Cybersecurity in the industrial control systems

Yugo Neumorni, EMBA, CISA

President, CIO Council Romania

CIO COUNCIL
Romania

Yugo Neumorni

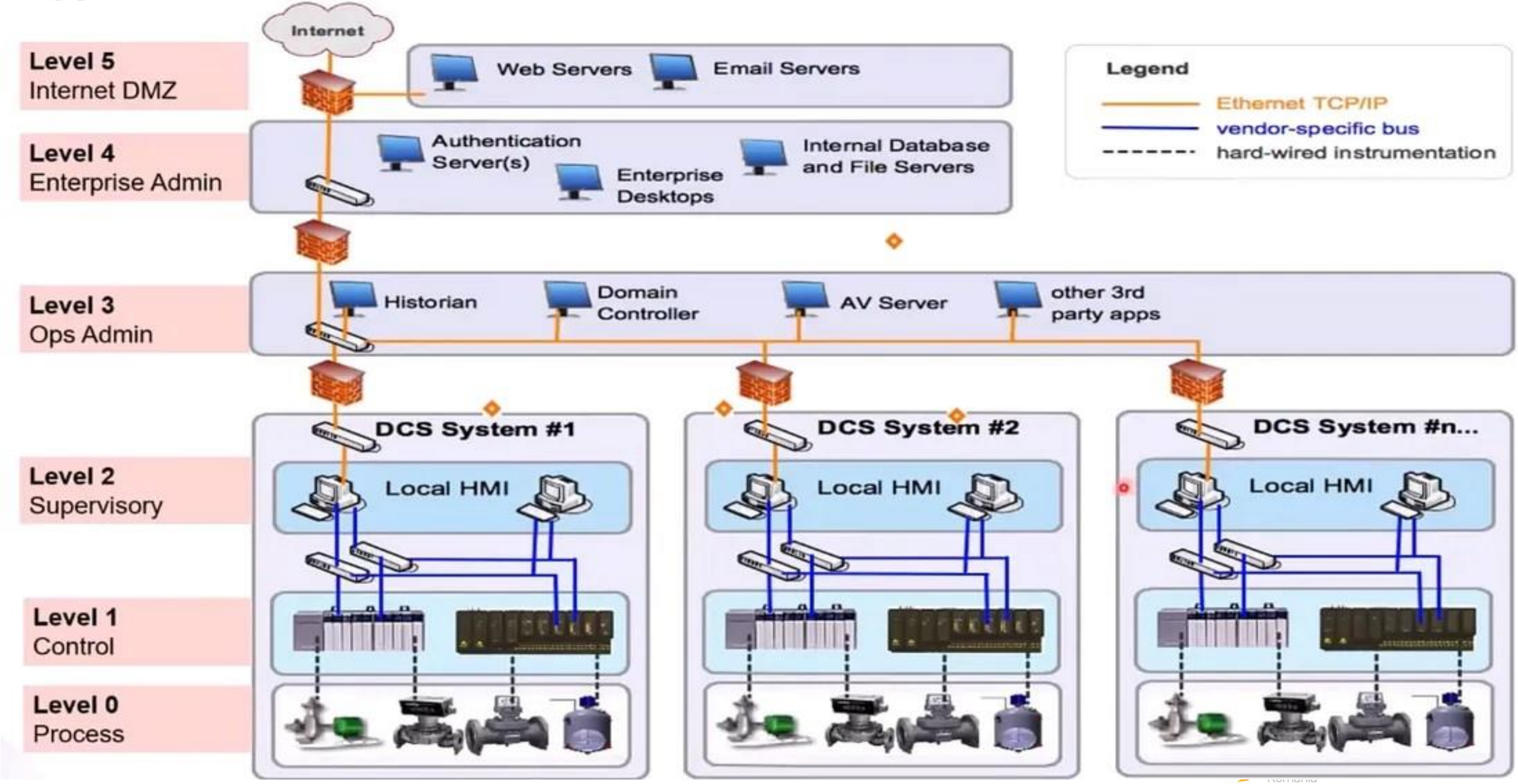
- ✓ ContourGlobal, CIO (2022 – 2023)
- ✓ ClusterPower, CDO (2021 – 2022)
- ✓ Urgent Cargus, CIO (2019 – 2021)
- ✓ Hidroelectrica, CIO, (2014 – 2019)
- ✓ Vimetco, CIO, (2004 – 2014)
- ✓ Deloitte & Touche Central Europe, IT Manager, (1998 – 2004)
- ✓ Board member EuroCIO (www.eurocio.org), 2017 - 2022
- ✓ Chairman of EuroCIO 2020 - 2022
- ✓ CIO Council President and co-founder (www.ciocouncil.ro) since 2009
- ✓ ISACA Romania President and Board Member 2007 – 2016. www.isaca.com
- ✓ Advisory Board Member – Forum International de Cybersecurity, Lille (www.forum-fic.com), since 2018
- ✓ EMBA, Asebuss- Kennessaw State University, 2007 - 2009
- ✓ CISA, Certified Information System Auditor, 2001, Budapest, Hungary
- ✓ CIO Council National Conference organizer (www.cioconference.ro)
- ✓ Gold Winner of the 2017 SAP Quality Awards, Fast Delivery category in CEE with Hidroelectrica.
- ✓ Speaker in IT international conferences

