Royal Norwegian Ministry of Government and Reform
Royal Norwegian Ministry of Justice and the Police
Royal Norwegian Ministry of Defence
Royal Norwegian Ministry of Transport and Communications

Guidelines

National Guidelines on Information Security 2007 – 2010

Preface

We live in an information and media society, and over the last few years we have become more and more dependent on ICT (Information and Communication Technology). The Internet has become more important, both nationally and internationally, for trade, industry and commerce, both for the Government and the individual user. Electronic interaction is expanding, and often the information exchanged can be defined as sensitive for the companies concerned.

Malfunction in the ICT infrastructure can cause grave consequences for an enterprise, a sector, or for an entire society. Consequently, it is very important that we are aware of the potential risks and vulnerabilities, and the importance of continuous work to prevent failures in the ICT infrastructure.

Information security is not only related to the creation of secure technical systems. It is of significant importance that we also are well aware of the sharing of responsibility, and that approved routines and plans for the ICT security are being continuously reinforced.

Information security implies a total approach when it comes to the decision and introduction of technical safety equipments, making the individual person responsible trough awareness, knowledge, education and training in safety measures. Information security is an administrative responsibility. The foundation for a well-organised plan on information security in the various enterprises, whether it is a private, governmental, or a municipal enterprise, depends upon the management being aware that well-functioning ICT infrastructure is a crucial factor when it comes to fulfilling their goal achivemments.

When everything is "running smoothly" in a business, and has done so for a while, it can be a challenge in many cases to get the management to give priority to security and safety precautions – until a disaster happens. Suddenly, many unanswered questions arise. For example: What kind of shared information is administered by the enterprise? Where is it stored? What is the value of this information? What happens if critical information is lost or compromised?

These guidelines have been devised to describe the growth trends within information security, and the challenge they involve. The guidelines also pinpoint the Norwegian priority areas that can meet these challenges. The document is also meant to be a contribution to create a general awareness of information security at management levels in enterprises. In this way, we can together, strengthen Norway's information security.

Oslo, December 2007

Heidi Grande-Røys
Minister of Government Administration and Reform

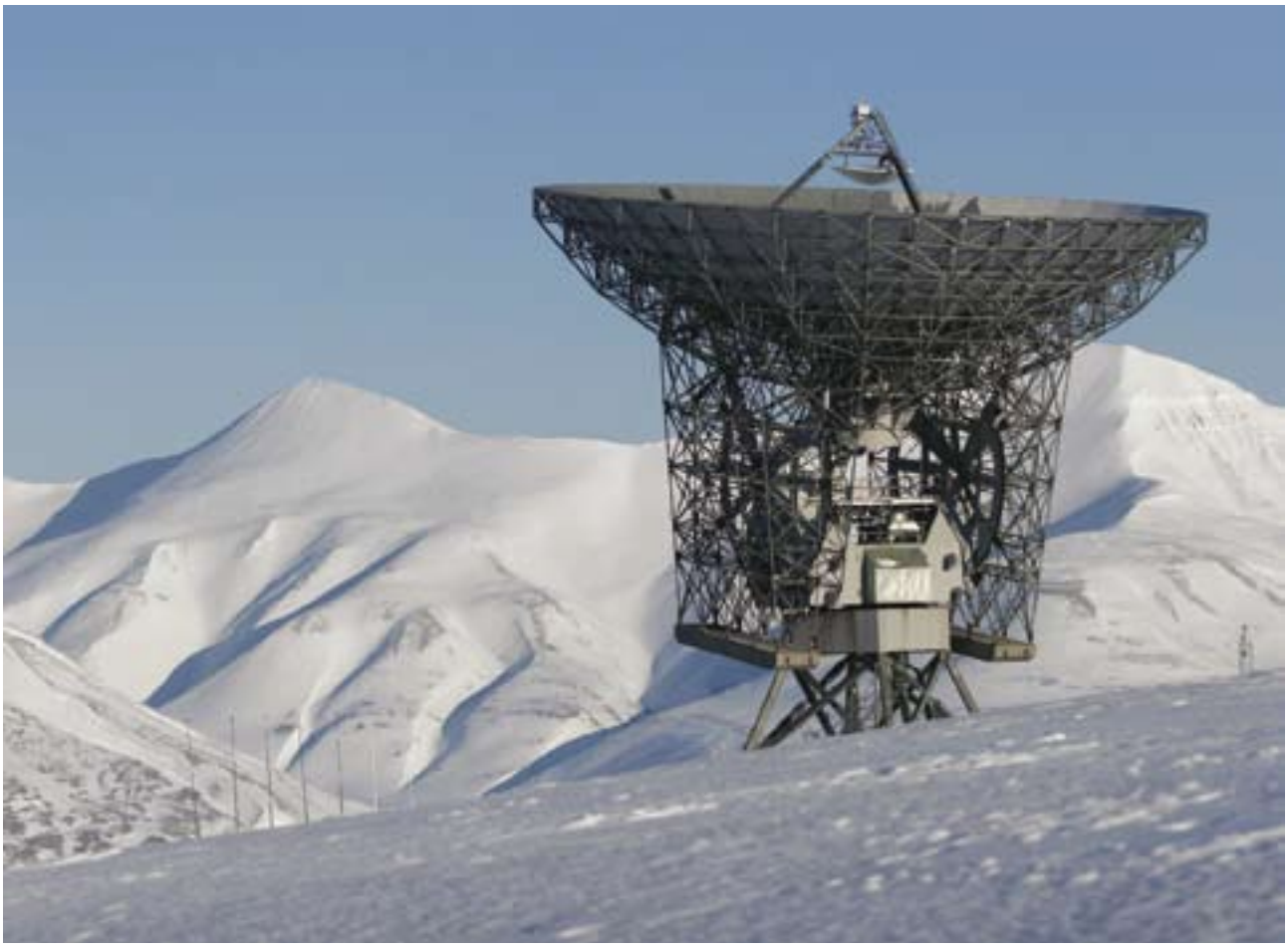
Liv Signe Navarsete
Minister of Transport and Communications

Anne Grete Strøm-Erichsen
Minister of Defence

Knut Storberget
Minister of Justice

National guidelines on information security 2007 – 2010

1 Introduction



© Fredrik Naumann/Samfoto

1.1 The purpose of this document

The purpose of issuing national guidelines to strengthen information security is to create a shared understanding of what challenges we are facing and to identify areas in which extra efforts are needed to strengthen the national information security. These guidelines shall contribute to promote a better understanding of how users, developers and Information and Communication Technology (ICT) providers can benefit from, and contribute to, developing a culture of security.

The time horizon for these guidelines stretches into 2010.

