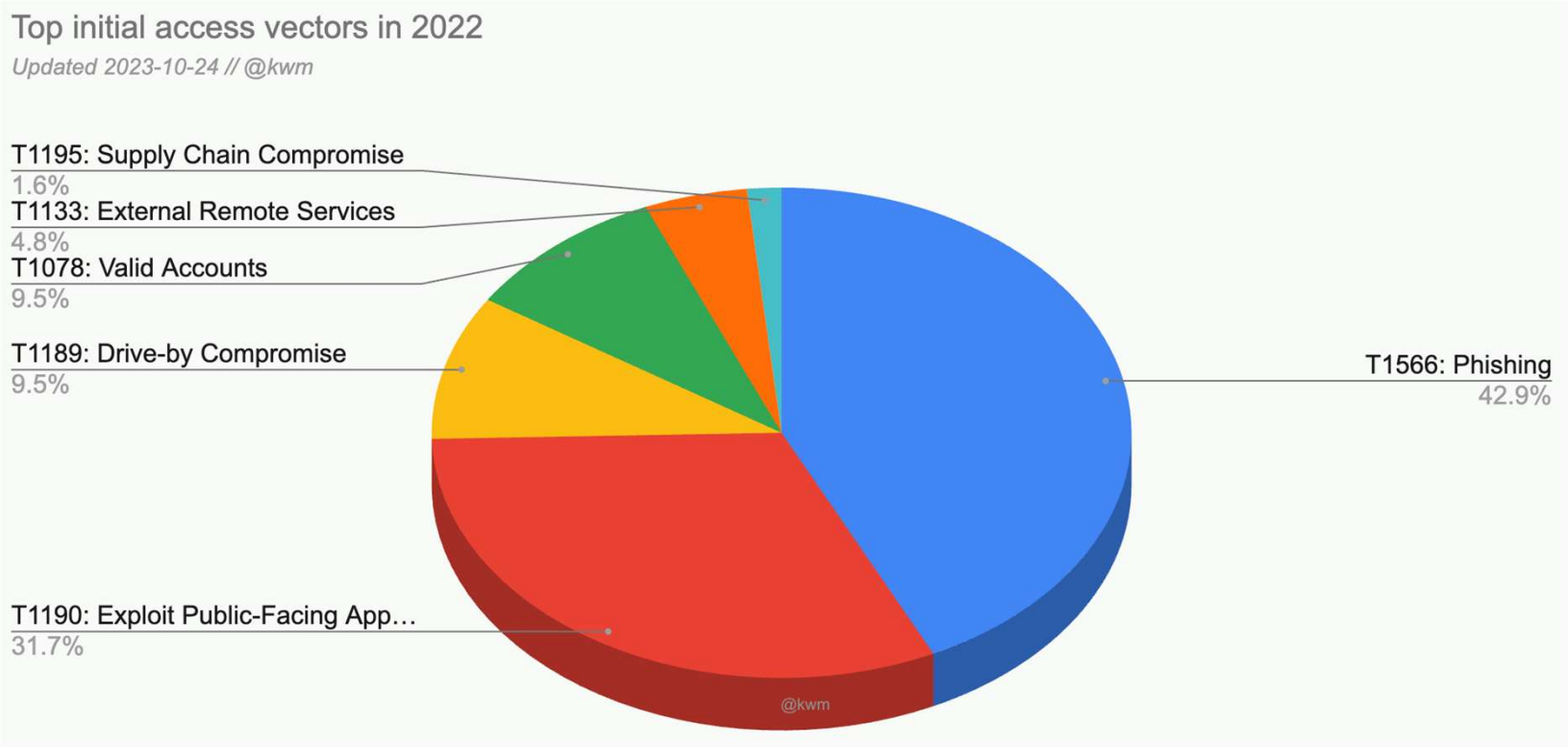
Informatie, begeleiding & advies Subsi

edrijven in 2024
cyberaanval

rijven (45,8%) slachtoffer van een
berokkenden in 1 op de 10 schade
nieuwe cybersecurity barometer.

howest university of applied sciences

De grootste gevaren



howest university of applied sciences

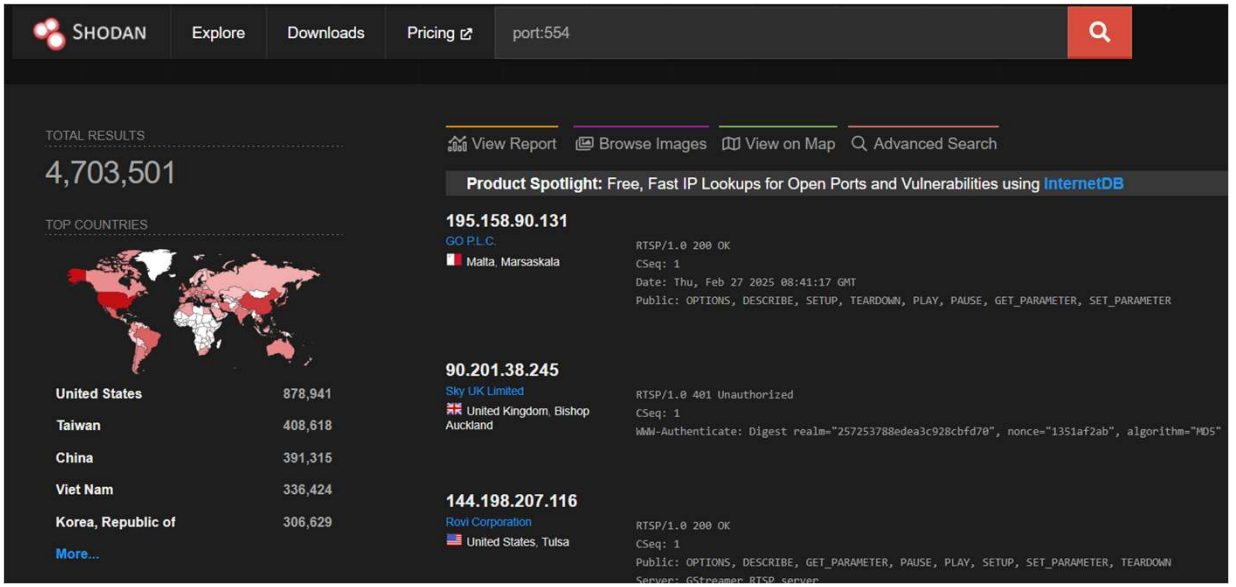
Public-facing applications

Shodan is a search engine for devices

Automatically scans and indexes the entire public IP range for multiple TCP ports