- ✓ *Yugo Neumorni is specialized in reorganization, planning, design and implementation of complex industrial IT environments for multinational companies. His area of expertise includes ERP (SAP) projects, large scale IT division reorganization and development, IT security & cyber, SCADA and industrial control systems, IT audit and IT governance, business processes in energy, aluminum and manufacturing, COBIT framework, ITIL.*

There are two types of companies: those who have been hacked, and those who don’t yet know they have been hacked.

John Chambers
Chief Executive Officer of Cisco

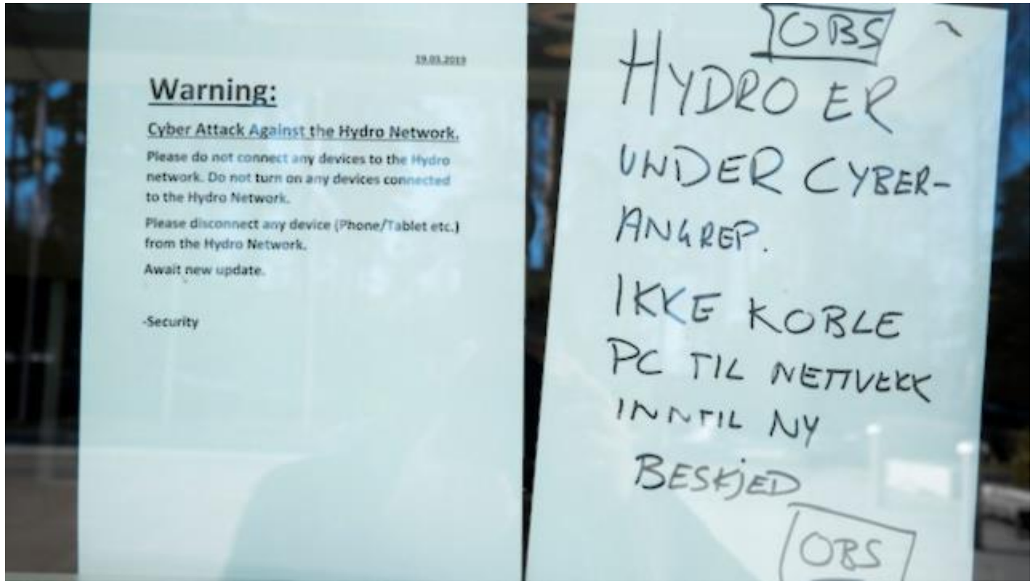
Typical Industrial Network Architecture: Purdue Model



https://medium.com/@srank2000/industry-4-0-security-iiot-iot-ot-scada-purdue-model-of-industrial-network-architecture-d86c70f06c74

Norsk Hydro held hostage by a ransomware attack

- Did not pay the ransomware
- Norsk operated on manual
- Norsk restored from backups
- 22,000 computers affected
- 170 sites in 40 countries
- 35.000 employees back to pen and paper



19.03.2019

Warning:

Cyber Attack Against the Hydro Network.

Please do not connect any devices to the Hydro network. Do not turn on any devices connected to the Hydro Network.

Please disconnect any device (Phone/Tablet etc.) from the Hydro Network.

Await new update.

-Security

OBS

HYDRO ER UNDER CYBER-ANGREP.

