Outline

• Background
  • NICC thematic area Process Control

• Benchmark approach
  • SCADA (in)security issues
  • analysis method
  • from results to managed risk and cross-sector actions

• Questions
National Infrastructure against Cybercrime

- The drinking water sector petal of the NICC put SCADA security on its agenda early 2007

- Decision to use a simple, fast investigative approach across the sector
  - questionnaire
  - anonymous sector-wide analysis
  - in 2008, same quick-scan benchmark in the energy sector

- In 2010, benchmarks were repeated in both sectors
  - comparison with previous benchmark per sector
  - comparison between sectors per risk issue

SCADA (in)security issues

Literature analysis led to simple questionnaire addressing
- Policy area
  - written policy, relation with IT, responsibilities
  - awareness, audits, business continuity
  - procurement …

- SCADA networking architecture area
  - office - SCADA network separation, remote access, modems …

- SCADA system management area
  - passwords, patching, antivirus
  - 3rd party access …
SCADA information security questionnaire

Open and closed questions covering
1. 15 questions on SCADA security policies in relation to general company policies
2. 14 questions on SCADA network architecture area
3. 10 questions on SCADA system management
   - 2010 questionnaire has some additional open questions
   - some questions validate truthiness of answers (e.g., top 5 worries)

Analysis phase - protect company data privacy

- Data entered in a spreadsheet column ‘sector-x company-y’ where y is randomly assigned
- Lock-up in some vault …
  - company-y mapping to the real company name
  - original questionnaire replies
Analysis reporting mechanism

- **TLP AMBER/sector specific** - 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 VLAN soon]
Reporting mechanisms (3)

- Sector-wide security posture – school mark approach
  - vector diagrams showing sector-wide security posture
    (average and worst in class per security indicator)
  - SCADA security policies
  - SCADA network architecture
  - SCADA system management
  - using expert derived weights

- Sector-wide “school report” showing all organisation-y results

SCADA policies (example)
Reporting mechanisms (5)

- For each individual organisation
  - vector diagrams showing security posture
    (relative to sector averages and maximum score)
  
- handed over in closed envelop to protect the company privacy
Main SCADA security issues

- SCADA not in business risk analysis / EDP audit processes
- Insufficient SCADA specific security policies
- SCADA security awareness weak
- Procurement – *improving (e.g., WIB-standard)*
- Remote access not in control
- 3rd party access
- Patch & antivirus
- Password management

- Very risky
  - mixed office – SCADA networks
  - default passwords 1234

- SCADA SECURITY INCIDENTS OCCUR!

Cross-sector comparisons

- SLIDE TO BE PRESENTED NOT FOR PUBLICATION
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
- Cross-sector analysis towards security improvement activities
- Full paper in next issue Int’l J. of Critical Infrastructure Protection

Questions?

eric.luijijf@tno.nl
A flying wheel in motion:
SCADA Security Good Practices

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

- downloadable English version
  
  www.samentegencybercrime.nl
  www.tno.nl

- Japanese and Italian translations available