i2010: A strategy for a secure Information Society.

Network and information security (NIS) is a key enabler for further development of the Information Society in Europe and beyond. Legislation, research and a new European Network and Information Security Agency are helping to build this confidence. In addition, the Commission is promoting a new approach to network and information security based on open and inclusive multi-stakeholder dialogue.

The context

Production and use of ICTs (Information and Communication Technologies) account for around 40% of productivity growth and one quarter of overall growth in Europe. The eCommunications services sector is the largest segment of the overall ICT sector (44.4%). The Internet has become a fixture of both business and private life: 89% of EU enterprises actively used the Internet in 2004; 65% had a website; 47% of people regularly use the Internet. With 25% of households using broadband, millions are now almost permanently connected. NIS is crucial for the smooth development of new systems, applications and on-line services, and thus for the whole European economy.

NIS needs to be seen as a virtue and an opportunity rather than a liability and a cost.

The challenges

As the systems and networks continue to grow and become more and more complex, we can expect more security issues to emerge. Moreover, while traditionally most attacks on computer systems have been motivated by curiosity or a desire to show off technical virtuosity, many current attacks are motivated by profit. Links to organised crime put the phenomenon in a particularly alarming light. New technologies and applications, such as mobile devices, RFID (radio frequency identification), and ubiquitous computing (computing embedded in everyday objects) are likely not only to unveil new opportunities, but also present new challenges for security and privacy.

The European NIS policy

The importance of NIS for European policy has already been recognised in many ways[1)]. The i2010 Strategy (the digital component of the EU's revised Lisbon strategy for growth and jobs) highlighted the issue of security as a prerequisite for offering affordable and secure high - bandwidth communications. Recently, a new strategic approach to NIS based on dialogue, partnership and empowerment has been proposed by the Commission: http://ec.europa.eu/information_society/doc/com2006251.pdf.

The Strategy proposes an inclusive process in which all stakeholders take up their part of responsibility:

- **Public administrations** have a particularly important role to play, for example by giving high priority to the security of their own networks and thus serving as an example to other stakeholders.
- **Private sector enterprises**, in turn, need to address security as an aspect of customer service and an enabler for new business opportunities and innovative societal services rather than a necessary evil or a purely legal obligation.

What makes Network and Information Security important?

NIS is the primary element for ensuring trust and confidence in the electronic communications networks and services that increasingly underpin critical aspects of our economy and society. Information and related systems need to be protected, for instance to maintain competitive edge, commercial image, business continuity, prevent fraud or ensure legal compliance (with privacy and data protection laws). Appropriate levels of network and information security provide such protection by ensuring that information transmitted and accessed over electronic communications networks remain available, reliable, authentic and confidential. For a definition of NIS, see MEMO/06/223, available at: http://europa.eu.int/rapid/

- **Individual users** need to understand that the integrity of their home system is an important component of overall network stability. They must ensure their own machines do not damage other user's data and systems.

The Strategy consists of three elements:

- Given the important and complementary roles of both public and private sector actors in the development of a security culture in Europe, security policy can only be developed in an effective manner on the basis of an open and inclusive multi-stakeholder **dialogue**.
- **Partnerships** are needed so that each actor can fulfil their own role in the broader context of network and information security.
- The **empowerment** of each stakeholder group is a prerequisite to foster awareness of security needs and risks in order to promote network and information security.

ENISA

ENISA is the European Network and Information Security Agency which was established in 2004 in Heraklion (Greece) as the EC's response to security threats. The Agency will build on national efforts to enhance security and to increase the ability to prevent and respond to major network and information security problems.

The activities of the Agency focus on advisory and co-ordinating functions, where data on information security is collected and analysed.

ENISA will consult industry and other stakeholders in pursuit of its objectives. It will ultimately serve as a centre of competence where Member States and EU Institutions can seek advice on matters relating to security.

Research & Development

Important research in Trust and Security is undertaken in the IST (Information Society Technologies) research programme. It is also pursued in a range of related areas including e-government, e-health, mobile services, and embedded systems (special-purpose systems in which the computer is completely encapsulated by the device it controls).

The research focuses on digital identity management and privacy, biometrics (automated methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits, like fingerprints or signature) and digital asset protection. Significant work is also done in the areas of resilient infrastructures (capable of proactively responding to both anticipated and unexpected stresses and strains, like man-made events, component failures and natural disasters), novel crypto-technologies, immunity of networks, trustworthy sharing of digital assets, security assurance and open trusted computing.

But more efforts are needed, for example, to promote e-inclusion (making sure everyone can participate fully in the information society) or better public services.

Related policies

In addition to specific initiatives addressing NIS, the Commission is pursuing a number of related policies, including the protection of personal data; regulatory framework for electronic communications (currently under review); fight against cyber-crime; and the protection of critical infrastructures (including critical information infrastructures).

The Commission attaches particular importance to international cooperation for creating, fostering and enhancing a global culture of security, as part of the approach agreed at the World Summit on Information Society in Tunis in 2005.

See also:

- Fact sheet 24: Protecting privacy and fighting spam
- Fact sheet 25: An international perspective for a global information society
- Fact sheet 35: i2010

All fact sheets can be found at :

http://europa.eu.int/information_society/factsheets/index_en.htm

Further Information

- **Principal Website**
  http://europa.eu.int/information_society/activities/index_en.htm
- **Europe's Information Society: Thematic Portal**
  http://europa.eu.int/information_society/index_en.htm
- **ENISA**
  http://enisa.europa.eu/
- **NIS**
  http://europa.eu.int/rapid
- **ICT for Trust & Security**
  http://cordis.europa.eu/ist/trust-security/index.html
- **Information Society and Media Directorate-General:**
  Av. de Beaulieu 24, 1160 Brussels
  infsodesk@cec.eu.int

1) See e.g. the Communication from the Commission "Network and Information Security: proposal for a European Policy approach" COM(2001) 298 final