- Explore the possibilities: https://www.shodan.io/explore

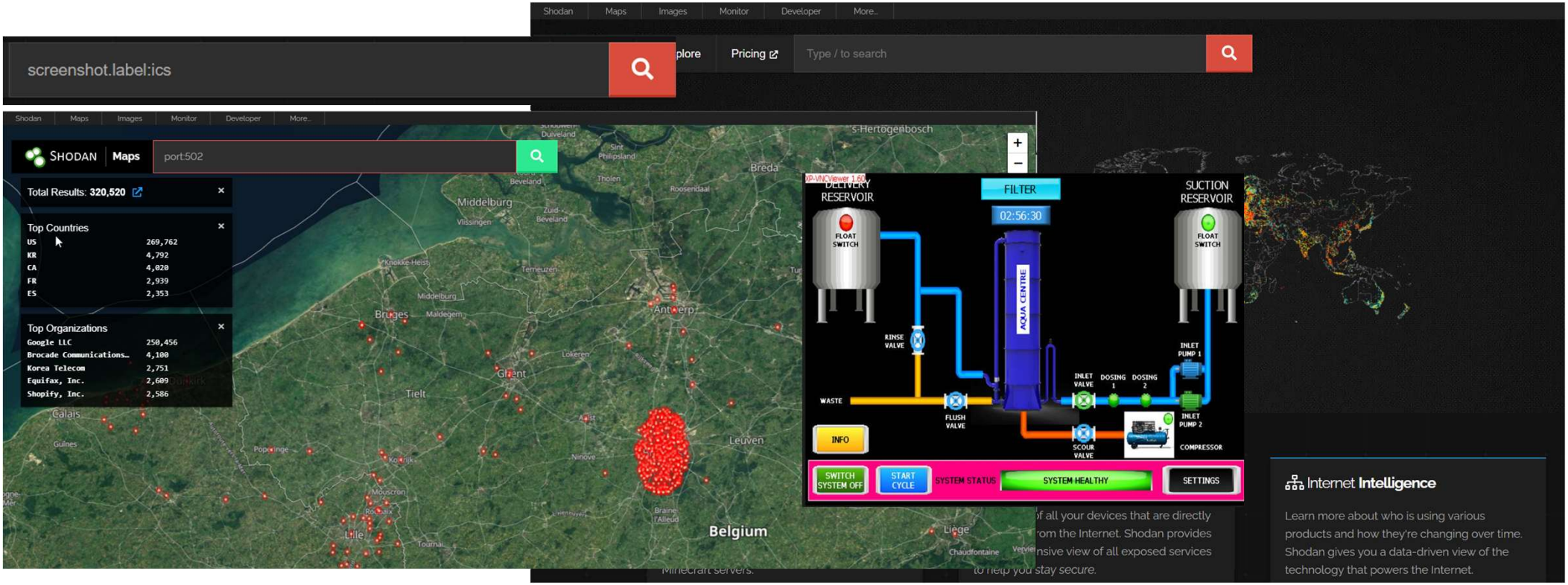
- Hint: It's free, you can check your own public IP's!