1.2 Information security goals

In Report No. 17 (2006-2007) to the Storting (The Norwegian Parliament), the Government called attention to the need to ensure that

- the Norwegian information infrastructure is well protected by taking *preventive* measures
- that an ability is developed to be able to respond effectively to ICT security incidents through *preventive action*, and
- to ensure that security efforts remain *sustainable* through, i.a. competency development and standardization.

The Government has three general objectives with its information security work:

1. Robust and secure critical infrastructure and support systems for crucial functions in society.
2. A solid security culture with respect to the development and use of information systems and in electronic information exchange.
3. High competency levels and focusing on information security research.

The ICT security efforts will primarily be designed to protect and develop information systems and networks. ICT security is also about working to introduce new ways

of thinking and acting in terms of how information systems and networks are used and how information is exchanged. The measures taken in this area will also contribute to strengthen privacy protection, even though privacy is not the main focus in the present context.

An adequate level of ICT preparedness shall, at all times, exist in society. All preparedness efforts taking place in sectorial enterprises must include ICT preparedness, even when not mandated by rules and regulations.

1.3 Target group

These guidelines are directed at state government authorities. The implementation of these guidelines might also affect municipalities, municipal counties, private enterprises, private organizations, households and individuals.

The Ministries and their agencies are responsible for implementing measures within the action areas in the present guidelines. The management in the county municipalities, the municipalities and the private sector should, on their own initiative, take responsibility for implementing measures and for promoting a security culture in accordance with these guidelines. In that connection, the central authorities will have a role in facilitating the involvement of county municipalities, municipalities and the private sector in the implementation of measures of cross-sectoral nature.

1.4 Background

Today's Information and Communication Technology (ICT) is becoming increasingly complex. Services supported by ICT expand into all areas of society. This implies increased technology dependencies within the individual enterprise, between enterprises, between social sectors and across national borders. Disruptions in such services can have great consequences for an enterprise, a sector or for society at large. It is therefore, a precondition that technology solutions that are chosen are reliable, secure and contribute to create trust in the individual user. The complexity of technology and its interdependencies mean that strategic choices that are being taken to strengthen information security must be seen in association.
By *"Information security"* is meant protection against breaches of confidentiality, integrity or availability of the information that is being processed in a system, or the protection of information systems and networks in themselves. A precondition for having good information security presupposes users and developers of systems and network that are aware of, and understand ICT security issues.

Today, provisions on information security are integrated into various laws and rules and regulations. Examples of such laws are the Norwegian Security Act with Regulations, the Norwegian Data Protection Act, the Norwegian Act on Electronic Signatures with Regulations and the Norwegian Freedom of Information Act with Regulations. Information security is also incorporated into various sector laws and regulations. The Norwegian Electronic Communications Act with Regulations and the Norwegian Patient Data Act with Regulations are prime examples.

These national guidelines are anchored in the applicable body of rules. In addition, the present guidelines identify challenges that should be considered in the adaptation and further development of this body of rules.

The previous *National Strategy for Information Security (in Norwegian: Nasjonal strategi for informasjonssikkerhet)* was presented in 2003. A number of measures and activities were implemented over the course of the strategy period 2003-2006. [1]The major part of this security work was carried out in the sectors, primarily by agencies and enterprises. Securing the critical ICT infrastructure in society was a priority. The organization of cross-sectorial work was strengthened. The Ministries' responsibilities regarding national coordination of warning, advice and assistance was clarified. The National Information Security Coordination Council (KIS) was founded in 2004. The Council is composed of representatives from the various Ministries and Agencies with a role in the area of ICT security. The Council's mandate includes ordinary ICT security, security in critical ICT infrastructure in society and national security.

[1] See www.kis.stat.no for an overview of implemented measures and established entities.

2 Security challenges and trends

After launching the National Strategy for Information Security in 2003, primarily four technological and user-related developments have stood out:

- There has been an increase in society's dependency on ICT and the Internet. Society at large has become increasingly vulnerable to even brief operational disruptions in systems and networks.This growing vulnerability is partly a result of increasing systems and network complexities.
- There is a growing tendency for targeted, customized and professional attacks.
- Financial gain continues to be the most important motivation for attackers, who are increasingly going underground to steal confidential data. There are clear signs that the criminal activities have become more professional. Currently there exists an illegal market for trading tools to commit security violations.
- The great increase in the number of PC and Internet users, with varying skills, has brought an increasing need for awareness raising, information sharing and training. All users must obtain a better understanding of their responsibility towards other users of the Internet, and the skills they need to manage that responsibility.

Privacy is also challenged by new methods of communication and ways of using information systems and networks. Users must therefore become better at utilizing existing tools that can help strengthen privacy protection. In developing new security solutions, consideration should be given to the challenges in the area of privacy protection.

In the following the most central security challenges and information security trends are described.

2.1 Interdependencies between critical infrastructures are increasing

In this context "critical infrastructure" is defined as the facilities and systems that are necessary to maintain the functions that are critical for society. These functions cover basic needs in the society and contribute to a sense of safety in the population.[2]Electronic communications, power and electricity, water and drainage, etc. are identified as critical infrastructures. What critical infrastructures have in common is that their failure or destruction might have serious consequences for society.

Today, there is a strong interdependency between ICT and provision of electricity. This interdependency represents a significant vulnerability in society. Providers of ICT infrastructure and services have, to varying degrees, implemented protective measures against irregular supply of electric power. While the old telephone network functioned even without electricity, broadband telephony depends on the users' access to electricity, or that they have an emergency power supply such as batteries or generators. Secure power supply is therefore, especially crucial for ICT providers and enterprises that depend on ICT.

Knowledge about interdependencies is vital for the efforts to reduce vulnerabilities, and should therefore, be developed further. This is particularly important with respect to the interdependencies between critical ICT infrastructures, ICT operations and the power supply.

ICT is an integrated part of critical infrastructures in society and functions in society (enterprises) that are based on these infrastructures. Enterprises in charge of critical infrastructures have a special responsibility to protect information, systems and networks. Other enterprises might also be responsible for critical ICT infrastructures in society in the sense that they provide services, products or have competencies that are essential for managing critical functions in society.

2.2 Dependency on the Internet is increasing

In recent years, developments in society have made us more dependent on secure and well-functioning communication on the Internet. The Internet is becoming increasingly important, both domestically and internationally, for large parts of the private sector and for the individual user. There is a clear tendency for more and more companies to base their entire or central parts of their business on ICT and to use the Internet to offer an increasing number of services. The need for data transfer capacity is increasing. And this in turn increases the importance of having a secure and robust communication infrastructure.

Increased use of Internet services for commercial purposes has made many Norwegian companies' more vulnerable to even brief operational disruptions. More and more companies say that they would have significant problems if they had to shut down operations for one day, some after just one hour.

