Welcome to SANS ICS Europe 2019 Summit & Training
#SANSICS EUROPE
OT SECURITY REQUIREMENTS VS. REAL LIFE STORIES AND HOW TO COUPLE THIS TWO WORLDS
SO HOW IMPORTANT IS SECURITY WHEN IT COMES TO PRODUCTION FLOOR

After 14+ hours shift, trying to start 800MW unit for the 3rd time this day (with Plant Manager hanging over your shoulder) - guess where’s OT security on your priority list.
ICS SECURITY
LESSONS FROM THE FIELD

SECURITY INCIDENTS HAPPENS

DON’T UNDERESTIMATE „GETTING THE JOB DONE” ATTITUDE

THEY HIT THE BOTTOM LINE

WHEN IT GETS HOT, OT SECURITY IS ONE OF THE LAST CONCERNS
In everyday practice we use following standards to secure OT systems
• NIST
• ISA 62443
• COBIT
• ISO/IEC 27001
• …and more

WHEN IT COMES TO THE PLANT FLOOR IT’S ALL ABOUT GETTING THE JOB DONE

Now, try to explain it to average field-engineer-Joe.
ICS REQUIREMENTS VS. REAL WORLD EXPERIENCE

SOME SECURITY CONTROLS THAT HAVE MET THE PLANT REALITY
What says the requirement?

Protective and other ICS software is kept reasonably up to date and patched to reduce the risk of publicly known vulnerabilities existing in the system.

What about reality?

- Maintenance windows – rare and short
- Time and accessibility are limiting factors
- Maintenance usually doesn’t mean you can lose all your controls
- Validated patch doesn’t necessary means the same in vendors language
- Don’t fix a working thing approach
- OS’s and OT patches compatibility may be tricky
How to marry the two?

- Patching should be part of Management of Change process – evaluate the risk.
- Working with IT isn’t a bad idea
- Speak to your vendor to know the major pitfalls
- Automated patch deployment is a major improvement
- Test it first – test environments are a good-o
- Have a rollback plan no matter how trivial it seems
What says the requirement?

Network integrity is protected, incorporating network segregation where appropriate (e.g., ICS network is segregated from office IT network).

What about reality?

- When something works in the lab doesn’t mean it will work on site
- VLAN’s are used as a substitute of segmentation
- Industrial protocols are always a trouble
- ACL’s - „ANY ANY” for commissioning – usually means forever
- Cost and complication sometimes kills the idea
- This is our standard – that’s what vendors say
- Validation of actual needs
NETWORK SEGMENTATION
ROUTING, ACL’S, FIREWALLS RULES – THOSE ARE KILLING MY IEC61850! AND MY NTP…

How to marry the two?

• Plan it, test it, improve it – then implement

• Be reasonable – it’s OT – overkill is as bad as having no segmentation at all, but be sure you know and monitor the gaps

• Don’t think you can do it in one approach – limit allowed communication in small steps to see how much it can be narrowed

• Review your ACL’s and firewall rules from time to time, especially after any modification in the system structure and after maintenance or commissioning of any sort
REMOTE ACCESS

Hey, I need that LTE modem hanging in the cabinet! Oh, and ofc I need that admin account while I’m in!

What says the requirement?
Remote (i.e. originating from a different host than the one being accessed and usually located outside the ICS network, for example in the office network or external network) access is managed and avoided if feasible.

What about reality?

- Remote access is a daily practice
- If it’s not in the papers it doesn’t mean it’s not there
- It’s cheaper to connect remotely than to go to the site
- Full access to the system via remote connection
- Get the job done – engineers are good in finding solutions
REMOTE ACCESS
HEY, I NEED THAT LTE MODEM HANGING IN THE CABINET!
OH, AND OFC I NEED THAT ADMIN ACCOUNT!

How to marry the two?

• Don’t forbid it until really necessary – it’s usually leading to opposite results
• Control it instead – connect on demand, monitor sessions, disconnect on inactivity, MFA
• Assess the needs - allow only for what’s necessary while in remote connection
ENDPOINT PROTECTION
ARE YOU REALLY GOING TO SCAN MY 32GB USB FULL OF TREND FILES NOW? AND THAT FIREWALL KILLS MY OPC

What says the requirement?
Malicious code is detected. Applications communications should be controlled. Know your endpoints.

What about reality?

• AV definitions are not kept up to date
• Scanning removable media is automatically triggered but usually it’s possible to cancel the scan
• Windows firewall is usually the first thing to be switched off during commissioning
• Whitelisting may be troublemaker – especially after updates
• Asset inventory is a rare good
ENDPOINT PROTECTION
ARE YOU REALLY GOING TO SCAN MY 32GB USB FULL OF TREND FILES NOW? AND THAT FIREWALL KILLS MY OPC

How to marry the two?

• Check with vendor – sometimes this magical OT purposed definitions is nothing more than standard updates

• Not all at once – AV updated in groups starting with less critical assets

• Don’t allow external USB’s scanning to be cancelled – use alternative ways to move files if needed

• Admin rights are really not needed all the time

• AD is good – use it where you can
TAKEAWAY SUMMARY

• Make „an average Joe” aware

• Spending more time sometimes means loosing less money – design!

• OT myths are no longer true

• IT is not always that bad

• Make your requirements real but stick to them

• Assess your system – day to day ingenuity is surprising

• Don’t assume, check if there is a better way
Thank you for your attention!
Welcome to SANS ICS Europe 2019 Summit & Training

#SANSICS EUROPE