IKKE KOBLE PC TIL NETTVERK INNTIL NY BESKJED

OBS

Workshop:
- To pay or not to pay?
- Where do I get Bitcoins?
- Where is my backup?
- Was backup affected?
- IS there a DRP plan for ransomwere situations?
- What is the first service restored? Active Directory? ERP?
- Do we need additional hardware? Where do we get from?

https://www.bbc.com/news/business-48661152

CIO COUNCIL Romania

Attacks on DSOs.
Ukrainian power grid attack

- 225,000 people were left without power for approximately 6 hours on December 23, 2015, in Ukraine.
- Spear-phishing schemes, malware, and manipulation of long-known Microsoft Office macro vulnerabilities
- Collected the credentials to gain access to SCADA systems
- Virtual workstations inside SCADA systems that were trusted to issue system commands
- Co-opting remote terminal units within SCADA systems to issue “open” commands to specific breakers at substations
- Severing communications by targeting firmware in serial-to-Ethernet devices
- Installing and running a modified KillDisk program that deleted information on what was occurring while making recovery reboots nearly impossible
- Shutting down uninterruptible power supplies at control centers
- Executing a large denial-of-service attack on utility call centers that prevented customers from reporting outages
- Spear phishing is a targeted email that appears to be from a known business or individual

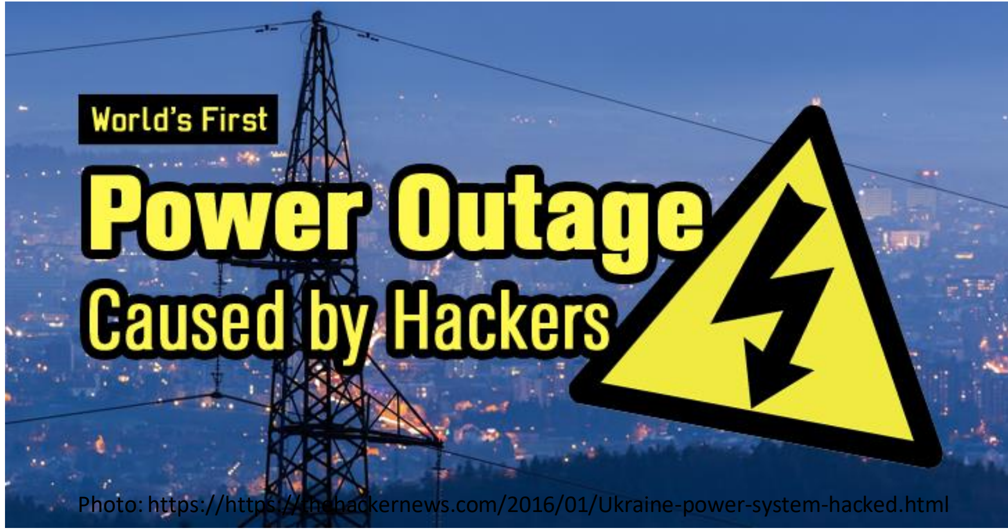


Photo: https://https://thehackernews.com/2016/01/Ukraine-power-system-hacked.html