howest
university of applied sciences

Shodan

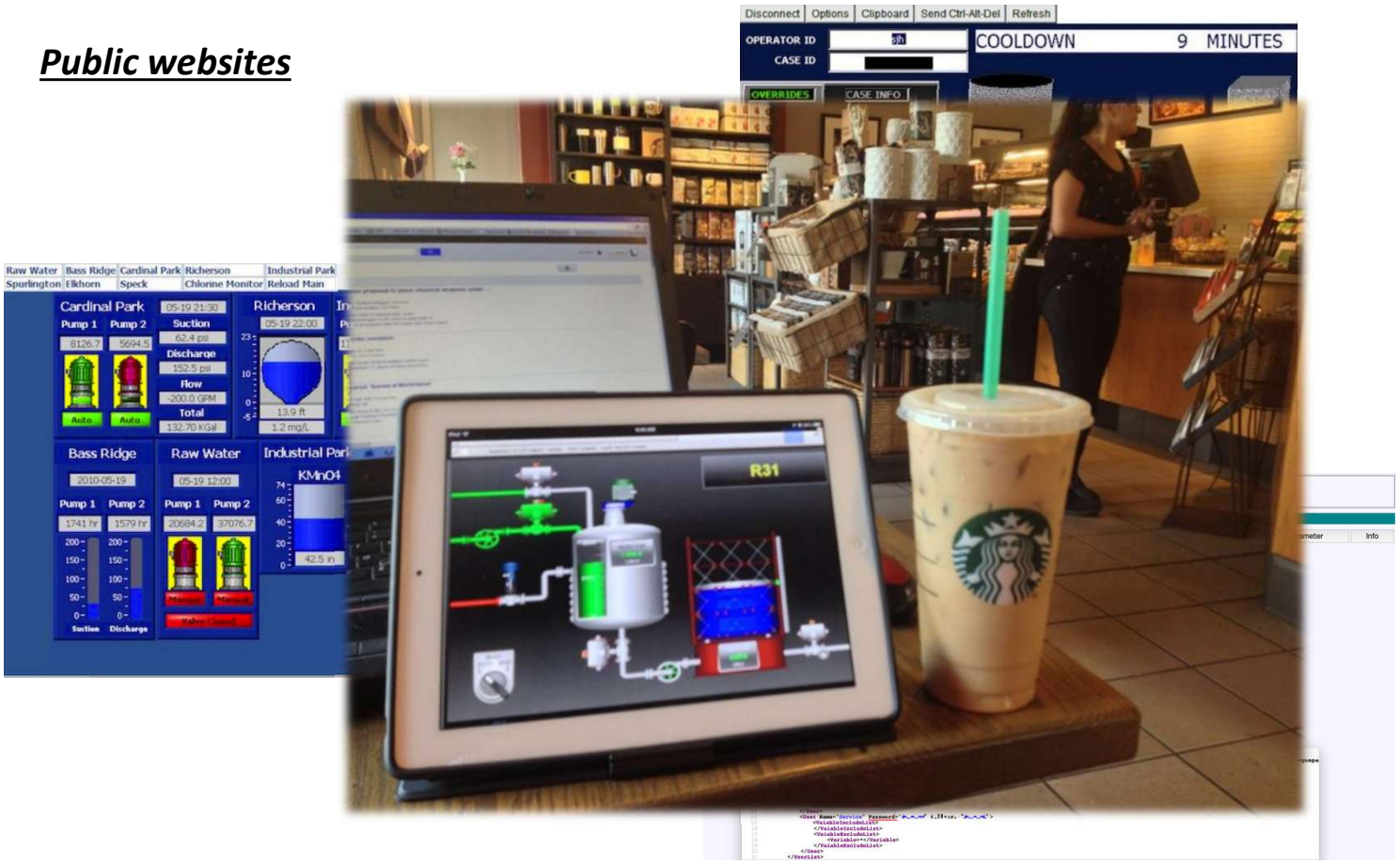
- https://www.shodan.io/

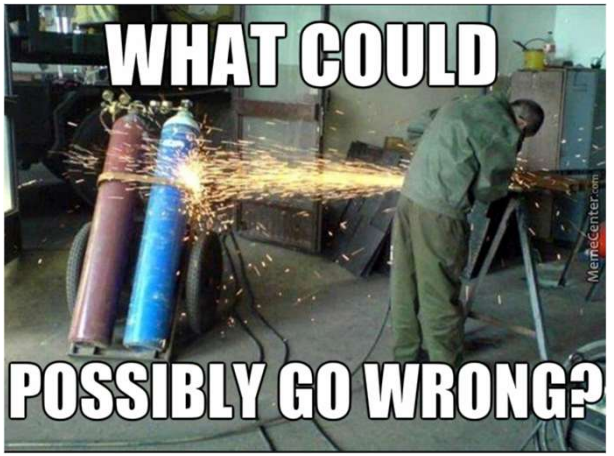


howest university of applied sciences

Remote access over internet to ICS

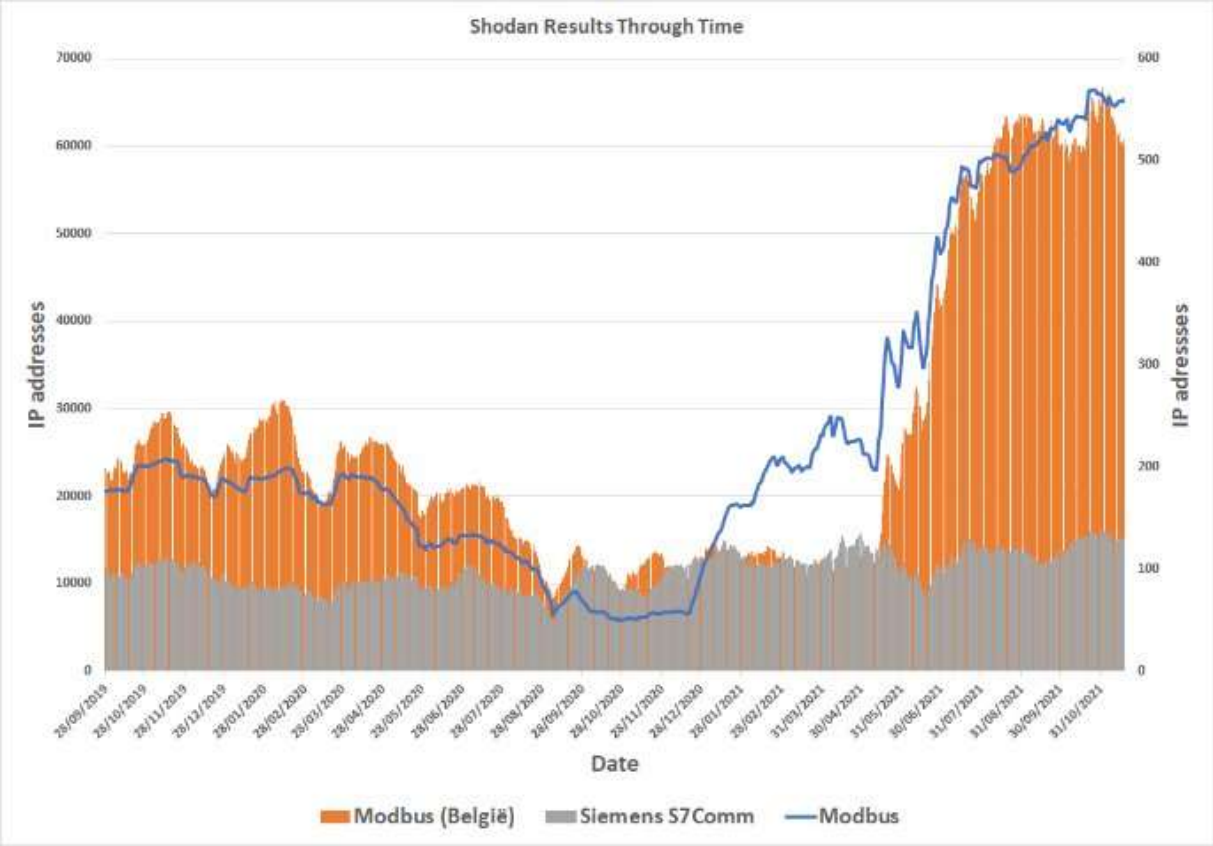
Public websites





howest
university of applied sciences

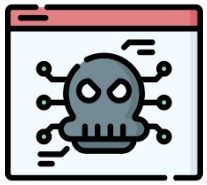
Current day?



howest
university of applied sciences

What are cyberthreats

Cyber threats are malicious actions aimed at gaining access to computers and networks to cause damage or steal information.



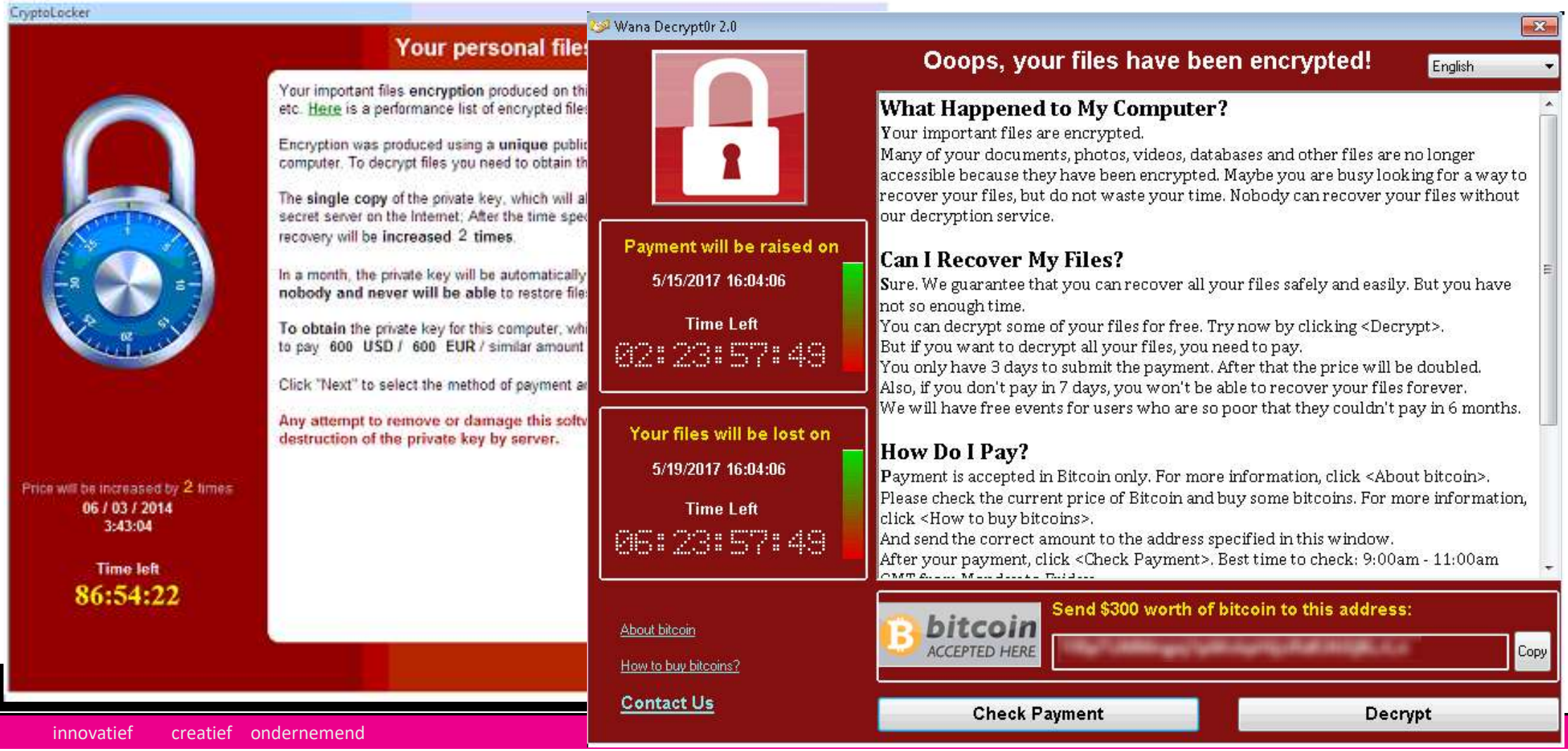
Their goal:

