Building CERT Team in the Large Energy Company

MIROSŁAW MAJ
Cybersecurity Foundation
ComCERT.PL
Building CERT Team in the Large Energa Company

MIROSŁAW MAJ
Cybersecurity Foundation
ComCERT.PL
Agenda

#Background

#Methodology

#Challenges

#BestPractices
#Background

#Methodology

#Challenges

#BestPractices
Background

- Energy Sector in Poland
- The object is one of the companies
- Initial interest in having IRT
- CERT Energa
Background

- National Critical Infrastructure Protection Programme
- Recommendation 2.8.2.10
  - To establish CERT
Background

- Incidents
- Only ICT domain
- Malware
- Phishing both sides
- Targeted attacks
- "Twitter" stock exchange attacks
- Not recognized OT domain
#Background

#Methodology

#Challenges

#BestPractices
# Background

# Methodology

# Challenges

# Best Practices
Methodology

CERT SERVICES

**Reactive Services**
- Alerts and Warnings
- Incident Handling
- Vulnerability Handling
- Artifact Handling

**Proactive Services**
- Announcements
- Technology Watch
- Security Audits or Assessments
- Configuration and Maintenance of Security Tools, Applications and Infrastructure
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

**Security Quality Management Services**
- Risk Analysis
- Business Continuity and Disaster Recovery Planning
- Security Consulting
- Awareness Building
- Education Training
- Product Evaluation or Certification
Methodology
8 steps by CERT/CC

STEP 1
Obtain Management Support and Buy-In

STEP 2

STEP 3

STEP 4

STEP 5

STEP 6

STEP 7

STEP 8
Methodology

- ENISA Good Practice Guide for Incident Management
Methodology
Methodology

- SIM3 - Security Incident Management Maturity Model
# Background

# Methodology

# Challenges

# Best Practices
#Background

#Methodology

#Challenges

#BestPractices
Challange #1
Formal regulatory mess

- Personal data protection
- Classified information
  - State level
  - Company level
- National Cybersecurity Policy
- National Strategic Plan For Protecting Critical Infrastructure
Challenge #2
Documentation

• Different documentation in all companies
• A lot of documents
• Inconsistency
• No clear rules about incident reporting schema
• In fact – many changes needed

Picture: http://rcmguy.com/
Challenge #3
Heterogeneous ICT environment

- ICT
- OT
  - Various ICS systems
  - Outsourcing
  - Remote access
- 2 SIEMs
- 2 SOCs (?)/NOCs
- 2 Teams
Challange #4
Distributed security roles

- ENERGA
  - RISK AND SYSTEM SECURITY DEPT
    - ICT SERVICES
      - IT DEPT
        - IT SECURITY TEAM
          - CRISIS MGMT TEAM FOR SECURITY AND ASSETS
  - ICS SERVICES
    - RISK AND SYSTEM SECURITY OFFICE
    - IT DEPT
  - ENERGA DISTRIBUTION
    - IT DEPT
  - ENERGA PRODUCTION
    - IT COORDINATOR
      - INFORMATION SECURITY DIRECTOR
      - OUTSOURCING COMPANIES
Challange #5
Internal politics

• The first question was:
  • Where in the organizational structure the CERT will be situated?
#Background

#Methodology

#Challenges

#BestPractices
#Background

#Methodology

#Challenges

#BestPractices
Best Practice #1
Use their knowledge about crisis management

• They work in crisis management situations almost all the time
• Recognize the existing processes and try to find specific things for cybersecurity
Best Practice #2
Ensure ICT and OT technical competences

- Do not build only coordination center without technical knowledge
- You do not need your technical knowledge operationally but you must understand to incident and have common language and esteem for technical partners
- Ensure access to technical tools – e.g. SIEM
- Do not propose IPS in OT environment
- Make simple port scanning

Picture: http://tenabla.com/
Best Practice #3
CSIRT SERVICES are your foundations