[2] Ref. Norwegian Official Report NOU 2006:6, *When security comes first: Protecting Norway's critical infrastructure and critical social functions* (in Norwegian: *Når sikkerheten er viktigst, Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner)*.

The society is facing an increasing level of electronic interaction. The extent of the information being exchanged, sensitive information included, is continuously increasing. Citizens and companies' use of the ever more integrated financial and economic service structure in Norway — and globalization in general — might be hindered because of the lack of mechanisms, such as electronic identification (eID), that make it possible to enter into binding agreements on the Internet. Use of eID can also reduce the risk of personal data abuse. These developments place demands on the solutions that are used to secure information and transactions on the Internet. Such demands particularly apply to authentication, integrity, confidentiality and non-repudiation of electronic messages or transactions. In addition, there are the demands for authorization of the interacting parties. .

eID can be used for authentication and can be realized with various technologies, including PIN codes, SMS passwords, PKI, etc. Electronic signatures are solutions that link a specific content with an identity in a non-repudiable way. Such solutions can be realized through the use of PKI or by using eID in combination with other technologies, for example, by logging and tracking.

2.3 Society is getting more vulnerable to attacks on the ICT infrastructures

Internet access failures can have great consequences for those who use the Internet to provide service and services. The already extensive use of Internet gives opportunities for quicker spread of malicious code and denial-of-service attacks. A denial-of-service attack can, at its most extreme, mean that a service is made inaccessible as a result of a targeted attack, often manifested as extremely heavy network traffic. A growing number of ICT and Internet users also increase the risk of undesired events that result from human error.

There is a growing trend for Internet attacks to be financially motivated. Internationally, we are seeing an increase in fraud attempts by acquiring personal information, which can then be used for financial gain through the use of e-mail. More than 90 percent[3] of all phishing attempts are directed at financial institutions in an effort to obtain banking and credit card information and other data. The attacks are more targeted and adapted toward smaller target groups than previously. E-mailing smaller groups makes it difficult to detect and react to fraud attempts.

In order to make operations more efficient, many companies have connected control systems for critical infrastructures to their administrative systems, which in turn are connected to the Internet. The danger is that malicious software, intentionally or unintentionally, can be downloaded from the open Internet and spread via the administrative network to the control system. This kind of "tunnel" into the control system can be deliberately exploited by criminals or, as its most extreme consequence, by terrorists in order to carry out acts of sabotage. It can also open up for espionage by making it possible to gain access to enterprise-sensitive information. If the enterprise under attack is important in terms of critical functions in society, the potential for damage is great, especially during crises or war.

© Mimsy Møller/Samfoto

2.4 Networks, terminals and services melt together to create complexity and opaqueness

Telephony, radio and television are moving toward using one unitary physical infrastructure, in which traffic is principally based on the use of Internet Protocols (IP). Today's Internet is being used for e-mailing, searching and retrieving information, interactive services such as e-commerce and Internet banks, file sharing and interactive gaming, among other things.

A new trend is that more and more people are using IP

[3] Anti-Phishing Working Group, Phishing Activity Trends Report, June 2006.

© Scanpix

telephony, conversations over the Internet, often accompanied by image transfers. As many start to use this form of telephony, replacing the usual telephony, the need for Internet robustness and service quality will increase. Convergence therefore requires that the Norwegian portion of the Internet be expanded in a robust manner. Internet technology can use various types of physical infrastructure, such as fiber, cable, copper and radio. This can make it easier to establish a robust infrastructure where users have several alternative connections. But it also provides opportunities for selecting low priced solutions where many different communication services use just one single physical connection. In that case the infrastructure that is created is vulnerable. It is of great importance that alternative traffic routes are established so as to make important categories of users — such as the rescue services, the health and social services — less vulnerable. Disruptions and failures in the IP telephony service may, for some users, threaten life and health. A likely development is that several players will begin using IP technology to produce services, but retain these as closed private networks. Such networks will share the physical infrastructure with the Internet, but exist as separate networks.

2.5 Wireless networks and mobile services create new usage patterns and increased vulnerability

Increased usage of mobile equipment and mobile network components provide a new set of challenges when Internet-based services are developed. So far, mobile data tools have had weaker security protection than personal computers. Connections are made both via wireless networks and mobile phone networks. Unsecured wireless access points provide a high degree of anonymity on the Internet and can camouflage individuals who wish to attack specific services or the network in general.

2.6 New vulnerabilities in software are a problem

Designing, producing and subsequently managing an advanced information system are complicated and demanding tasks. It is therefore important to perform security assessments to verify that accessibility, integrity and confidentiality as well as authentication and authorization requirements are handled in a satisfactory manner. An ICT system is not static. New functionality is added, and programs and hardware are upgraded regularly. It is not known how many data security breaches Norwegian companies are exposed to due to self-inflicted errors, but the number is assumed to be significant. This is not often talked about. A company that has been exposed to this kind of event usually does not wish the general public or the authorities to know if it has experienced serious problems as a result of unavailable ICT systems. Still, we occasionally read about, for example, Internet banks or mobile networks being out of order.

Users of dominant software platforms are exposed to malicious codes and viruses more often than other users.

2.7 Lack of security awareness among users constitutes a high and increasing risk

One of the greatest challenges to information security is the lack of security awareness among users. Many companies and individuals underestimate the risk of poor information security. The failure to prioritize such efforts by enterprise management and anchoring the efforts in the management is also a challenge. One of the reasons leaders lack awareness is that there is an absence of vulnerability and risk analysis and lack of documented cost-benefit analysis with respect to the benefits of good information security. Individuals, whether they are home users or employees in an enterprise, seem to have a general lack of knowledge and awareness with respect to the need for information security and the role they themselves are playing as actors on a network. Computers without protection can, without the owner's knowledge, be controlled remotely and thereby be used, for example, as a platform from which to

launch denial-of-service attacks (DoS attacks) against the Internet infrastructure. A denial-of-service attack on critical parts of the Internet infrastructure can have consequences for Internet usage nationally, regionally and globally. This requires all Internet users to take greater responsibility for their own conduct on the Internet and for the security of their own data environment. Today the security problems on the Internet are complex. To be able to act securely on the Internet and to protect one's own environment requires awareness and knowledge about the various security challenges.

2.8 The Competency challenge are growing in step with the increased complexity

Growing systems and network complexity makes it more difficult for those who buy systems and networks to place clear and precise demands on security. Choosing among ICT systems and products that shall meet certain security requirements requires that one has thorough knowledge of the strengths and weaknesses of the various solutions. A lack of such knowledge can lead to bad investments or inadequate information security. Furthermore, the complexity makes it more difficult for the individual user to gain an overview of all the security-related challenges that might be associated with the use of ICT.