- Financial losses
- Reputation damage
- Loss of sensitive information

howest university of applied sciences

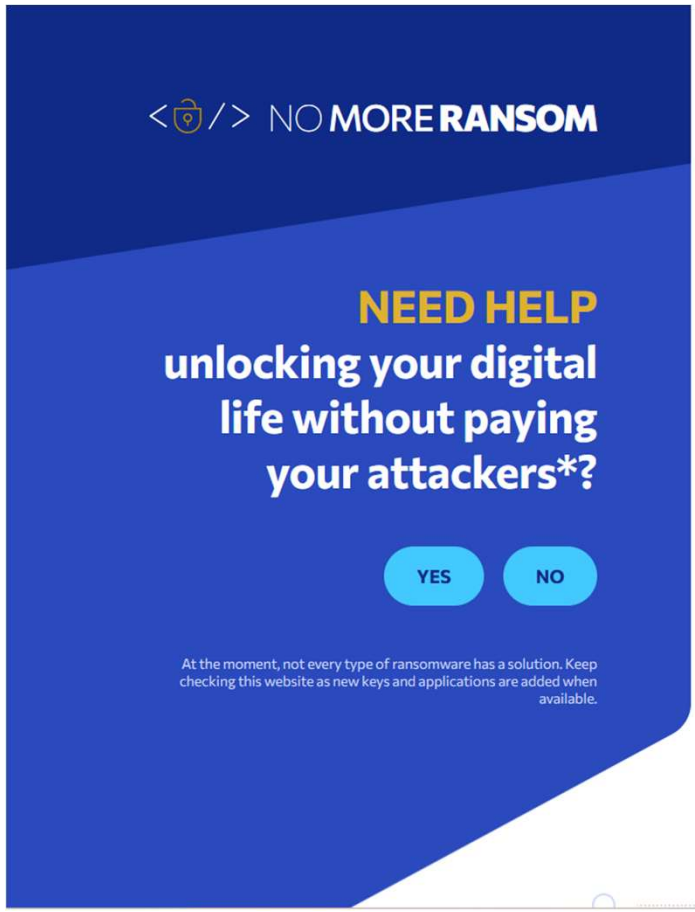
howest
we develop people

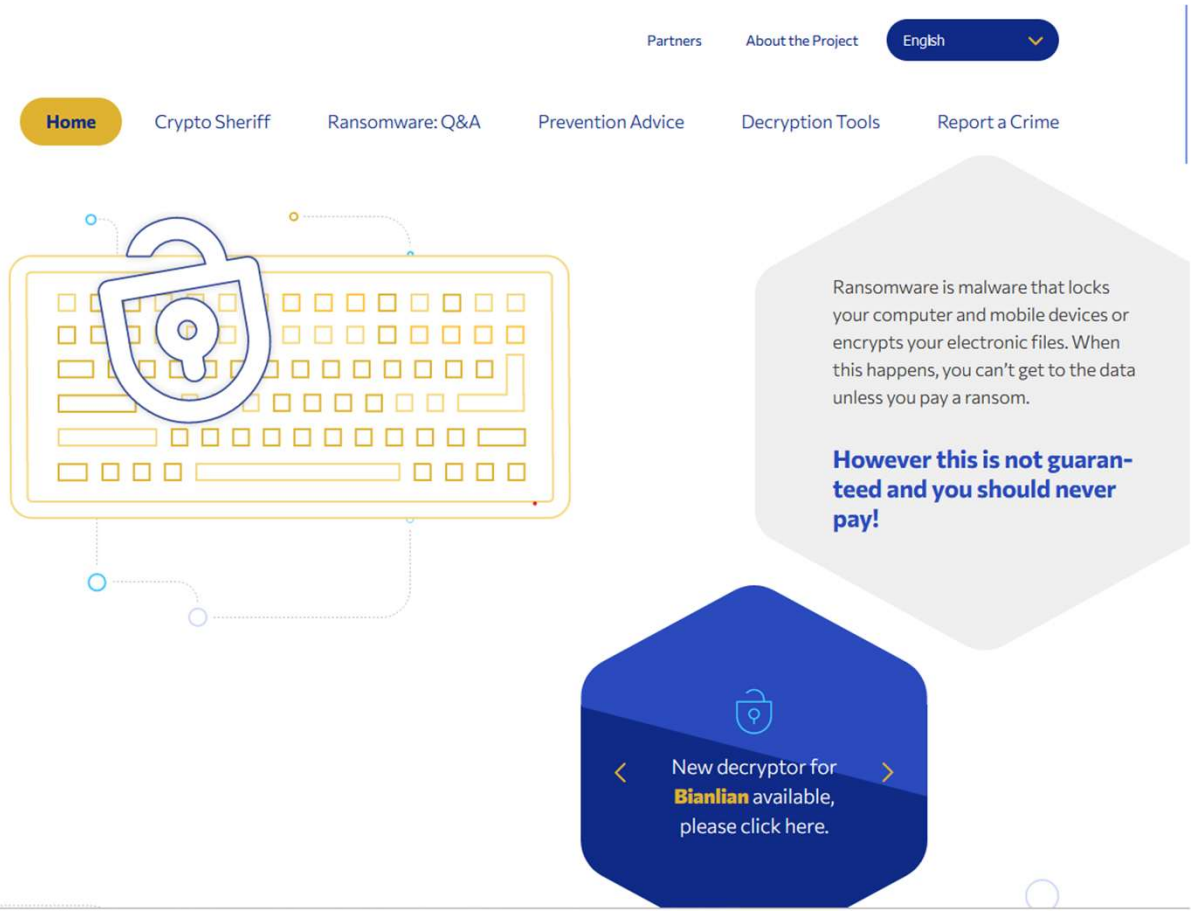
Malware... not something new



Malware for sale

https://www.nomoreransom.org/nl/index.html





Q&A

Wat is de gemiddelde tijdspanne van een inbraak tot ransomware?