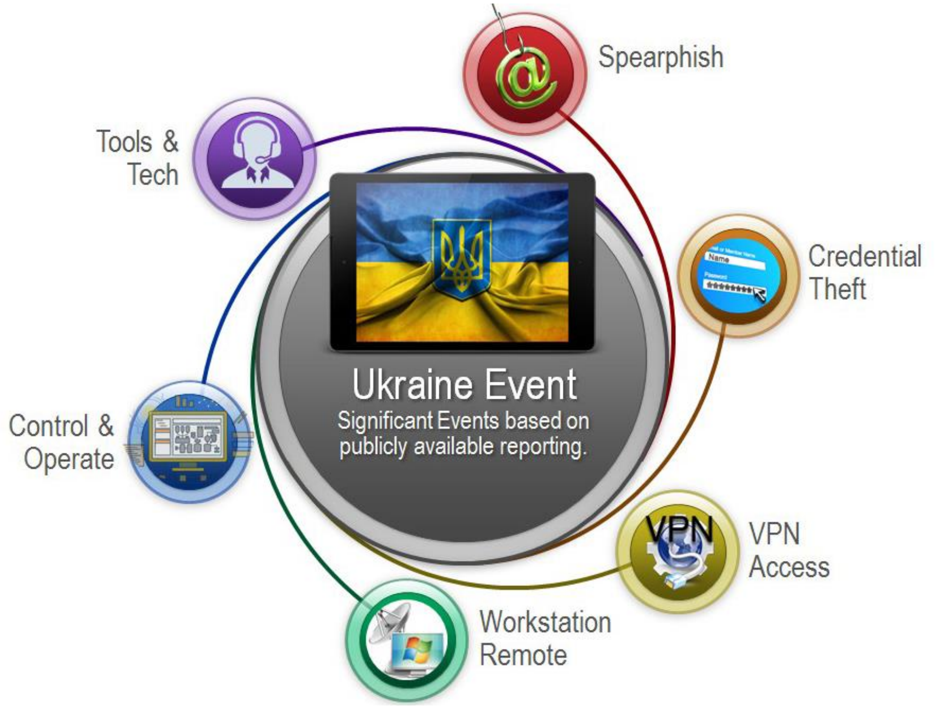
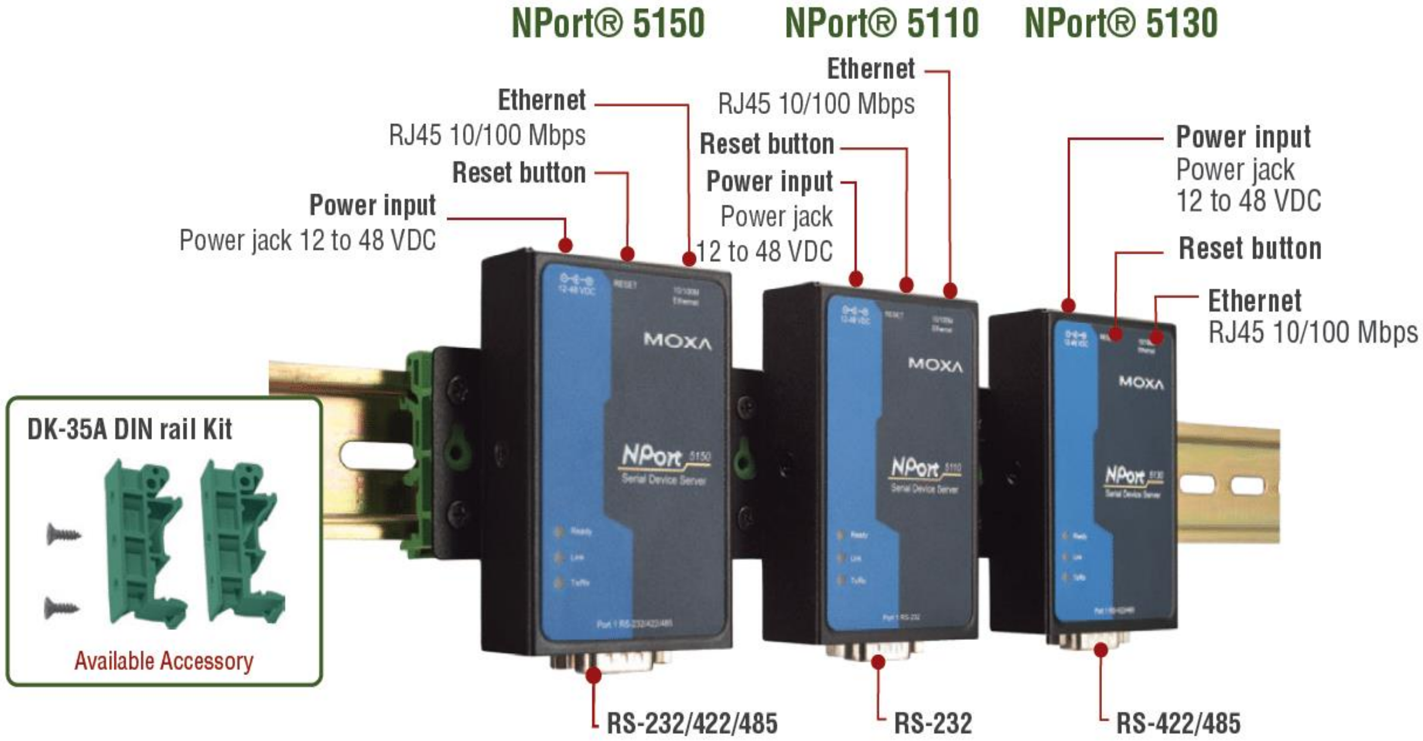


Photo: https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

Serial To Ethernet Converters are the Huge Critical Infrastructure Risk Nobody Talks About