- You learn the organization
- They learn a CERT concept
- Make a survey

What services do you serve?
What services you would like to serve?
What services your constituency need?
Best Practice #4
Work with workflows

- In sophisticated organizational structure this is the best to identify parties and tasks
- Take main types of incidents and work with them
- Use graphics rather than text
Best Practice #5
Recognize a structure of regulations

- Use an umbrella document to introduce CERT in the organization
- Focus on regulations relate to incident response but not the whole security
  - Find existing regulations
  - Add regulations
- Try to put CERT as high as possible
  - Separation of IT and CERT -> MUST
  - Separation of IT security and CERT -> recommended
Best Practice #6
Use this time to introduce metrics

- Number of incidents
- Classification
- Reaction times
- etc

<table>
<thead>
<tr>
<th>Incident Class (remaining type field)</th>
<th>Incident Type (remaining but ignored type field)</th>
<th>Description / Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intrusions</td>
<td>Privileged account compromise</td>
<td>A successful compromise of a system or application (service). This can have been caused remotely by a known or new vulnerability, but also by unauthorized local access.</td>
</tr>
<tr>
<td></td>
<td>Unprivileged account compromise</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Application compromise</td>
<td></td>
</tr>
<tr>
<td>Availability</td>
<td>DoS</td>
<td>In this kind of an attack a system is bombarded with so many packets that the operations are delayed or the system crashes. Examples of a remote DoS are SYN- a, PING- flooding or e-mail bombing (DoSs: TN, Trinity, etc.). However, availability can also be affected by local actions (destruction, disruption of power supply, etc.).</td>
</tr>
<tr>
<td></td>
<td>Sabotage</td>
<td></td>
</tr>
<tr>
<td>Information Security</td>
<td>Unauthorised access to information</td>
<td>Besides local abuse of data and systems, the security of information can be endangered by successful compromise of an account or application. In addition, attacks that intercept and access information during transmission (eavesdropping, spoofing or hijacking) are possible.</td>
</tr>
<tr>
<td></td>
<td>Unauthorised modification of information</td>
<td>Besides local abuse of data and systems, the security of information can be endangered by successful compromise of an account or application. In addition, attacks that intercept and access information during transmission (eavesdropping, spoofing or hijacking) are possible.</td>
</tr>
<tr>
<td>Fraud</td>
<td>Unauthorised use of resources</td>
<td>Using resources for unauthorized purposes including profit-making ventures (eg, the use of e-mail to participate in illegal profit chain letters or pyramid schemes)</td>
</tr>
<tr>
<td></td>
<td>Copyright</td>
<td>Selling or installing copies of unlicensed commercial software or other copyright protected materials (Warez)</td>
</tr>
<tr>
<td></td>
<td>Masquerade</td>
<td>Types of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it</td>
</tr>
<tr>
<td>Other</td>
<td>All incidents which do not fit in one of the given categories should be put into this class.</td>
<td>If the number of incidents in this category increases, it is an indicator that the classification scheme must be revised.</td>
</tr>
</tbody>
</table>
Best Practice #7
Keep asking and implement answers

• Prepare the final document backbone at the very beginning and feed it with your findings all the time
• Give an open access to your partners at organization side
• Document all Q&A as the special chapter
• Start your project diary
Best Practice #8
Have friends of your idea

• Tell nice stories about CERT
• Inspire by the picture of future CERT in the organization
Best Practice #9
Avoid politics

• Just listen to them

• Do not change your pragmatic plan

• Do not write the most important document yourself
  • They will do it better
  • They know the organization wording
  • They will learn more about what they are building
Best Practice #10
Build the external contacts

- Build the external contacts from the very beginning
  - Sectorial
  - Country level
  - International level
- Explain how these communities work
- Start to share information – having live cases during the process only can help you
Best Practice #11
Understand the organization

Beer Trusted Party 😊
Thank you!

Questions?

miroslaw.maj@cybsecurity.org
miroslaw.maj@comcert.pl