90 dagen

De problemen met OT

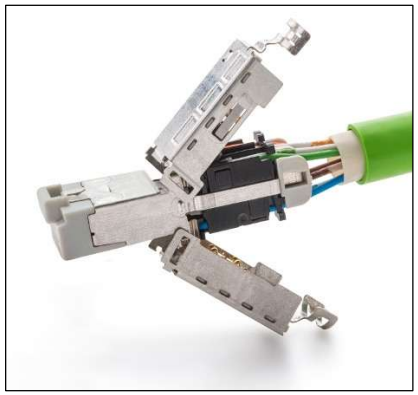
howest
university of applied sciences

Why OT Security now

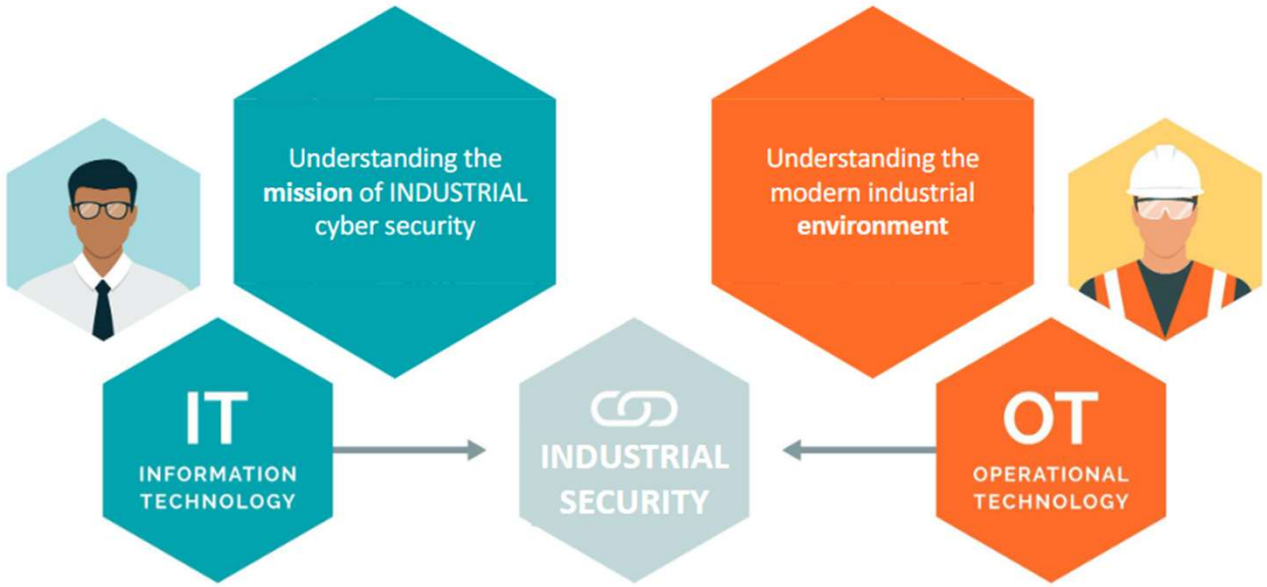
Several migrations have happened over time:

- ± 15 years ago: all systems still used fieldbus protocols
  - There was a movement to Ethernet based protocols
- ± 10 years ago: networking became abundant, everything started to become intra connected
  - Engineers / operators / managers connecting to their **production** devices from everywhere in the company
- ± 5 years ago: the age of IoT, Big Data and Industry 4.0
  - Engineers / operators / managers want to monitor, manage and connect to their **production** devices from at home

And all this using protocols that were developed +40 years ago and have zero support for security, authentication, encryption …



Ownership


Understanding the mission of INDUSTRIAL cyber security
Understanding the modern industrial environment
IT
INFORMATION TECHNOLOGY
INDUSTRIAL SECURITY
OT
OPERATIONAL TECHNOLOGY

