Experiences from establishing a national Centre for Information Security in Norway

Lillian Røstad & Maria Bartnes Dahl
Centre for Information Security, SINTEF Telecom and Informatics
S.P. Andersens vei 15, 7465 Trondheim, Norway
lillian.rostad@sintef.no, maria.b.dahl@sintef.no

December 2002

Keywords: information security, national strategy, incident reporting

Today, the society increasingly depends on information and communication technology (ICT). This leads to greater vulnerability in information systems, both to intended and unintended incidents. Secure and robust computer systems and networks are a necessity for trade, government administration and private individuals to utilize available technology for productivity and economic gains.

In June 2002, The Vulnerability Committee published a report recommending a strategy for reducing the vulnerability within Norwegian ICT systems. As part of this strategy, the establishment of a national centre for ICT security was suggested. Therefore, the Ministry of Trade and Industry commissioned the Centre for Information Security (SIS) as a three-year pilot project starting April 1st, 2002. The aim of the project is to establish a centre, which in the longer term may be responsible for national coordination of incident reporting, alerting, incident tendency analysis, and exchange of experiences related to threats towards ICT systems.

One of the main tasks of the Centre for Information Security (SIS) is to coordinate activities related to ICT security in Norway. The centre receives reports about security related incidents from companies and agencies, both private and governmental, and is working on obtaining and providing an overview of threats towards Norwegian ICT systems based on these reports.

The main activities of SIS include the following:

- obtain and provide an overview of threats towards Norwegian ICT systems.
- ?spread information, expertise, and knowledge about possible threats and relevant countermeasures.
- establish contact and cooperation with organizations providing similar services in other countries.

The target groups of SIS are:

- ?companies and agencies.
- security authorities, who can utilize the information for their own analysis.
- politicians and others who can utilize the information as a basis for considerations about the state of security in the society.

The centre has no official authority. The functions of the centre will be a supplement to those activities already in place in the area of information security in Norway. In the trial period, the centre is not intended to have responsibility regarding ICT security in emergency situations.

Similar activities can be found in other countries as well – some are well established while others are just starting up. In Sweden and Denmark they are planning similar activities to what we are doing in Norway. In the United Kingdom the Unified Incident Reporting and Alert Scheme (UNIRAS) was established as early as in 1992. The National Infrastructure Protection Center (NIPC) in USA was established in 1999.
SIS is hoping to establish close relationships with the other Nordic centres. The main goal is to be able to exchange information about ICT-security related incidents, and also to learn from each others experiences.

The Centre for Information Security is located at SINTEF Telecom and Informatics in Trondheim. SINTEF is the largest independent research organization in Norway. The reasons why SIS is located here, include the close relationship between SINTEF and the Norwegian University of Science and Technology (NTNU). Furthermore, SIS' main activities depend on the close relationship with UNINETT, which is also situated in Trondheim. UNINETT is the company which manages the academic networks in Norway, that is, the networks between academic and research institutions. They have a computer emergency response team (CERT), and can contribute with unique knowledge and experience to SIS. One person from UNINETT also works for SIS.

The choice of placing SIS at an independent, private organization, and not at a public agency, was deliberately made. One reason is that companies often refuse to report about security related incidents to governmental instances. Secondly, in present constitution, SIS does not have to report anything the Norwegian Economic Crime Unit (ØKOKRIM), the national authority for investigation of computer crime. Also, there were divided opinions on how SIS may end up after 2004. Placing it at an independent organization would leave all possibilities open until then. Then, there were the question of who could offer the best professional basis for this kind of project, and SINTEF was chosen to be the host for SIS.

The main challenge for a new establishment like SIS is to gain trust from its target groups. If this does not succeed, the centre has no chance of surviving because nobody will rely on it to be a national coordination centre. All information related to computer security incidents is sensitive, and nobody gives out such information without trusting the receiver.