Personal computers are becoming ever more powerful, and are available 24-hours a day with broadband connection. They are used in a growing number of areas and are thereby also becoming a more tempting target for intruders. As a result of this development, unsecured personal computers in the home constitute a greater risk than previously. This is, among other things, due to the increased diffusion of so-called "botnets", which are groups of personal computers that can be controlled remotely from a central source. The infected personal computers can be remote-controlled by means of malicious software, and can then be used for extorting money by commanding them to initiate attacks that block access to central computer systems in a company or other enterprise.

2.9 Increased internationalization contributes to national networks and systems increasingly falling outside national control

Monitoring of operations and managing serious errors and disruptions on the networks require staff with high skill levels that are available 24-hours a day. For reasons of cost and efficiency, providers of electronic communication networks and services work continuously to increase the automation and centralization of their operations. Increased globalization will imply that many national and international providers will offer outsourced operational centers and tasks to countries with lower costs. This kind of centralization and remote control of traffic make electronic communications more dependent on how well connections function across country borders. Increased outsourcing can mean that portions of our critical social infrastructure will be controlled from abroad. Monitoring is more difficult when parts of the enterprise is managed abroad and governed by the host country's rules and regulations. In the long term extensive outsourcing of portions of critical ICT infrastructure abroad contributes to a downscaling of skills levels and capacity. In turn this might lead to a weakened ability to manage national information security in an appropriate manner.

New methods to solve tasks, which in turn create new application areas, can also open up for new forms of abuse. Even if most innovations do not directly threaten the protection of privacy or information security, it is a challenge to handle such considerations in a globalized world.

2. 10 Changes in the manner in which technology is used by organizations create new security challenges

The software used in many organizations is currently much more standardized than previously. The development within modern ICT is designed toward the reusing of software, and toward connecting data systems using the Internet across organization structures. Today this happens in a completely different way than previously. So-called Service Oriented Architecture (SOA) makes it possible to technologically integrate value chains over the Internet. Such integration challenges established collaboration patterns among organizations. A customer can quickly transfer from data system to data system across several enterprises to order a product or a service. Transfer of user data from system to system in order to give users access without having to be re-authenticated and re-authorized — also called "federation" — might require a reassessment of the principles of accountability with respect to information security in their own organization. Similarly, the trend toward establishing joint portals, such as Altinn and MinSide, is a challenge for participating enterprises with respect to overall responsibility for information security. Outsourcing or disaggregation and professionalization of parts of internal ICT operations create similar problems.

In that connection it is important to clarify who is responsible for what at all times, so that responsibility for important network or systems components that fall outside organizational borders also is accounted for and do not become points of vulnerability for potential attacks.

2.11 The Internet creates new social trends – and increased vulnerability for participants in their social interaction on the Internet

The development toward the so-called Web 2.0 — or participatory web — opens the doors for an unknown range and type of social interaction over the Internet. Net sites such as MyPage, MySpace, YouTube, Facebook and similar sites attract millions of users and create a potential hotbed for the dissemination of malicious software or other types of attack. Chat rooms open up for direct attacks of the type "social manipulation" (social engineering) with serious consequences as a result.

This development creates a challenge in terms of competency and awareness raising. Users of such services need knowledge about privacy protection, potential security hazards, and the responsibility that each individual has to prevent the spread of malicious software, and resulting consequences for other Internet users. Exposure of own personal data can also constitute a threat to individuals that hold positions of trust within information security in various types of enterprises in that the data can be used for blackmail or other forms of manipulation.

3 Action areas

The areas of action described in this Chapter are defined on the basis of identified security challenges and the Government's main objectives for the work with information security. The action areas support one or more of these objectives, and the descriptions of each area have been kept at a general level. Processes for the further concretization of the action areas and the implementation of concrete measures are described in Chapter 4.

3.1 Critical ICT infrastructures must be better protected

All enterprises that own critical ICT infrastructure must introduce protective measures and establish redundancy solutions that ensure the maintenance of operations and supply. Preparedness for handling breakdowns in the critical ICT infrastructure must be strengthened both with providers and users.

The responsibility for securing the critical ICT infrastructure belongs first and foremost to the enterprise that plays a part in operation of the infrastructure. Failures in critical ICT infrastructure can lead to immediate and serious consequences for great parts of society. All enterprises that own a piece of critical ICT infrastructure must introduce protective measures and establish redundancy solutions that ensure the maintenance of operations and supply. Both the enterprises and ICT providers should prioritize measures to ensure robustness by among other things duplicating important components. Quick recovery after a breakdown is both a commercial and public goal. Preparedness for handling breakdowns should therefore be strengthened both with providers and users.

Society is critically dependant on an extensive ICT infrastructure. For many enterprises ICT is an enterprise-critical factor. An important action area is conducting exercises in how to handle events in which critical ICT functions fail. Exercises can uncover organizational weaknesses and provide increased skills and important experience with how to restore normal functions. Regular exercises make it possible to reduce the negative consequences of serious events that hit ICT infrastructure. Exercises should be carried out at all levels of society. Exercises will also contribute to reduce vulnerabilities in the ICT systems of individual enterprises. .

Identifying critical ICT infrastructure is important for enterprises to be able to prioritize preventive measures and preparedness actions. Each ministry is responsible for identifying critical ICT infrastructure in their sector and ensure that it is protected, cf. the principles of accountability, conformity and proximity. A body of methodologies should, on the basis of existing tools, be established as an aid to identify critical ICT infrastructure and critical functions that depend on ICT.

Outsourcing services are becoming more widespread. Enterprises responsible for critical ICT systems have a special responsibility to ensure that the interests of security and preparedness are met when outsourcing. Enterprises must ensure that security and preparedness obligations are managed in a satisfactory manner through agreements with service providers. The authorities should advise on the security and preparedness-related consequences of outsourcing.

Internet service providers should offer security solutions as part of their service provision. The conditions on which the provided solutions are based, and the security risks covered by the solutions, should be evident. The efforts involved in attaining a satisfactory security level with respect to electronic communications services should predominantly be met through self-regulation. However, the authorities need to follow industry developments closely. In case the authorities assess that an adequate security level has not been met through self-regulation, it might be relevant to issue orders to improve the security. A lack of security, however, can also be due to a lack of knowledge about ICT security. Further measures targeting awareness-raising efforts with respect to users of Internet services and other electronic communications services will therefore be equally important, cf. subsection 3.5.