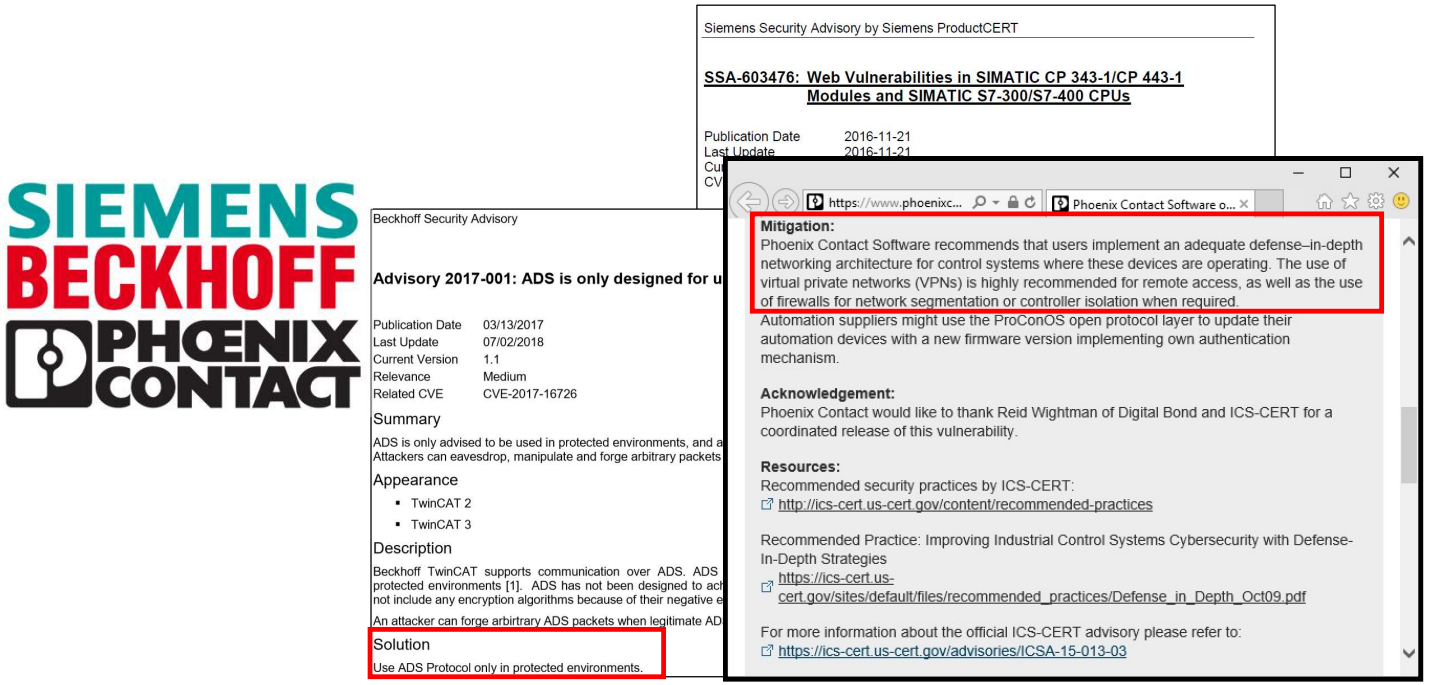
Forced usage of outdated systems

Rockwell Automation Compability 2019	RSLogix 5000 14.01.00	RSLogix 5000 18.02.00	RSLogix 5000 19.01.01	RSLogix 5000 20.01.01	Studio 5000 Logix Designer 21.03.02
Windows 7 Enterprise SP1 32-bit	!	✗	✓	✓	!
Windows 7 Enterprise SP1 64-bit	!	✗	✓	✓	!
Windows 7 Home Premium (32-bit)	!	✗	✓	✓	!
Windows 7 Home Premium (64-bit)	!	✗	✓	✓	!
Windows 7 Home Premium SP1 32-bit	!	!	!	!	✓
Windows 7 Home Premium SP1 64-bit	!	!	!	!	!
Windows 7 Professional (32-bit)	!	✗	✓	✓	!
Windows 7 Professional (64-bit)	!	✗	✓	✓	!
Windows 7 Professional SP1 (32-bit)	!	✗	✓	✓	!
Windows 7 Professional SP1 (64-bit)	!	✗	✓	✓	✓
Windows 7 Ultimate SP1 32-bit	!	!	!	!	!
Windows 7 Ultimate SP1 64-bit	!	!	!	!	!
Windows 8 (home) 32-Bit	!	✗	✗	✗	!
Windows 8 (home) 64-Bit	!	✗	✗	✗	!
Windows 8 Enterprise 32-Bit	!	✗	✗	✗	!
Windows 8 Enterprise 64-Bit	!	✗	✗	✗	!
Windows 8 Professional 32-Bit	!	✗	✗	✗	!
Windows 8 Professional 64-Bit	!	✗	✗	✗	!
Windows 8.1 Enterprise 32-Bit	!	✗	✗	✗	!
Windows 8.1 Enterprise 64-Bit	!	✗	✗	✗	!
Windows 8.1 Professional 32-Bit	!	✗	✗	✗	!
Windows 8.1 Professional 64-Bit	!	✗	✗	✗	!
Windows Vista Business (32-bit)	!	✓	✓	✓	!
Windows XP Pro (32-bit)	!	✗	✗	✗	✗
Windows XP Pro SP1 (32-bit)	!	✗	✗	✗	✗
Windows XP Pro SP2 (32-bit)	!	✗	✗	✗	✗
Windows XP Pro SP3 (32-bit)	!	✓	✓	✓	✗

Rockwell Automation Compability 2019	RSLogix 5000 14.01.00	RSLogix 5000 18.02.00	RSLogix 5000 19.01.01	RSLogix 5000 20.01.01	Studio 5000 Logix Designer 21.03.02
Linux	!	!	!	!	✗
Windows 2000	!	✗	✗	✗	✗
Windows NT Workstation 4.0 (NTFS)	!	✓	✓	✗	✗
Windows 10 Enterprise, 32-bit, Version 1511	!	!	!	!	!
Windows 10 Enterprise, 32-bit, Version 1607	!	!	!	!	!
Windows 10 Enterprise, 64-bit, Version 1511	!	!	!	!	!
Windows 10 Enterprise, 64-bit, Version 1607	!	!	!	!	!
Windows 10 Enterprise, 64-bit, Version 1703	!	!	!	!	!
Windows 10 Professional, 32-bit, Version 1511	!	!	!	!	!
Windows 10 Professional, 32-bit, Version 1607	!	!	!	!	!
Windows 10 Professional, 64-bit, Version 1511	!	!	!	!	!
Windows 10 Professional, 64-bit, Version 1607	!	!	!	!	!
Windows 10 Professional, 64-bit, Version 1703	!	!	!	!	!
Windows 2003 Standard (32-bit)	!	✓	✓	✓	✗
Windows 2003 Standard SP1 (32-bit)	!	✓	✓	✓	✗
Windows 2003 Standard SP2 (32-bit)	!	✓	✓	✓	✗
Windows 2003 R2 Standard (32-bit)	!	!	!	!	✗
Windows 2003 R2 Standard SP2 (32-bit)	✓	✓	✓	✓	✗
Windows 2003 R2 Standard SP2 (64-bit)	!	!	!	!	✗
Windows Server 2003 Standard R2 SP1 [32-bit]	!	!	!	!	✗
Windows Server 2008 Standard (32-bit)	!	✓	✓	✓	✗
Windows Server 2008 Standard SP1 (32-bit)	!	!	!	!	✗
Windows Server 2008 Standard SP1 [64-bit]	!	!	!	!	✗
Windows Server 2008 Standard SP2 (32-bit)	!	!	!	✓	✗
Windows Server 2008 Standard SP2 (64-bit)	!	!	!	✓	✗
Windows Server 2008 R2 Enterprise SP1	!	!	!	!	!
Windows Server 2008 R2 Standard	!	!	!	!	!

howest
university of applied sciences

Vendor warning



howest university of applied sciences

Living off the land

- Use native tools
- Low detectability
- Minimal footprint
  - Powershell scripts
  - WMI abuse
  - Credential dumping
  - Using certutil.exe bitsadmin.exe, wmic.exe to move data and execute commands

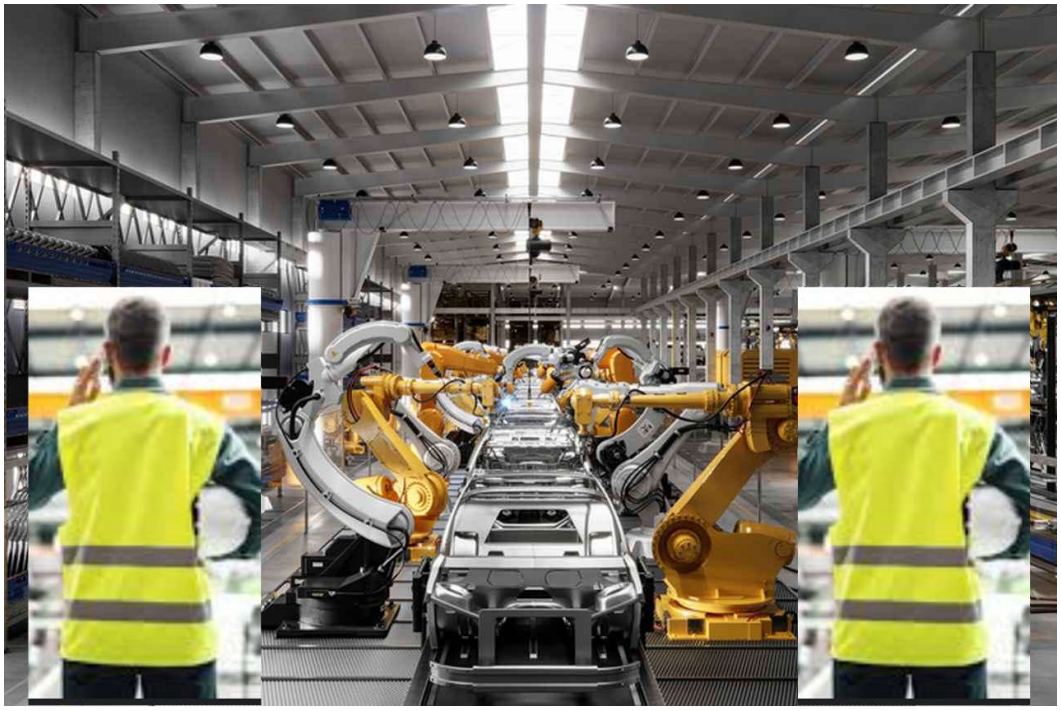
Real world cases

howest
university of applied sciences

Risk awareness: “Public devices”