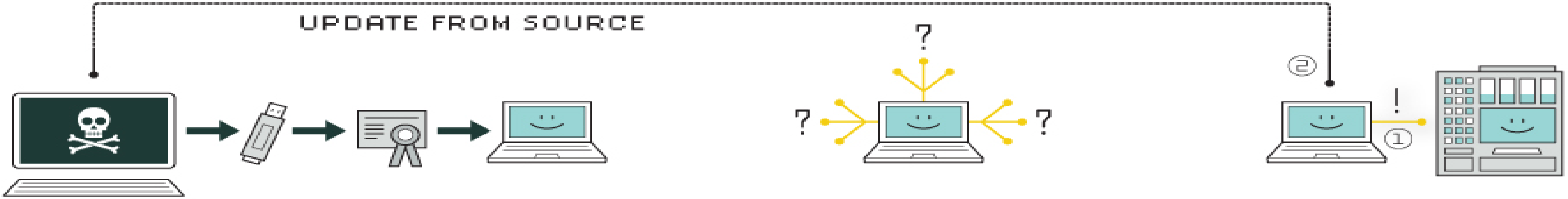
There are more warnings that a common piece of hardware known as Serial-to-Ethernet converters are very vulnerable to remote attacks – and more evidence that the vendors who manufacture them aren't in a rush to fix the holes.



https://securityledger.com/2016/04/serial-to-ethernet-converters-the-giant-infrastructure-risk-nobody-talks-about/

CIO COUNCIL Romania

HOW STUXNET WORKED



1. infection

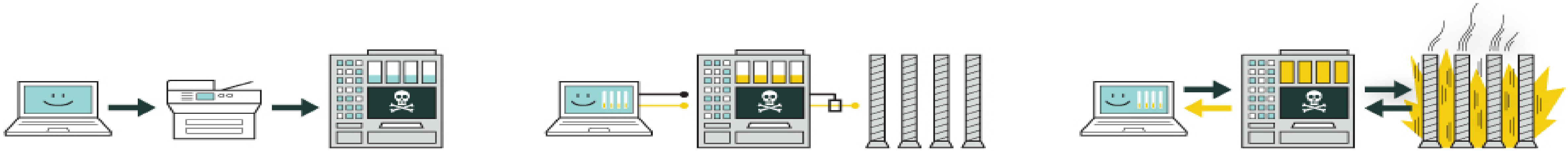
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control

