



# Digibewust unites vital industries against ICT failure

Thijs Kout  
WIB mini-seminar  
April 26, Sofitel, The Hague

Platform voor eNederland



## Agenda

- Critical Infrastructure Protection
- Telecommunications/ICT
- SCADA
- National Platform Continuity Vital ICT

Platform voor eNederland

# ECP.NL , Platform for eNederland

- Founded: 1997
- Goal: promotion of the information-economy and -society
- 150 participants: private, public
- Board: chairman Roger van Boxtel
- Advisory Board (2004)
- Team: 16 fte
- Active participants!

Platform voor eNederland



## ECP.NL: Vision and Mission

In the information society electronic communication (*e-business, e-government, e-health ..*) is an important strategic issue.

ECP.NL sets the agenda for relevant obstacles for the digital economy and society, and helps to overcome them, from her unique and neutral position between market and policy.

Platform voor eNederland

# Agenda

- Critical Infrastructure Protection
- Telecommunications/ICT
- SCADA
- National Platform Continuity Vital ICT

## Critical Infrastructure Protection I

2001: Dutch Parliament requested government to draw-up a cross sector approach for the protection of critical infrastructure

2002: start CIP project; 3 aims:

- To prevent large scale failure or disruption
- To ensure public and private sectors are adequately prepared for the consequences of failure or disruption
- To allow effective repressive measures to be taken in order to diminish damage caused by failure or disruption



## Critical Infrastructure Protection II

Quick-scan classifying 12 critical sectors:

- Energy
- Telecommunications and ICT
- Drinking Water Supply
- Food
- Health Care
- Finance
- Surface Water Stemming and Management
- Public Order and Safety
- Legal Order
- Public Administration
- Transport
- Chemistry and Nuclear

Platform voor eNederland



## Critical Infrastructure Protection III

2005: project output:

- Confidential sector reports
- Current level of protection is reasonable well
- The acceptability of residual risks is important
- In some sectors additional measures are taken
- Vulnerabilities between sectors
- Foundation of a Critical Infrastructure Strategic Consultation Group (SOVI)
- The importance of a European approach

Platform voor eNederland

## Critical Infrastructure Protection IV

Three remaining issues:

- Insufficient clarity about the necessary level of security for critical infrastructure
- The availability of ‘knowledge and expertise’ in the area of security is too limited
- There is a gap in the way in which private and public parties attune their security effort to one another.

## Agenda

- Critical Infrastructure Protection
- Telecommunications/ICT
- SCADA
- National Platform Continuity Vital ICT



## Telecommunications/ICT

- Highly dependent on critical sectors ‘energy’ and ‘stemming and managing surface water’
- The Telecommunications Act provides a proper basis for continuity: NACOTEL
- Programs like KWINT (vulnerability on the Internet), Safe Surfing (Surf op Safe) and Digibewust are increasing the awareness for internet vulnerabilities for public and private internet use
- The foundation of the National Platform Continuity of Vital ICT will raise awareness and solutions for ICT failure within vital industries in the Netherlands

Platform voor eNederland



## Agenda

- Critical Infrastructure Protection
- Telecommunications/ICT
- **SCADA**
- National Platform Continuity Vital ICT

Platform voor eNederland

# SCADA I

## **Supervisory Control and Data Acquisition:**

- The total process of automation, electronics and ICT, that will be used for:
  - Monitoring (supervisory)
  - Manage and control processes
  - Acquisition of data
- Process Control Systems:
  - Distributed Control Systems (DCS)
  - Energy Management Systems (DCS/EMS)
  - Programmable Logic Controller / Remote Terminal Units

# SCADA II

## **SCADA in the vital infrastructure:**

- Electricity
- Drinking Water Supply
- Food & Medicine
- Surface Water Stemming and Management
- Public Order and Safety
- Public Administration
- Transport
- Chemistry / Nuclear

## SCADA III

It is relatively easy to enter vital SCADA-systems:

- Via public networks
- Via business / corporate networks

SCADA Security:

- Technical
- Physical
- Organizational

## SCADA IV

Incidents:

- 1998: GazProm
- 1999: nuclear installation UK
- 2000: drinking water, Australia
- 2001: 18 intrusions within 18 energy suppliers in the UK
- 2003: US nuclear power plant, train
- 2004/05: Several attacks energy sector, US

## SCADA V

### International:

- Growing issue
- Lots of initiatives
- Not many international contacts.....
- No co-ordination
- Do we have a problem?

## National Platform Continuity Vital ICT

- Founded: 2006 April 25
- Goal: sharing best practices
- Confidential
- Members: large companies in sectors energy, transport, telecommunications, banking



## Questions? / Discussion!



Platform voor eNederland