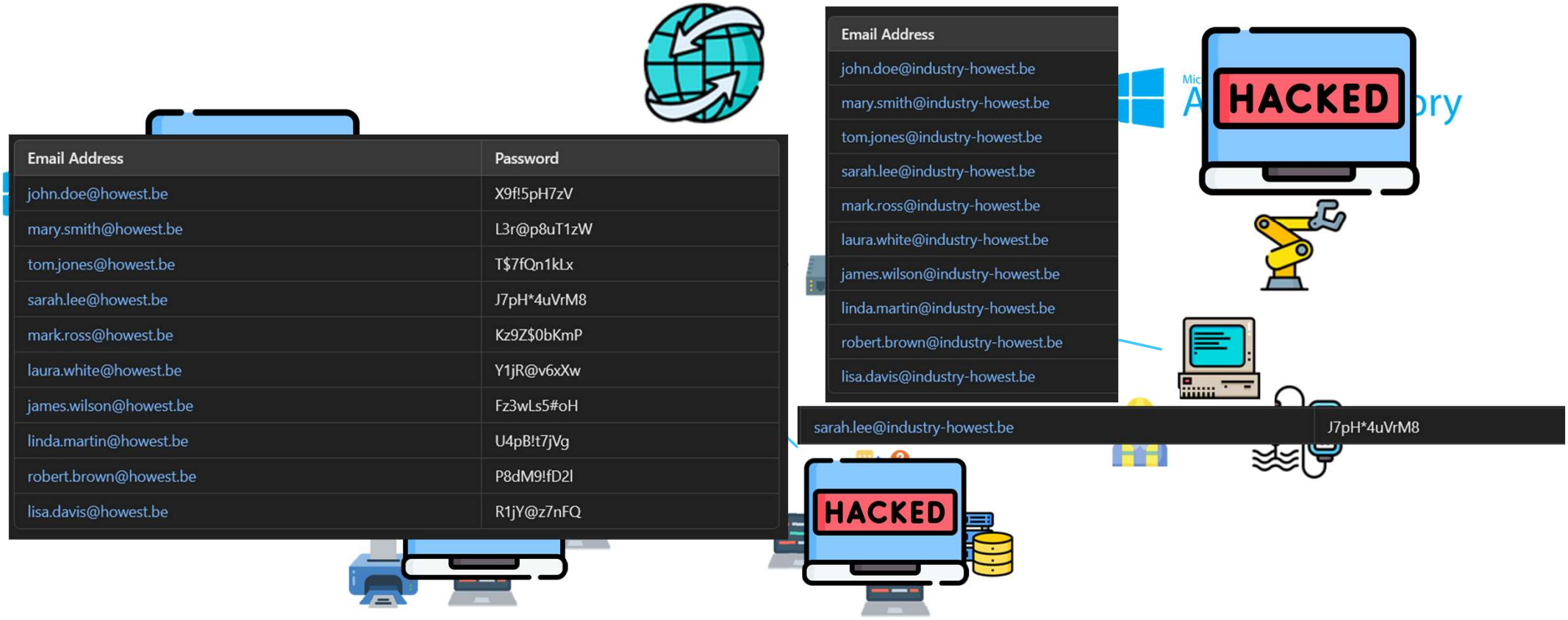
howest
university of applied sciences

Risk awareness: “Physical security”



howest university of applied sciences

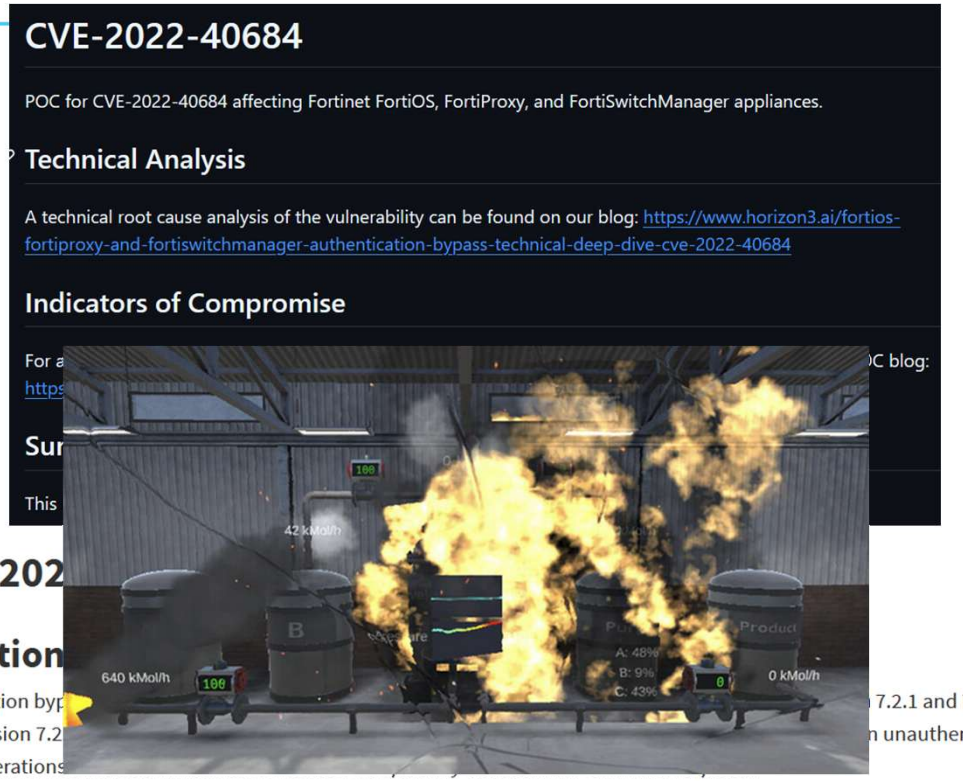
Risk awareness: “Passwords”



howest university of applied sciences

Realistic real word scenario

- Let's say we want to target factory.xyz
- Find their public facing applications with Shodan zoomeye, crt.sh…
- Enumerate those endpoints.
- VPN access into the netowork
- Enumerate hosts
- Exploit the weak protocols



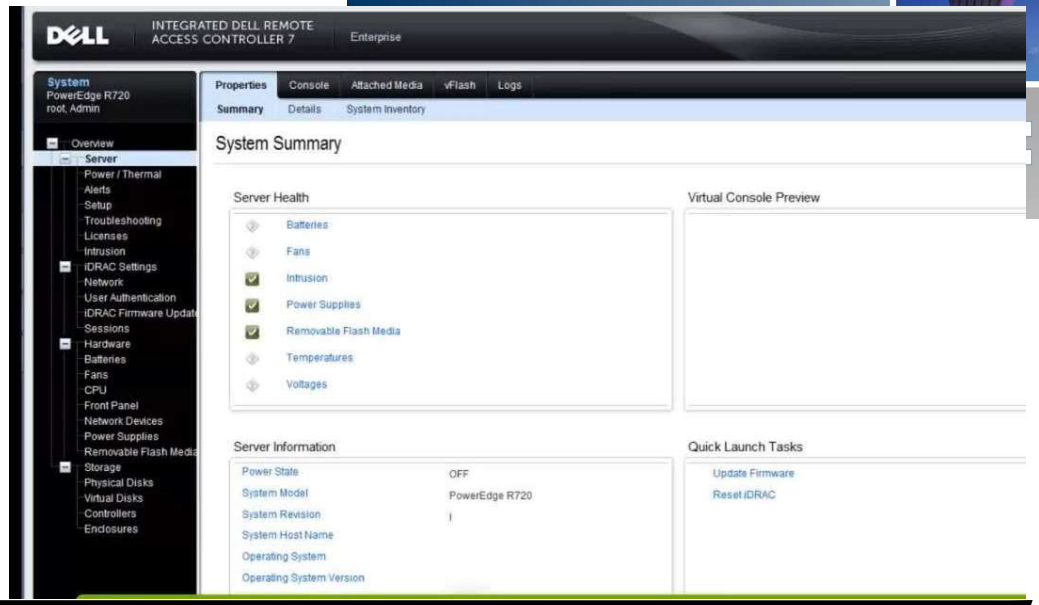
IPMI 2.0 (intelligent platform management interface)

Via IPMI beheer je servers op afstand.

https://www.rapid7.com/db/modules/auxiliary/scanner/ipmi/ipmi_dumphashes/

Als je de naam van een useraccount kent kan je de hash opvragen.

