In a grid operator’s security trenches

From Comic Sans to Common Sense
Ing. Erwin Kooi, MSIT CISSP SCP RCX …

Information Security Architect at Alliander, IT Asset department

Primary focus on ICS and “new developments”

Background in healthcare IT and energy IT

erwin.kooi@alliander.com, PGP key 0x45914eee

Nerd creds: µControllers (AVR FTW!), 3D printing, FreeBSD, lockpicking, Club Mate, hedgehogs and no Oxford comma.

\[
\left((m_a)^{e_b}\right)^{d_b} \equiv (m_a)^{e_b \cdot d_b} \equiv (m_a)^{1 \mod(\varphi(n_b))} \equiv (m_a)^{1 + k \cdot \varphi(n_b)} \\
\equiv m_a \cdot (m_a)^{k \cdot \varphi(n_b)} \equiv m_a \cdot ((m_a)^{\varphi(n_b)})^k \equiv m_a \cdot (1)^k \\
\equiv m_a \mod(n_b)
\]
Rik van Hees

Information Security Architect at Alliander, IT Asset department

Primary focus on ICS and “new developments”

Background in substation automation and energy IT

rik.van.hees@alliander.com
Deploying advanced cybersecurity measures within next generation SCADA systems whilst preserving functionality, flexibility and integration with other systems.
What is security?

Alliander resilience vision*:

*Alliander is a resilient organization capable of anticipating and responding on a range or threats against her mission*

Alliander security mission:

*Protecting the mission of Alliander and her stakeholders by securing our crown jewels against (intentionally caused) damage through human actions*

* Underwriting the WEF resilience principles
Dynamic Developments

- Anticipation
- Monitoring
- Responding

Anticipation
- Knowledge (Proactive)

Attention
- Competence (Interactive)

Rational Response
- Resources (Reactive)
ISO27002:2013 - 13.1.3

Anyone?...
Segregation in networks

Control
Groups of information services, users and information systems should be segregated on networks.

Implementation guidance
One method of managing the security of large networks is to divide them into separate network domains. The domains can be chosen based on trust levels (e.g. public access domain, desktop domain, server domain), along organizational units (e.g. human resources, finance, marketing) or some combination (e.g. server domain connecting to multiple organizational units). The segregation can be done using either physically different networks or by using different logical networks (e.g. virtual private networking).
ISO27002:2013 - 13.1.3

So we went ahead and did it…

TL;DR
Good segmentation is much, much more than just adding a firewall

Ukraine-type attacks proved us right.

IT/OT integration: Share knowledge, not servers
NIST Smart Grid Framework 2.0
(simplified model, US centric)
Resilient households...
IT/OT Integration

Still 2 domains with integration on an information level, but

- No unsolicited connections into OT domain
- No direct Internet connectivity into OT domain
- No remote connectivity into OT domain, unless emergency.
  - Management of the domain is located within the domain
  - Also $vendor has to come on-site or it has to be life-and-death
  - Enforcement is done by separate team
- No dependency on other domains for mission-critical operation
- No unnecessary intra-domain communication
  - Zoning and sub-zoning
“Zoning” and “Siting”

Zoning: Build stand-alone supporting infrastructure and its processes
• Physical network (switches/routers/firewalls)
• Time synchronization
• Authentication/authorization
• Information exchange with IT
• Logging
• …

Siting: Place the applications in their new zones
• Telephony
• EMS/DMS
• Element managers
• …
Worst case scenario grid operation: “rebuild the grid from a cold start”

Which services are a must have? (we identified eight, they are in scope for OT)
• Identify dependencies on supporting infrastructure (are they still there or else add them to the pizza bottom)

Which services are a should have?
• Discuss if they should be included in the scope

Which services are a nice to have?
• Move them to the IT domain and build for degraded operation
Anticipate degradation
Anticipate degradation

Really grok what is important for your company:
- video streaming
- program guide
- account management (add/modify/delete)
- personalized program guide
- other stuff

Cut resources from less important components to support critical components.
And test every time, all the time.
Anticipate degradation

Simian Army Projects

- Chaos Monkey
- Chaos Gorilla
- Chaos Kong
- Janitor Monkey
- Doctor Monkey
- Compliance Monkey
- Latency Monkey
- Security Monkey
Anticipate degradation

Really grok what is important for grid operations: *

• Communication (telephony)
• SCADA (EMS)
• SCADA (DMS)
• (Security) monitoring
• Documentation
• …
• …
• Analytics
• Grid planning
• Other stuff

* this *will* change over time, so re-evaluate regularly…
Anticipate degradation

Business requirements for (real-time) OT data are growing
- SCADA on an iPad, why not?...

Store-and-forward principle with sufficient buffer storage between OT and IT

Management of OT domain must be done from within OT domain
- No remote control from IT domain
- Can have huge impact on current operations!
  - IT operations
  - Field service engineers
  - Security
The red button...
Defense in depth is much more than two firewalls by different vendors.

Defense in depth only works if you can detect someone breaching your layers.

“And only the middle window is in scope for the penetration test.”
SIEM installation 1.0

Console

- Processor
  - Flow
  - Log

IT DC 1 & 3

OT DC 1

OT DC 2
SIEM installation 2.0

- Console
- Processor
- Flow
- Log
- IDS Flow
- IT DC 1 & 3
- OT DC 1
- OT DC 2
Use cases

- Virus Detected
- Proces shutdown
- 104 traffic anomaly
- User created
- Unknown Device detected
- Successful Logon
- Login Failure
- Unusual Login
- ...
Added value for operations too
In previous presentations Erwin complained

- Default passwords
- Service backdoors
- “open” wireless connections
- Internet connections (basic hygiene)

- No secure design
- Underestimating the motivation of the attacker

- More than enough people writing policy (chiefs)
- Not enough people to implement and run it (indians)
- More than enough people telling me what’s wrong
Recap

If you don’t know where you’ll be going, how do you know when you get there?

- Set clear goals
- Allow flexibility in the journey (agile-ish approach)

Support at board level (CxO)

- Prioritize fundamentals (build pizza crust first with topping in mind)
- Cancel vital resources claims from other projects (like analytics)

Support at operation level

- Build a team (not an org chart)
- Listen and respect every member’s expertise and input (even if you do not agree)

Communicate why this is still a good idea (and then communicate some more)

- Ukraine incidents helped…
SO LONG
AND
THANKS FOR ALL THE FISH