# Establishing a Centre for Information Security:

## *Experiences from the Trial Period and Recommendations to Similar Initiatives*

Lillian Røstad and Maria Bartnes Line

SINTEF ICT

Trondheim, Norway

# Contents

- The Norwegian Centre for Information Security (NorSIS) 2002-2005
  - Background
  - Operation
  - Challenges
  - Recommendations

# The Norwegian Centre for Information Security (SIS)

- Initially a trial project
  - 2002-2004
  - http://www.norsis.no

- Trial period prolonged until the end of 2005
  - While the government debated a decision…

- NorSIS permanently established January 1st 2006
  - Name changed to correspond with web-address
  - New location, new people
  - New mandate

# Background

- Main goals:
  - To provide an overview of threats towards Norwegian ICT systems
  - To obtain and share information, expertise and knowledge about possible threats and relevant countermeasures
  - Establish contact and cooperation with organisations providing similar services in other countries
- In the longer term:

  Responsibility for national coordination of

  incident reporting, warning, analysis and exchange of experience

  related to threat against ICT systems

# SIS target audience

- Initially:
  - Commercial companies and government departments, regardless of size
  - National security authorities, who could benefit from utilizing information from SIS
  - Politicians and others who could utilize the information as a basis for considerations about the state of security in society
- In the end:
  - Focus shifted to small and medium-sized enterprises (SMEs)

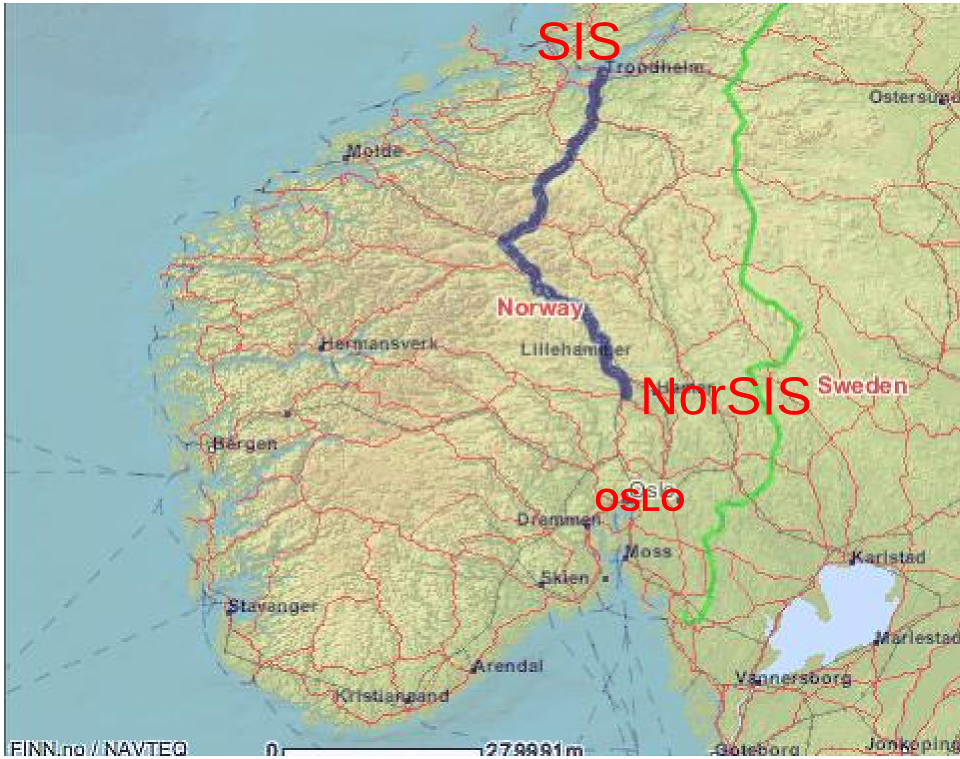
# Conundrum…

- SIS was supposed to be a supplement to existing efforts
  - Not to overlap or assume responsibility assigned to anyone else
  - Responsibility for information security in Norway was (and still is) scattered among several ministries
    - Defence
    - Legal
    - Communication
    - Trade & industry (main sponsor of SIS)
  - Result: SIS had no formal responsibility or authority
  - Goal of trial period: decide how SIS could best co-exist with existing efforts
  - Now: The information security coordination council (KIS) added…

# Geography & resources

- SIS located in Trondheim
  - SINTEF, UNINETT and NTNU
  - Approx 5 full-time positions
  - Fully government funded

- NorSIS located at Gjøvik
  - Gjøvik University College
  - BlueLight
  - Approx 4 full-time positions
  - Government + private funding



# Operation

- Information gathering
- Information sharing
- International cooperation

# Information gathering

- What information did SIS need?
  - Attacks
  - Vulnerabilities
  - Exploits
  - Incident reports

- How to get that information?
  - Public/open
  - Closed

# Information gathering: difficulties

- Gathering incident reports…
  - Established trust and personal relationships
  - The real issue:
    - needed to demonstrate return on investment
- Solution
  - Informal information gathering
    - Participating in existing networks and informal forums
  - Establishing information sharing groups
    - Within business sectors
    - Regular meetings

# Information sharing

- Target audience:
  - Almost everyone..
- Means of communication
  - Web site and mailing lists
  - Information sharing groups
  - Presentations and speeches
  - Participating in work groups
    - National and international

# Information sharing: web and mail

- www.norsis.no
  - Threat reports
  - Advisories
  - Monthly reports
  - Alerts
  - News
- Mailing lists
  - Alerts – threats and vulnerabilities
  - News – relevant information and events

# Information sharing groups

- Specific to business sectors
  - Transportation
  - Financial
  - Energy
  - Oil
  - IT
  - Research and education
  - Local government (municipals)
  - ..
- Some new – some existing
- Regular meetings facilitated by SIS
  - Hosted by the participating organizations
  - Approx 8-12 people
  - Focus on common problem
    - Presentations
    - Informal discussion

# Information sharing: presentation and speeches

- At professional conferences

- At universities and colleges

- A vide variety of topics related to information security
  - Threat assessment
  - Wireless security, security culture, awareness training, secure software, malware….

- Mainly national, but also some international conferences
  - TERENA 2003
  - FIRST 2004

# Information sharing: participation in work groups

- National survey on the underreporting of crime in Norway
  - 2003
  - 2006 (NorSIS)
- Public information security portal (NettVett)
- Research project on protection of national critical information infrastructure
- Establishing an annual conference on ICT security

# International cooperation

- Established a Nordic CERT cooperation network
  - Norway, Sweden, Denmark, Finland, Iceland
  - The Nordic CERT forum
  - Annual meetings
- Attended FIRST conference and some TF-CSIRT meetings
  - UNINETT is a member of FIRST
- SIS staff attended the TRANSITS course for training of computer incident response teams (CSIRT)
- Visited
  - NISCC/UNIRAS
  - US-CERT

# Main challenges – and recommendations

- Challenges:
  - Information gathering
  - National coordination of efforts
  - Critical infrastructure and responsibility
  - An ever-changing mandate
  - Lack of long-term planning

- Recommendations:
  - Need sufficient backing and stable conditions
  - CERT activities should be included
  - Need clearly defined authority

# Questions?