UDP 623

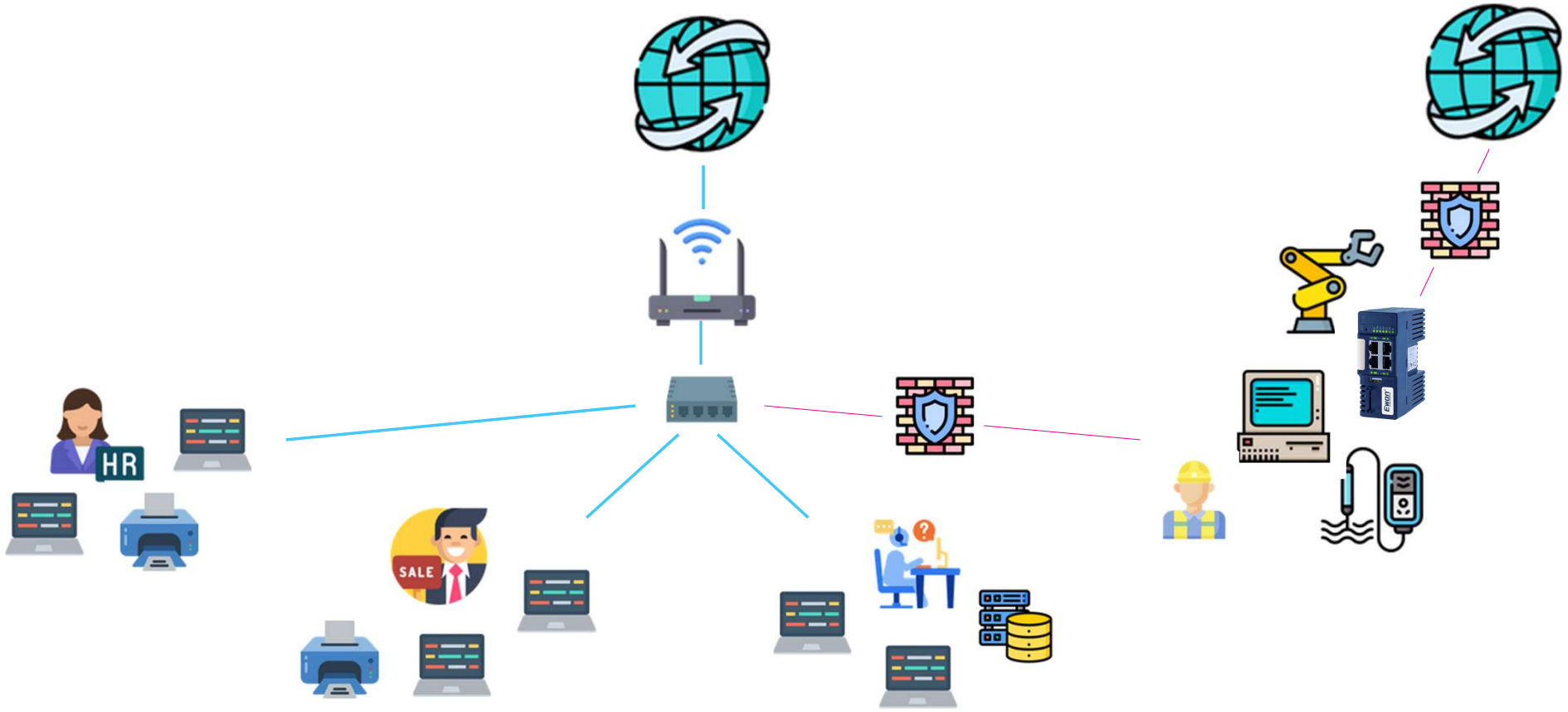


howest university of applied sciences

Eerste stappen

howest
university of applied sciences

Segmentatie



howest
university of applied sciences

Limit need access

- Separate guest - office WiFi
- Separate or put layers (firewall, data diode,…) between OT & IT
- Don’t connect anything to the outside without it being absolutely necessary. (IIoT data, VNC connection to HMI,…)
- Implement accountability, use users/roles to limit access and log who does what in case something goes wrong.

howest university of applied sciences

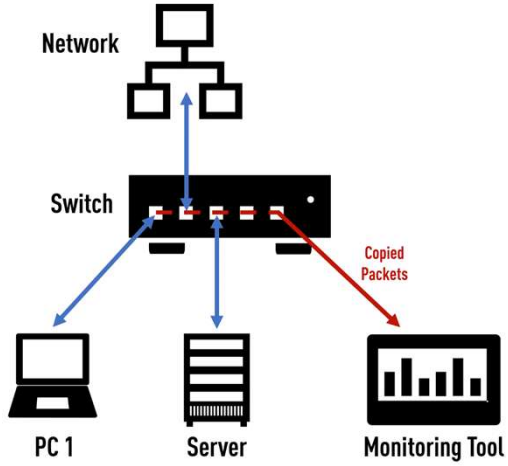
Monitoring solutions

- **Visibility**
  - Asset discovery & inventory
- **Detection**
  - Pin-point security threats in real time
- **Response**
  - Accelerate remediation efforts

Kaspersky Industrial CyberSecurity

NOZOMI NETWORKS

CLAROTY



howest university of applied sciences

Evolution

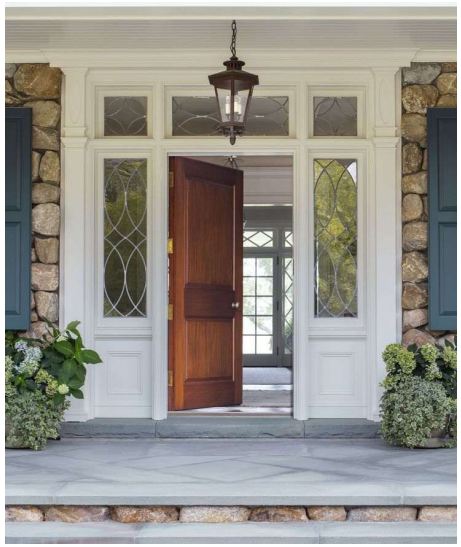
default password change

segmentation & risk awareness

security architecture & asset management

start incidence response plan

monitoring



howest university of applied sciences