Incident response in critical infrastructure

Margrete Raaum
margrete.raaum@kraftcert.no
Margrete.raaum@first.org
Protection vs readiness

• There is no such thing as absolute security
• Perimeter protection only takes you so far
• Key elements to meet the threats:
  • Continuous vulnerability assessment
  • Good detection capability
  • Incident response readiness
Why discussing with industry is difficult

• The perceived security level or threat picture is wrong
• Some do not seek help to avoid exposing themselves as less knowledgeable
• Some are afraid of regulators
• Some think discussing security issues attracts attackers
  • They do not actively attack in particular the ones who care about security
  • It is the internet, they will find you
Security capacity issues in companies

- This work requires highly specialized skill set that has to be maintained continuously.
- If there is not a continuous improvement internally, the overall level of security will drop.
- Considerations to be done in each company whether other companies be in the same situation, and is this grounds for cooperation?
What does it imply, being in the same situation?
Critical infrastructure - And threat actors

- Larger energy companies supply power to many
- Oil & gas is important to industry, the economy and private parties
- Healthcare – potentially direct loss of life
- Smaller utilities provide power to homes

Threat actors:
- Nation state actors
- Hacktivists
- Corporate espionage
- Theft/criminal activity
Same attack methods
Same threat actors
Same threat actors
Same threat actors
Same vulnerabilities
Security maturity
What now?

• What are we trying to protect?
• Against whom?
• Why do we prepare for the worst?
• How do we prepare?
• How much will this cost me and how mature do we have to be?
Physical consequences

• 2000: Vitek Boden let out millions of liters of sewage, polluting parks, rivers and buildings
• 2006: Gabriel Murillo and Kartik Patel removed 4 traffic light control boxes from the control grid
• 2008: Polish youth modifies remote control to perform track changes on the tram in Lodz
• 2014: German process industry attacked using APT, the blast furnace ended up in an undefined state
And Stuxnet of course

Malware especially designed to destroy Siemens systems

Nuclear power plant, not networked
This triggers our innermost fears

We cannot rely on feedback:

• What we see is not the reality (healthcare, energy, water, food)
• The commands you perform does something other than what it’s supposed to do
• Undefined states
• What kind of leaks are we protecting?
Sensitive information - sabotage
Sensitive business information
Sensitive marked information
Privacy-sensitive information
Critical services

• Cannot be taken offline
• Logging, audit or forensic activity cannot affect the system
• 1st priority is to get systems back online
  • Replace, overwrite, reset
• What if the problem already propagated?
• How important is finding root cause?
Security solution issues

- Sales people want to sell
- Open source is coming but resources are needed
- Who’s first
Asset control

• Where does the data flow
• What kind of data
• Which protocols
• How do you isolate an incident
  • In the critical part of the network
• Is the classification of criticality clear?
Logging in critical infrastructure

Without a timeline this makes no sense:

• The technician asks to change his phone number in the 2-factor authentication system
• Some PLCs become unavailable
• The technician is climbing the Kilimanjaro
• There is a non-functioning link in an email from a vendor
Some PLCs become unavailable

The technician is climbing the Kilimanjaro

The technician received an email and clicked a link

There is a non-functioning link in an email from a vendor

The technicians computer starts talking to an address in Germany

Email
Proxy and firewall
Vendor link
Technician’s machine - pcap

The technician asks to change his phone number in the 2-factor authentication system

Email systems
Support-logs
VPN-concentrator
Proxy and firewall
Technician’s machine

The new number was used to access the admin network

The technician logs onto the process control system

The technician logs onto the process network

VPN-concentrator
Proxies, firewall
Control system
Pcap, Network logs
Technician’s machine

Some PLCs become unavailable

Evidence:
Testimony/transcripts, logs pcap, forensic image from technician, vendor, control system
Tidiness

• What happened and why, how do we isolate it?
• Evidence and chain of custody
• How to store evidence
• Digital signing
• Working with legal departments
Readiness

• Knowing where the logs are and how to access them
• To be able to look at raw network traffic
• Basic forensic capability
• Keeping the toolbox up to date
• Knowing your network and whom to ask for assistance
The dedicated incident response team

- Incident handling will be done quick and consistent
- Avoiding costly mistakes
- The team knows what to do and whom to inform
- They gain control
- The defuse the situation internally and with partners or customers
- They break down the silos
- The ensure learning and provide material for regulator reports
Tying it all together across borders

- We can share
  - Attack patterns
  - Target trends
  - Adversary intelligence
  - Vulnerabilities

- We can join forces in assessing the real threat presented by specific vulnerabilities or attacks

- If all are to do this, there will be a lot of overhead
Building a robust network

- Large variations in company size and level of competence
- Larger actors
  - Can be a resource to the others in the sector
  - Can have done investments that can benefit all
  - Can initiate and demonstrate the benefits of information sharing
  - Will also learn from participating
- We hoped that a sector based CERT would facilitate a trusted environment
- Bring the smaller actors are brought up to a level where they can to a larger degree collaborate well with the large actors
It is all about trust

• Private non-profit or public support
• Voluntary vs mandatory
  • Mandatory is not trust based, less likely to increase information sharing
• Hierarchical networks
  • Data ownership
  • Delay
  • Sector specific challenges and competence
• Smaller and more homogeneous constituency:
  • Makes it easier to agree on mandate and services
  • Makes it easier to achieve acceptance for extra cost