Responsibility for the implementation: All Ministries that have identified critical ICT infrastructure in their sectors, the Norwegian Ministry of Justice and the Police in its capacity of responsibility of security and preparedness

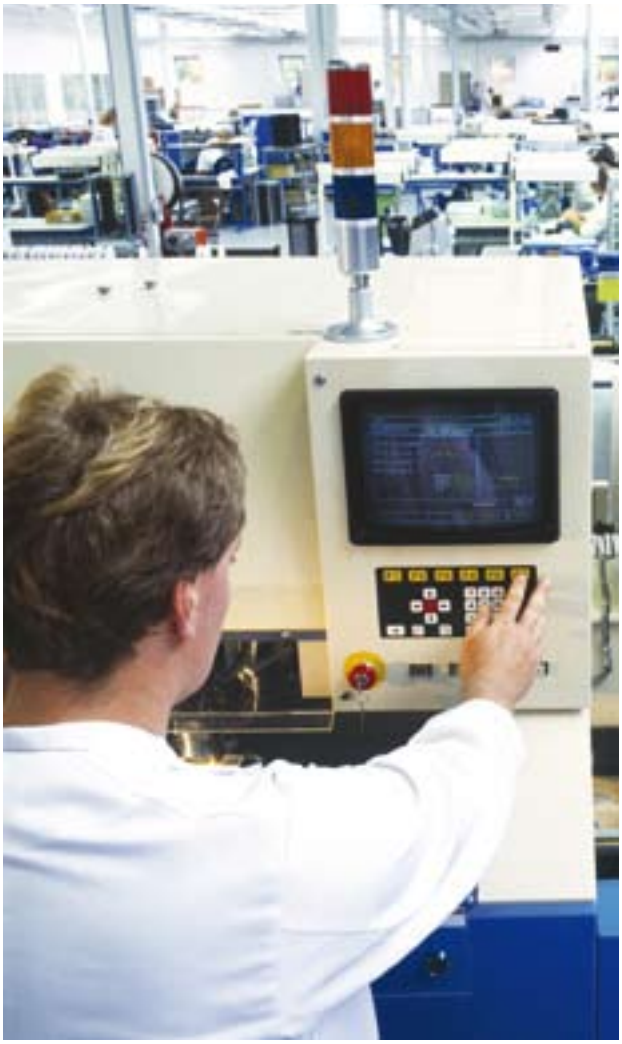
3.2 Regulations on information security must be made more consistent and intelligible

Regulations on information security shall be reviewed in order to pave the way for simplification and harmonized use of concepts. The authorities must communicate better with each other and with the enterprises covered by the regulations. Guidance efforts need to be intensified, especially with respect to municipalities and small and medium enterprises.

Many developments related to the Norwegian regulations on information security are influenced by international decisions and legal codes developed outside Norway. This entails a number of obligations, and this is one of the reasons for inconsistent use of concepts. When formulating law and sub-regulations that affect information security, it should be emphasized that such texts need to be easily understood while aiming to use a shared cross-sectoral conceptual system. Guidance can help to achieve a more accurate interpretation and better implementation of the regulations so that terms, definitions and interpretations are made as consistent as possible. If not, variations in interpretation will make it difficult for enterprises that are subject to several different regulations to meet their obligations. Formulating new regulations should be coordinated with existing regulations to the greatest extent possible so that the number of new provisions is limited.

Ministries and supervisory authorities shall improve communication with the enterprises covered by the regulations. This applies particularly to municipalities and small and mid-sized enterprises. Knowledge about experiences and perspectives on how the regulations are perceived and function is an important basis for developing the regulations, and one of the objectives of this communication. It must be presupposed that government bodies collaborate and coordinate their efforts to the degree necessary when communicating information about the regulations. Existing collaboration arenas between the administrators of regulations should be continued and further developed.

Responsibility for implementation: All Ministries administering regulations pertaining to ICT security, including ICT security in sector regulations.



© Scanpix

3.3 Information and information systems should be categorized to facilitate assignment of action items

All ICT systems and all data processed in ICT systems important to national security or privacy protection shall be categorized according to applicable regulations. Owners of information and information systems not covered by the regulations shall be encouraged to implement value assessments in order to identify which information it is necessary to protect.

There might be various considerations that justify protection, including privacy protection, shielding trade secrets, considerations related to national security, accessibility, etc. In certain cases this is warranted by law, for example, by the Norwegian Security Act and the Norwegian Privacy

Data Act. Categorizing information and information systems increases awareness of the significance and value that enterprise information or the ICT system represent. Another objective is that such categorization will simplify the efforts to secure the ICT systems and the information.

Owners of information and information systems not covered by the regulations shall be encouraged to implement value assessments in order to identify which information it is required to protect. Similarly, value assessments must be carried out to identify which ICT systems it is necessary to protect.

Categorization of information and ICT systems contribute to clarifying what needs to be defined as critical information or a critical ICT system. Shared approaches on how information and ICT systems should be categorized will reduce the likelihood that collaborating enterprises categorize similar management and control systems and administrative systems in different ways, and perhaps demanding different security levels for the same type of information.

Responsibility for implementation: All Ministries and agencies and enterprises under their control.

3.4 Risk and vulnerability analysis should be carried out by everyone, especially by owners of critical infrastructures

Enterprises that handle critical ICT infrastructure or ICT operations have a special responsibility for carrying out regular Risk and Vulnerability Analyses. The authorities must, in collaboration with relevant participants, facilitate the implementation of the risk and vulnerability analyses, and actively seek to raise the skill levels of the participants by contributing with guidance and advice. Where provided by the regulations, implementation of such analyses shall be included in an established management system for enterprise risk management. Risk and vulnerability analyses must be anchored within the management.

Implementing risk and vulnerability analyses is a necessary measure to manage risk and it enables the enterprise to uncover what areas are vulnerable and exposed to risks. In some cases orders to perform risk and vulnerability analysis are warranted by law, but such analyses should be part of a continuous activity in each enterprise. The analysis should be performed regularly or when needed. The implementation of the analysis should be part of an established management system for enterprise risk management and must be anchored within the management. It is in the individual enterprise's own interest to carry out risk and vulnerability analyses also when the enterprise is not covered by a body of rules that requires this.

Even if the risk and vulnerability analysis primarily is the responsibility of the enterprise, the Ministries must, in collaboration with subordinated agencies and relevant players, facilitate the implementation of such analyses. Through their subordinate agencies, the Ministries shall seek to raise the security skills levels of the participants in the various sectors. Where necessary the sector authorities must ensure that risk and vulnerability analyses are implemented through regulation. In some sectors this has already been done. And there are also cross-sector regulations that require the use of risk and vulnerability analyses for certain areas.

Enterprises that handle critical ICT infrastructures in society, or other functions depending on ICT, have a special responsibility for performing regular risk and vulnerability analyses. The enterprises will also need guidance as to the choice of method of analysis. Authorities responsible for security and preparedness must contribute to carry out these plans.

Responsibility for implementation: All Ministries, agencies and enterprises under their control.