In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

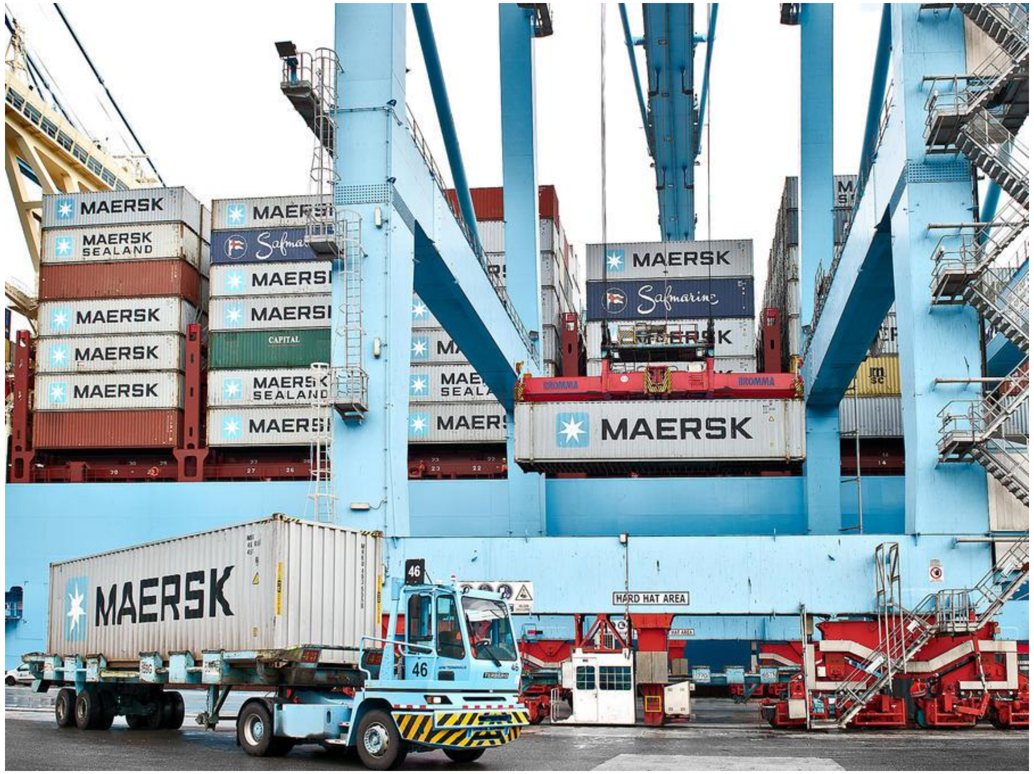
6. deceive and destroy

Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

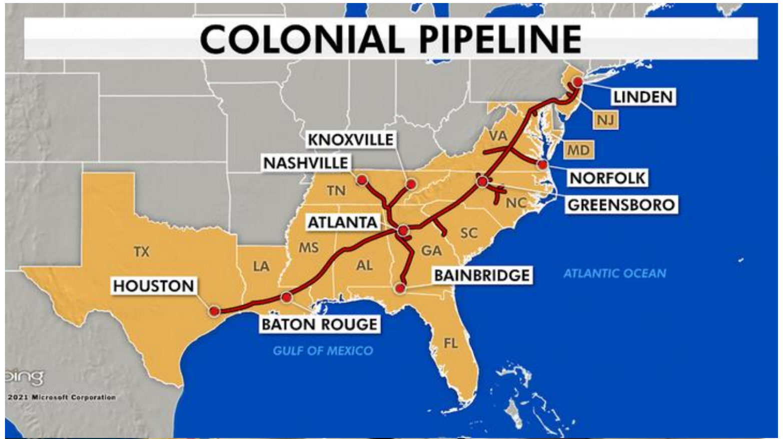
Maersk ransomware attack – 300mln

- Developed as a disk-wiping cyber weapon by the Russian military
- helped by a leaked version of the NSA's EternalBlue hacking tool – which is the same exploit that powered the WannaCry ransomware outbreak
- **NotPetya's target was businesses in Ukraine – but the malware quickly got out of hand**.
- It was spreading around the world, taking down networks and causing billions of dollars in damage and lost revenue.



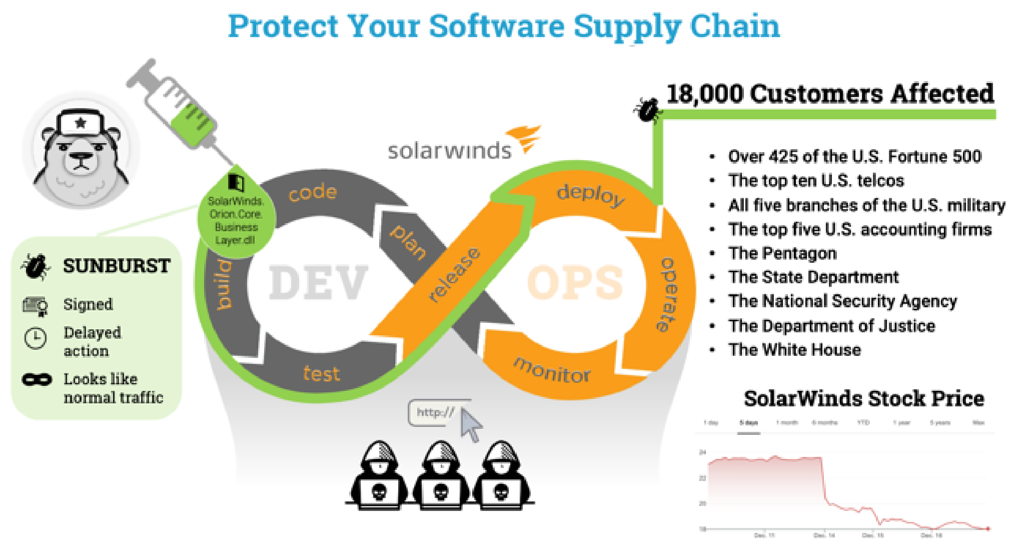
Colonial pipeline ransomware attack - 2021

- ✓ U.S.'s largest fuel pipeline offline for days
- ✓ Colonial Pipeline Co. paid hackers $4.4 million in ransom just hours after the attack took place (*Bloomberg*)
- ✓ Orchestrated by DarkSide a Russian sponsored group (*FBI*)
- ✓ DarkSide is ransomware-as-a-service entity(RaaS) *(CISA.gov)*
- ✓ "Double extortion". Hackers encrypt and lock up the victim's data, but they also steal data and threaten to make it public
- ✓ Colonial restored from backups
- ✓ Executive Order signed by President Biden intended to improve US cybersecurity after the hack



