Assess and improve SCADA security in the Dutch Drinking Water sector

Eric Luijff, Manou Ali and Annemarie Zielstra

Outline

• Background
  • NICC
  • Dutch drinking water sector

• SCADA (in)security – an issue?
  • investigative approach
  • results
  • development of SCADA good practices

• Next steps by NICC

• Questions
NICC: National Infrastructure against Cyber Crime

- Public-Private Partnership for CIIP
- CPNI 'flower' model with 'sector petals'
  - financial, drinking water, energy
  - mainports, (petro)chemical industry
  - multi-nationals / manufacturing
  - …
- NICC kernel
  - round-table support
  - info exchange sector - police - justice - GovCert.nl - intelligence services
  - initiates projects + thematic meetings
- cross-cutting themes
  - SCADA information security

Dutch drinking water sector

- 1950
  - 200+ municipality-oriented companies
- 2008
  - nine regional-based companies and one municipal company
Drinking water and SCADA security

- Drinking water sector petal
  - put SCADA security on top of its meeting agenda
  - wanted its SCADA security posture investigated

- TNO
  - developed questionnaire
  - NICC did interviews
  - processed answers in an anonymous way
    - sector-wide analysis
    - organisation-specific security posture marks

- development of SCADA Good Practices for the sector

SCADA information security questionnaire

- Open and closed questions covering three areas
  1. SCADA security policies
     (in relation to general company security policies)
     - 15 questions, e.g. ISO 17799, risk analysis, acquisition, ..
  2. SCADA network architecture
     - 14 questions, e.g. office network, external and remote links
  3. SCADA system management
     - 10 questions, e.g. patching, virus, 3rd party access

*English questionnaire blueprint obtainable through your Euro-SCSIE contact*
Protect company data privacy

• Data entered in spreadsheet in 'company-x' column where x is randomly assigned

• All mappings of company-x with real company are stored in a vault
  • single sheet of paper with 10 names – 10 values x (1..10)
  • original questionnaire replies

Reporting mechanism

• NICC Confidential / Drinking Water sector - eyes only report
  • discusses all implications of
    • sector-wide answers per question or combination of questions
    • risky behaviour (with explanation)

Next slides are based on artificial data to protect company / national sensitive information
Reporting mechanisms (2)

Question 14: LAN architecture

• Mixed process control and office automation networks are globally considered a bad design as unwanted loss of the SCADA integrity and control may occur [one company].
• VLANs sharing same physical network resources may have the risk of loss of control due to overloaded VLAN boxes due to e.g. a virus or bad NIC in office environment. Using this option regularly requires stress testing in a controlled environment [5 companies].
• Physically isolation SCADA networks is the best design [4 companies of which one is moving to VLANs]

Reporting mechanisms (3) – benchmarking

• Sector level benchmark – school mark approach
  • SCADA security policies
  • SCADA network architecture
  • SCADA system management
  • sector average and worst in class performances per key issue
  • sector-wide “school report” showing all organisation-x results
• For each individual organisations
  • results compared to sector average
  • presented in closed envelop to protect the company privacy
Experts established the security posture weights

- Weights for possible state of each key issue (based upon average value by three experts)

<table>
<thead>
<tr>
<th>PA – OA linked</th>
<th>100%</th>
<th>70%</th>
<th>20%</th>
<th>10%</th>
<th>0%</th>
</tr>
</thead>
<tbody>
<tr>
<td>modems</td>
<td>100%</td>
<td>90%</td>
<td>50%</td>
<td>N/A</td>
<td>0%</td>
</tr>
</tbody>
</table>

- Relative weights of the 5 - 6 key issues within a category (policies, network architecture, system management) to establish a ‘school mark’ 0 .. 10

- Final score = average all three categories

SCADA policies (example)
Main security issues - policies

- SCADA is not part of
  - business risk analysis
  - EDP audit process

- No specific SCADA security policies extending ISO/IEC 17799

- Security awareness is lacking in SCADA environment

- No security requirements in acquisition

- No priority delivery arrangements with SCADA vendors
Main security issues - networking

- SCADA security reference architectures and reality
  - room for improvement ..
- Office and SCADA data streams share low bandwidth links
- Control over Internet and GPRS (GSM data channel)

Main security issues – system management

- Worries about 3rd party to introduce a virus
  - but 3rd party engineer connects laptop just straight on
  - three-monthly signature updates if any …
- Patching
  - vendors sometimes have to press to apply patches
  - vice-versa: do not install patches if you want support
- Passwords
  - unchanged factory defaults
  - group passwords
  - change frequency = infinity
  - unchanged passwords after people leave
SCADA Security Good Practices

- 39 good practices were developed
  - based on findings from questionnaires
  - 11 address CIO/CSO level; 28 technical management level

- Dutch classified version explains each GP and current sector state
- downloadable English version

www.samentegencybercrime.nl
www.tno.nl

Next steps by NICC

- Same questionnaire and analysis used for Dutch Energy sector

- Comparison Drinking Water – Energy SCADA is on-going
  - scary SCADA risk taken on a day-to-day basis by utilities!

  - get CIOs involved
    - towards agenda setting
    - sharing SCADA incidents
    - ...

www.tno.nl
To conclude

- Sector self-assessment works! Truthful responses if trust exists
- Individual company data privacy of utmost importance
- Benchmarking and ‘school reports’ allow sector-wide communication
- Major steps taken in securing the Dutch drinking water sector
- NICC goes forward with securing all critical SCADA sectors

Questions?

eric.luijff@tno.nl