3.5 Efforts to raise awareness and disseminate knowledge must be increased

Everyone shall have access to information about threats and measures to prevent these. There is a need to ensure an increased user awareness and knowledge of ICT and the Internet. Established awareness-raising activities shall be continued and developed further. This applies to the activities of the Norwegian Centre for Information Security (NorSIS) and the information and advisory activities of the Norwegian Post & Telecommunications Authority (Post og Teletilsynet) including the security portal Nettvett.no. Long-term collaboration between government agencies and the private sector organizations should be established to develop programs for raising awareness, training and building a good security culture.

There are a number of dependencies between enterprises and between the various sectors in society with respect to the use of ICT. That makes it difficult for the individual enterprises to assess the total consequences for society if

there is a lack of action with respect to information security. In order to reduce society's vulnerability, information about threats, vulnerability and efforts shall be shared. Government agencies responsible for security and preparedness are responsible for obtaining and communicating information about threat situations at the national and general levels. In order for everyone to have access to the same information about threats and measures to reduce threats, all owners and vendors of components for critical ICT infrastructure in the public and private sectors, should be invited to participate in common venues to share information. Other businesses too, are encouraged to participate in arenas where such information exchange occurs.

The responsibility for information security resides with the management of each enterprise. The management must be familiar with the risks the enterprise runs when introducing new ICT tools to all or parts of the enterprise. The management must also possess the necessary ordering competence for purchasing new ICT tools, using the assistance of external consultants, or the outsourcing of the enterprise's ICT services. Management must, based on a risk assessment, establish the security level of the enterprise and ensure that the requirements for information security are followed up by everyone within the organization. Consequently, all enterprises should have a system for raising awareness and building competence within the area of information security. The system should cover everyone in the enterprise. It is difficult and time-consuming to bring about changes in attitudes. Long-term collaboration should therefore be established between the authorities and the private sector organizations in order to develop programs for awareness raising, training and building a good security culture.

Awareness of risks and available protective measures is the first line of defence for security in ICT systems. The public's awareness and knowledge therefore, generally needs to be increased. Established and goal-oriented measures to strengthen ICT security awareness shall be continued. This, among other things, applies to the activities of the Norwegian Centre for Information Security (NorSIS) and the information and advisory activities of the Norwegian Post & Telecommunications Authority (Post og Teletilsynet), including the security portal Nettvett.no. Good resource utilization in this area requires close collaboration between government agencies, the private sector and private organizations. Government agencies responsible for security and preparedness shall therefore, in collaboration with the private sector, contribute to raising awareness of threats, inform about measures and promote good attitudes. Product and systems providers will be encouraged to set up an environment in which all products and systems geared toward the mass market are accompanied by easily

© Jann Lipka / Mira/Samfoto

understood information and training materials related to information security.

Responsibility for implementation: Managers in all government enterprises.

3.6 Warning and event handling shall occur in an expedient and coordinated manner

Security events and threats against critical ICT infrastructure and functions critical to society that depend on ICT, must be discovered and reported promptly. A higher degree of competence and better training will be the results of systematic reporting and sharing of experiences associated with ICT security events. This will also contribute to the authorities' ability to provide good advice about the security situation from a preventive point of view.

The dependency of networks, including the Internet and increased globalization, mean that there is a substantial need for coordinated warning and guidance. There is a need for

enterprises to report ICT security events to the relevant sector authorities. Existing collaboration and information sharing between the actors in charge of warning and the supporting apparatus should be continued and developed further. A higher degree of competence and better training are ensured by systematically reporting and sharing experiences associated with ICT security events. This will also contribute to the public authorities' ability to provide good advice about the security situation from a preventive point of view.

The Norwegian Computer Emergency Response Team (NorCERT) of the Norwegian National Security Authority (NSM) is the contact and coordination point nationally and internationally in order to protect and respond to security events with serious or acute influence on the Internet.

NorCERT, the Norwegian National Criminal Investigation Service (KRIPOS), the Norwegian Police Security Service (PST) and the Norwegian Defence Forces should collaborate closely in order to exchange experiences about the threat picture, assist each other professionally and clarify the national division of labour against unwanted events on the Internet.

Responsibility for implementation: The Norwegian Ministry of Defence, the Norwegian Ministry of Justice and the Police and the Norwegian Ministry of Transport and Communication.

3.7 All Ministries should promote the use of standards, certification and selfregulation

Systems developed in accordance with acknowledged standards for information security are essentially more secure. The sector authorities should provide incentives to all enterprises and providers to start using certified solutions. The Norwegian Ministry of Government Administration and Reform will assess if certification or self-declaration (internal control) of information security for public enterprises shall be required. The Norwegian authorities must become more active in their promotion of functionality and security requirements in connection with the development of national and international standards for information security.

Providers and producers of information systems and networks important to critical ICT infrastructures must be able to document that their systems have been developed and implemented in accordance with the acknowledged standards within the ICT area.

The authorities must take a more active role with respect to specifying and requiring documented information security in connection with public procurement. The Norwegian Ministry of Government Administration and Reform will assess whether or not public enterprises shall be subject to requirements for certification or self-declaration (internal control).

Standards within information security are established by international standardization organizations. It is important that Norway participates in this work so as to be able to affect the development of the standards, as well as to ensure knowledge about and implementation of the results. The provision of information with respect to available ICT security standards should be strengthened.

The authorities should encourage all enterprises and providers to start using certified solutions. This will contribute to encourage the ICT industry use approved standards in its development, implementation and operational tasks.

International standards are becoming more and more important for the national use of ICT. The harmonization of applicable technical security requirements and operational security levels is a continuous process. Standardization efforts are primarily driven by the participants in the private sector. The public sector has so far participated only to a limited extent. This may have resulted in the under representation of the general public's interests concerning the development of standards. The Norwegian authorities must therefore, eventually in collaboration with authorities in other countries, become more active in promoting functional and security requirements in connection with the development of international standards for information security.

The Norwegian Ministry of Trade and Industry has asked Standards Norway to work out a national strategy for the increased use of standards, and strengthened participation in national and international standardization efforts by December 31, 2007. ICT will be an important area in this strategy. ICT security will become more important and will therefore be a natural focus area. Standards Norway has already performed extensive work within the areas of ID cards, e-signatures, biometrics and ICT security.

Standards for information security should support competition within the ICT market and the general work toward open standards in the ICT area.

Responsibility for implementation: The Norwegian Ministry of Government Administration and Reform, the Norwe-

gian Ministry of Trade and Industry, other Ministries.

3.8 Ministries should promote Research and Development (R&D), education and competency development on information security.

Norwegian enterprises and the population at large shall have a high degree of competence within the area of information security. R&D within information security must be strengthened nationally, and incentives should be provided for Norwegian participation in international venues.

Knowledge about information security must be strengthened. The National Curriculum for Knowledge Promotion in Primary and Secondary Education and Training has ICT as one of its five basic skills, and ICT is part of the professional competency goals. Information security should therefore be included as a natural part of ICT use in the educational framework. This places demands on basic education and competency development for teachers and on teaching materials.