SolarWinds attack - 2021

- ✓ highly sophisticated Russian Intelligence group has compromised the SolarWinds Orion platform infecting directly into the SolarWinds DevOps. the package was signed with a valid certificate
- ✓ 18,000 customers affected downloading the patches, opening a backdoor to the attackers
- ✓ Attackers penetrated and manipulated SolarWinds 9 months before, malware deployment estimated to December 2019
- ✓ Orion it is connected everywhere – from switches and routers, to firewalls, virtualization infrastructure, Active Directory, storage management tools and more
- ✓ US agencies, DHS, the Department of Energy, the National Nuclear Security Administration, and the Treasury — were attacked. Also private companies, like Microsoft, Cisco, Intel, and Deloitte
- ✓ Effects of this cyberattack will continue to generate effects
- ✓ This could lead access to OT / SCADA / Industrial Control System networks


Protect Your Software Supply Chain

18,000 Customers Affected

- Over 425 of the U.S. Fortune 500
- The top ten U.S. telcos
- All five branches of the U.S. military
- The top five U.S. accounting firms
- The Pentagon
- The State Department
- The National Security Agency
- The Department of Justice
- The White House

SUNBURST

- Signed
- Delayed action
- Looks like normal traffic

https://blog.adolus.com/blog/three-things-the-solarwinds-supply-chain-attack-can-teach-us

What if operating systems (Windows) supply chain will be hacked?

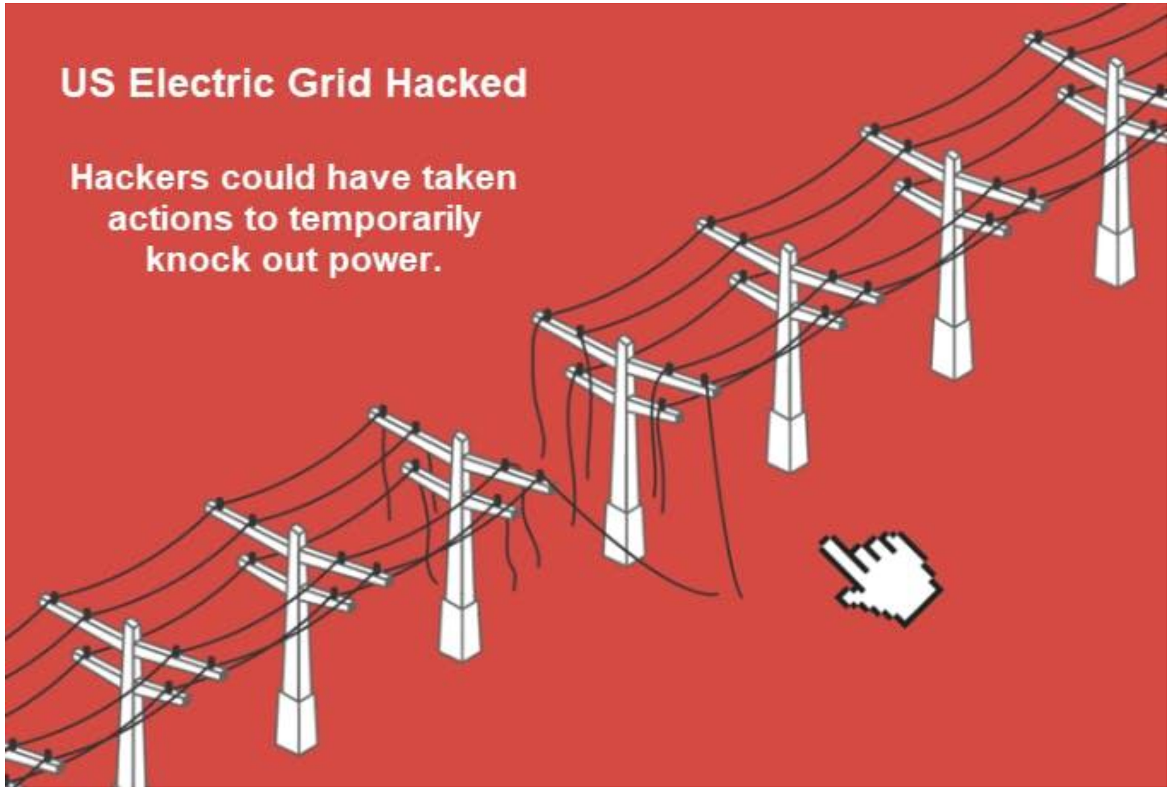
What if the hardware firmware of critical equipment is hacked?