It is important that Norwegian universities and university colleges offer educational components that provide a major within the area of information security. University and university college ICT classes should have their own information security component.

Graduate education and raising skills levels within information security must be strengthened for users of ICT. Certification is a means to ensure that security personnel have the approved competence. Ministries should ensure that certification within ICT security becomes a criterion for hiring ICT staff.

The public and private sectors should make better provisions for master students of information security to be given the opportunity to work with current security problems within a sector, or in an individual enterprise by proposing concrete topics for a Master's thesis within information security.

Provisions must be made so that the research environments within basic research and applied research can have a good interaction with leading ICT companies and specialist environments across sectors. It is important that the applied research within information security detect changes in technologies and methodologies at an early stage. Research within information security must be strengthened nationally and thus provide incentives for Norwegian participation in the international venues. In addition to direct R&D grants, the public sector also plays an important role as customer and purchaser of various goods, development projects and services. ICT security should also be integrated with other relevant research programs.

Responsibility for implementation: The Norwegian Ministry of Education and Research, the Norwegian Ministry of Trade and Industry, the Norwegian Ministry of Government Administration and Reform.

3.9 A coordinated arrangement should be established for identity management and electronic signature across sectors

A joint framework for authentication and signing in electronic communications with and within the public sector should be established. Interconnectivity for electronic ID's (eID) and signatures must be managed.

In selecting a security level for a given electronic interaction, all public enterprises shall carry out a risk analysis in accordance with applicable regulations, and then choose solutions for eID's or e-signature in accordance with that. To assist with such assessments, there must be a foundation of a joint framework for authentication and non-repudiation in electronic communications with and within the public sector. Several countries have developed similar frameworks in order to coordinate risk and security assessments, in cases where electronic interaction affects the general public and private enterprises.

In order to simplify the use of eID's and e-signatures for users, it is expedient to have a shared scheme for issuing eID's at a security level that enables eID's to be used in several different contexts. This could be an eID with medium security level, but adequate for securing many types of transactions. It could also be an eID with a very high level of security and an electronic signature.

In order for public enterprises to begin using eID's and e-signatures for electronic transactions with the general public and private enterprises in a simple and cost-effective manner, interconnectivity must be addressed.

Responsibility for implementation: The Norwegian Ministry of Government Administration and Reform, the Norwegian Ministry of Justice and the Police, the Norwegian Ministry of Trade and Industry.

3.10 The Ministries international collaboration on information security shall be further developed

Ministries that work with information security at the international level shall have a shared international approach to all strategically important questions of a cross-sector nature associated with the secure use of ICT and the Internet.

Norway is participating actively in several international professional arenas whose purpose is to strengthen cross-sector information security. The efforts are mainly concentrated within the frameworks of international organizations such as the European Union's European Network and Information Security Agency (ENISA), the Organization for Economic Co-operation and Development (OECD), the Internet Governance Forum (IGF), and others. Participation in such efforts contributes to better information security in Norway. It also gives Norway the opportunity to be present when international policies are drawn up to ensure a more secure Internet globally.

It is important that Ministries participating in the international arenas for securing ICT and the Internet across sectors have a joint approach to all strategically important questions. Norwegian participation in this area must be coordinated and developed further in order to leverage the actions that are taken.

Responsibility for implementation: All Ministries that work with ICT security at the international level.

3.11 Information security efforts shall be coordinated through the National Information Security Coordination Council (KIS)

KIS shall be carried on and developed further as a cross-sector coordination body within information security for central Ministries and subordinate agencies. The interface between KIS, the academia and the private sector needs to be strengthened.

The Norwegian Ministry of Government Administration and Reform is responsible for coordinating preventive and cross-sector efforts with respect to information security. Each sector ministry is responsible for handling information security within its sector. The sector ministries also assess which measures should be implemented within their sector.

Through the establishment in 2004 of the The National Information Security Coordination Council (KIS) which is headed by the Norwegian Ministry of Government Administration and Reform, a framework has been established for improving the coordination of the government agencies' preventive efforts involving information security. The interface between KIS, the academia and the private sector needs to be strengthened.

Responsibility for implementation: The Norwegian Ministry of Government Administration and Reform.

4 Implementation

© David Trood/Samfoto

Information security is first and foremost the responsibility of the individual enterprise. But implementation of measures within the various action areas presupposes effective assistance of the private sector, the central and local authorities and the individual user.

In accordance with the principle of accountability each Ministry shall be responsible for following up on the action areas of these guidelines within its respective area of responsibility. The Ministries must, in collaboration with their agencies and subordinate enterprises, ensure that each sector follows up on initiatives and that measures are coordinated with the other Ministries to the degree necessary. The Norwegian Ministry of Government Administration and Reform has a general coordination responsibility for following up on initiatives.

Strong dynamics in the professional field necessitates short strategy periods. These guidelines will be the basis for the Government's work on information security for the period 2007-2010. As old security issues are solved, new ones will come to light with the advent of new technology, changes in usage patterns and altered threat scenarios. Consequently, protective measures that might be relevant today could be outdated tomorrow. In this general document the Government has therefore chosen to focus on action areas rather than concrete measures. It is up to the participants within each sector, at any given time, to implement the most suitable measures necessary to strengthen information security within the individual action area.

Initiating concrete measures within the various action areas could, among other places, occur in connection with the preparation of the Ministries' annual budget allocation letters to their agencies and subordinate enterprises, in which the objectives and priorities for the agencies and enterprises are given. Actions that affect the private sector shall be carried out in close collaboration with the private sector's own bodies. Measures affecting consumers shall be implemented in collaboration with the consumer organizations. To the degree the security measures also affect privacy the authorities involved in the protection of privacy should also be involved in the implementation.The Government will follow information security developments by conducting regular reviews in order to map status and challenges within the area.

The National Information Security Coordination Council (KIS) will be responsible for keeping track of the implementation of measures taken within the action areas and may, via the Norwegian Ministry of Government Administration and Reform, report to the Government about the overall status as needed. KIS will also play a role when it comes to the identification of cross-sector challenges within the ICT security area, which need to be followed up. KIS can also act as a facilitator to initiate measures of a cross-sector nature without changing the Ministries sector responsibilities. In this context KIS can create working groups in order to prepare concrete measures on the basis of the action areas. The Ministries can use KIS to discuss coordination and prioritizing measures. A framework will be created to have a dialogue with the private and municipal sectors in connection with initiating measures. KIS can be the arena for such dialogue meetings.