Are you ready for the next cyberattack?

https://room42.lu/

U.S. Government Makes Surprise Move To Secure Power Grid From Cyberattacks

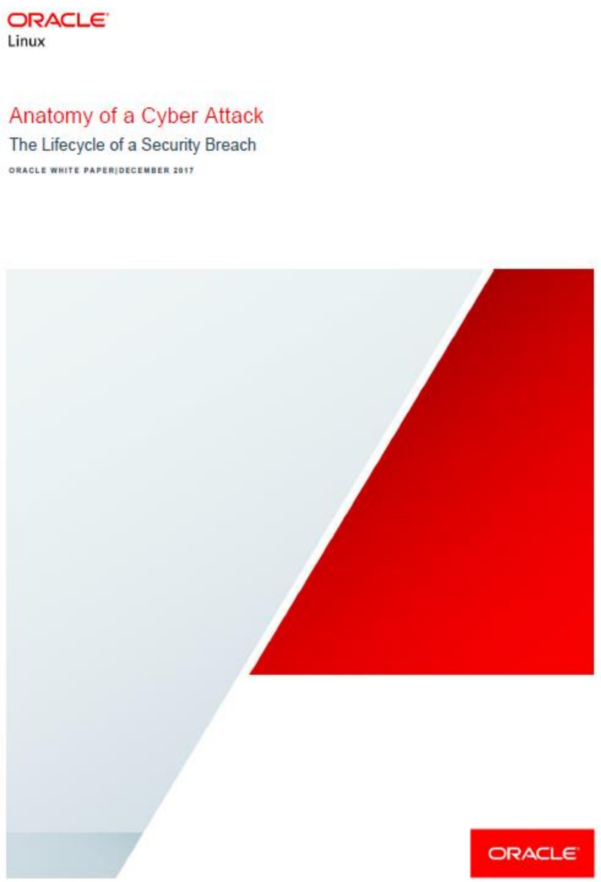
- The U.S. Government has announced a surprising move to secure power grids by using "retro" technologies. It comes after numerous attempts by foreign actors to launch cyberattacks on so-called critical national infrastructure (CNI).


US Electric Grid Hacked
Hackers could have taken actions to temporarily knock out power.

https://www.forbes.com/sites/kateoflahertyuk/2019/07/03/u-s-government-makes-surprise-move-to-secure-power-grid-from-cyber-attacks/#6d80412a3191

Cybercrime industrialized

- You can get someone’s complete health insurance data by paying $1,250.
- For just $7/hour, you can unleash a Distributed Denial of Service attack on your competition.
- You can purchase US Fulz records (someone’s identity, passport, SSN, and others). You can get all that for around $40.
- You can also get 10,000 fake Twitter followers for $15.
- And if you want access to a government server, that can be had for $6.
- You’re dealing with professional organizations that: Provide 24/7 customer service; Offer free trial attacks to demonstrate their prowess; Payment after the successful attack once you are satisfied with the results.
- The cost of cybercrime in 2016 is estimated to be around $445 billion, and it is predicted to increase to around $2 Trillion globally by 2019. 3 These estimates only include known attacks, not undetected cybercrime, industrial espionage, or state-sponsored attacks.



ORACLE
Linux

Anatomy of a Cyber Attack
The Lifecycle of a Security Breach
ORACLE WHITE PAPER|DECEMBER 2017

ORACLE

http://www.oracle.com/us/technologies/linux/anatomy-of-cyber-attacks-wp-4124673.pdf

Security is a culture!

Security = People + Process + Technology

Cybersecurity Hygiene.

Real time prevention.

Zero Trust

Secure your everything

Security by design.

Selling cyber security is hard.

Assume breach!

The best practices

- *Separate OT and IT*
- *Segmentation and traffic controls in ICS.*
- *Control networks divided into layers based on control function. (ANSI/ISA-99)*
- *Add hardware security appliance (PLC, DCS, RTU) instead of software*
- *Risk analyses. Permanent Audit and Pen tests.*
- *Improve security awareness on C-level*
- *Improve security awareness on industrial systems and operations (SCADA)*
- *Improve security awareness on industrial systems and operations (SCADA)*
- *Implement strong Security Policy*

- *Make Sure Network Security and Firewalls Are In Place*
- *Regularly Update Your Network Security Tools*
- *Establish a Incident Response Crisis Plan*
- *Cyber strategy and regulations for utility companies*
- ***Educate Your Employees***

INTRUSION DETECTION SYSTEMS

Active defense. Real-time threat detection and autonomous response

False positive vs False negative

AI, machine learning, data mining

Anomaly detection model

Misuse detection model

Q&A

Yugo Neumorni, EMBA, CISA

President, CIO Council Romania

CIO COUNCIL
Romania