5 Economic and administrative consequences

© Robert Bråthen/Samfoto

The owner or operator has the primary responsibility for securing information systems and networks. This responsibility falls within the management's line responsibility. Security efforts must be handled as part of the daily operational routines of the enterprise and be financed over the regular budgets. Each sector ministry has an overall sector responsibility. Sector measures must be financed within the existing budget frameworks. Proposals for financing extraordinary measures must be presented in the ordinary budget process. The coordination responsibility that the Norwegian Ministry of Government Administration and Reform has for information security shall only apply to preventive, cross-sector efforts.

Appendix: Words and expressions

Authentication	Mechanism for verifying a claimed identity - that you are who you claim to be.
Authorization	The process of granting access to certain ICT resources, or the right to perform certain actions in a system.
Availability	Security that a service meets certain requirements to stability, so that relevant information and services are available as needed.
Biometrics	Authentication solutions that utilize measuring physical properties of a person (typical characteristics of finger prints, facial shapes and similar properties).
Botnet	A group of infected computers that are remote controlled from a central source. The computers are controlled by means of a bot program and is referred to as a (ro)bot or a zombie. Botnets can, e.g. be used in connection with blackmail where a computer is commanded to execute distributed denial-of-service attacks (DDoS) against the website of an enterprise.
CERT	*English acronym: Computer Emergency Response Team*. Expert team that handles security events. CERT is a registered trademark of Carnegie Mellon University. Many therefore, use the abbreviation C(S)IRT, which stands for Computer (Security) Incident Response Team.
Confidentiality	Ensuring that only authorized persons gain access to data.
Convergence	The merging of media based on digital technology. The Internet has been the driving force behind the merging of telecommunications, broadcasting and data processing. Convergence means that the differences between the data processing, telecommunications, and media sectors are blurred.
Critical social infrastructure	The ability of society to function is heavily dependent on a number of physical and technical infrastructures. In case these infrastructures fail severely, society is not capable of maintaining the supply of goods and services on which the population depends (cf. Functions critical to society). These infrastructures can be referred to as critical to society.
Denial-of-service attack	Denial of Service Attack (DoS/DDoS). Attack on a website in the form of volume of requests. This makes it difficult for others to contact the services desired. As a worst case scenario, this can result in the break-down of the attached website's servers. Such attacks might involve the use of several powerful computers (potentially a network of computers) simultaneously (see also Botnet).
Digital signature	A PKI-based electronic signature. A data element that accompanies an electronic message or a document, which links the document to an identity. A digital signature is generated by first storing a digital ~~fi~~nger print~~of~~ the document, and then encrypting it with the private key for the person who needs to sign it. See also PKI.
Digital certificate	Electronic proof of identity for the owner of a private and an associated public key, which shows that the public key belongs to the person in question. See also PKI.
Distributed denial-of-service	A denial-of-services attack that is launched from several machines at a common target simultaneously. (See also Botnet and Denial-of-Service.)
Domain Name System (DNS)	Service on the Internet that translates domain names (e.g. www.regjeringen.no) to IP addresses (e.g. 195.225.0.230).
eID	Electronic identification of a person, an enterprise, a data system, or similar entities. Can be executed by means of user names, passwords, PIN codes or other relevant technologies.
Electronic tracking	Electronically stored information that can be used as proof or documentation. Also called electronic proof or digital proof.

Encryption	To garble a text (or a bit pattern) to an unreadable, incomprehensible so-called cipher text, which can only be decrypted by means of an encryption key.
E-signature	Data in electronic format linked to other electronic data, which can be used as an authentication method.
Functions critical to society	Functions that cover society's basic needs and the population's sense of safety, e.g. banking and financial services, health and care services, etc. See also Critical infrastructure.
Hash algorithm	Mathematical function that creates a ~~-di~~gital fingerprint ~~–fr~~om an amount of data. A good hash algorithm will always create different fingerprints for different amounts of data, even if the difference between the data is just one bit.
Hacking	A slang term for making small alterations to computer software. Is frequently used in a negative sense, and, if so, about the alterations made by unauthorized persons with dishonest intentions.
Information security	Protection against infringements of confidentiality, integrity and accessibility of the data that is being processed by the system or of the system in itself.
Infrastructure	Basic structures and systems required for an organization, a collection of organizations or a country to function in an effective manner.
Integrity	Know for certain that data and the data processing are complete, accurate and valid and a result of authorized and controlled activities. Ensuring that only authorized persons gain access to data.
Interconnectivity	Interconnectivity involves the interaction among various service providers at four levels: Technical, policy-related, business-related and legal. Interconnectivity between two eID providers' solutions means that you, as a user of their services, need only relate to one of them (similar to telephony services).
Non-repudiation	Know for certain that someone sending a message through an information system cannot deny or reject that he or she is the person in question that performed the action in question.
Phishing	Attempts to acquire unauthorized information, such as passwords and bank information. A typical example is a false e-mail from a bank in which the recipient is requested to follow a link to a false website, which seemingly belongs to the bank. There, the recipient will be asked to disclose personal bank information, which can then be used for theft or fraud.
PKI	*English abbreviation: Public Key Infrastructure*. A collection of security services, security components and players that make it possible to use digital signatures at a large scale. It is based on asymmetrical cryptography and the use of public and private keys linked by a mathematical function.
Social engineering	Social manipulation. A manner in which to manipulate other individuals' perceptions that contributes to establish credibility for a player with criminal intentions, and through that gains access to carry our illegal acts.
Spam	Unwanted e-mail. This is mostly a case of mass distribution of advertisements via e-mail. The threat consists in the resource consumption linked to the processing of these messages, as well as legitimate messages' drowning in all the spam. Spam can also be used to spread viruses. Similar to spam and e-mail, SPIM is used about instant messaging messages (Instant Messages – IM).
Trojans	Malicious software disguised as a legitimate program. The purpose might, e.g. be to gain remote access to a computer or to leak out information from the computer. It can either hibernate as it awaits an external event or work actively in the background.

Worms	Software capable of spreading from machine to machine. In addition to be able to spread itself, the software will perform undesired actions, such as leaving malicious software for, for example, keyboard logging, servers for remote access of the computer, botnets, etc.
Virus	Malicious software that reproduces itself. It is usually part of another program. When this program is executed, the virus program, too, will execute.
Vulnerability	The vulnerability of a system is an expression of the weaknesses and defects in the system and special circumstances that increase the likelihood that threats will materialize in a security event (examples of special circumstances include size, complexity, the number of players involved, geographical distribution, frequent alterations and exposed location).

Published by:
Norwegian Ministry of Government Administration and Reform

Public institutions may order additional copies from:
Norwegian Government Administration Services
Distribution Services
E-mail: publikasjonsbestilling@dss.dep.no
Fax: + 47 22 24 27 86

Publication number: P-0942 E

Print:
Norwegian Government Administration Services 10/08 - 500

Design: www.lucas.no