Speech for conference

Introduction

Today's **society and economy already depend heavily on networks and information systems**. New wireless applications will enable us to access the Internet from anywhere, at any time. More and more consumer products are connected to the Internet; from printers to refrigerators and central heating systems. The potential risks for security breaches and security breakdowns grow as fast as people invent new ways to use the Internet. As one of the most connected countries, You are certainly already aware of these new vulnerabilities of our networks and information systems.

A study commissioned by the UK Department of Trade and Industry shows that **a quarter of all UK businesses suffered a *significant* system failure or data corruption last year**. This survey also shows that more and more threats come from the outside and that the data security problems faced by companies are growing bigger, and more expensive to fix.

Another example comes from the Special Eurobarometer Survey on public opinion concerning issues relating to B2C e-commerce. This survey shows that in 2003, 3/4 of the EU consumers who *did not* shop on-line gave, as their **prime reason, not trusting the Internet for secure payments**. Interestingly enough, 48% of those who *did* use the Internet for shopping also said that the security of payments on-line was a big concern for them.

A survey from 2003 of home PC problems in Norway showed that almost **half of the users have experienced serious errors and faults with their equipment or software** over the last six months. "Serious" means that they have had either to seek help or have simply given up trying to correct the problems. Most of them looked for help from family or friends.

The record high numbers of worms and viruses that have plagued the Internet in recent years show how vulnerable we can be and show that the problems can affect all groups in society.

These few examples show that network and information security is a **concern for everybody,** from infrastructure and service providers to product and service consumers, that is, citizens, businesses and public administrations**.** It also shows that the issues can vary a

lot in size, complexity and impact. The worrying part is that these problems seem to have grown over the years, as we all know.

As electronic communications play an ever greater part in our daily lives we will also have to learn how to adapt to and manage new vulnerabilities. We are moving towards something that is now called ambient computing – where the information systems are all around and even inside us.

It is a big transformation where we all have to contribute; **we need to achieve a culture of security**. I am particularly happy to be in charge of one of the instruments to help Europe achieve this culture of security; the European Network and Information Security Agency; ENISA. This is also what I will be presenting to you today: the basic ideas behind ENISA and an outline of our plans for its first years of operation.

The creation of ENISA

Why ENISA?

Network and information security is certainly not a new issue. In fact most Member States have done considerable efforts during a long period of time to strengthen information security. We have seen policies on cryptography, privacy, electronic signatures and on awareness raising, just to mention a few areas. Now we have added the word "**network**" to the old notion of information security as the interconnected networks create a new set of issues that needs to be solved. The interconnection has also **increased the need to co-operate both across sectors and across national borders**.

This is what forms the basis for the ENISA. The Agency shall be a **forum where all stakeholders can meet in order to be able to increase information exchange and to increase co-operation on network and information security**.

Member States, European Parliament and European industry have shown a great interest in this Agency and I think it is clear that we start to realise that we share much the same interests and that we will all benefit from a higher level of security being reached in all areas.

ENISA will be able to **provide guidance and advice to the EU bodies, Member States and to other organisations in Member States**. As the Agency will have fairly limited resources, and there are organisations in all Member States already doing work in this area, the idea is not to take over from them. Enterprises, administrations and citizens shall still turn to their national organisations or authorities for help, but now ENISA will be able to quickly provide

these with input on how to handle the relevant issues. The main purpose of ENISA is therefore to increase security in order to support industry, end users and consumers.

Bringing the stakeholders together

ENISA will, when fully staffed, employ just over 40 experts in network and information technology. Even if the Agency itself will be small it will still be able to **bring all the stakeholders together in a public private partnership** which I think is a very important feature of ENISA. The Management Board has representatives from all Member States and also from stakeholders, which means university, business and consumer side. It has also been decided that EEA EFTA countries (Iceland, Lichtenstein and Norway) shall be able to participate as observers in the Management Board.

One of my most urgent tasks has recently been to appoint members to a **Permanent Stakeholder Group**. This group will be composed of experts from communication technologies industry and consumer groups as well as academic experts. It will advice me as Executive Director and assist in the drawing up of the ENISA work programme as well as facilitating the information flow between relevant stakeholders in Europe and ENISA.

The third part of this public private partnership is the possibility to create specific **ad hoc working groups** that can consist of a small number of experts to discuss particular issues, such as maybe mobile security, payment, risk assessment methods or any issue that arises and that might need some special attention for a while.

We must act in concert to get our choice of technical security options and organisational arrangements right. Applying these options in a non-harmonised fashion might lead to inefficient solutions and in practice create obstacles to the single market. For example, if security requirements for goods and services differ from one Member State to another, they could lead to obstacles to free trade across the EU.

Tasks for ENISA

Now I'll talk about the goals for ENISA, i.e. to increase information exchange and co-operation between stakeholders. More in detail ENISA will have an annual work programme that for this year has been recently adopted. As this is its first year and only a limited staff available to work for ENISA we will start and focus on a few important tasks on which we can build the activities for the forthcoming years.

Information exchange and cooperation

Stepping up co-operation among all stakeholders and improving information sharing are key drivers for change.

There is a lot of information in Member States on the security problems that exist and also on solutions and remedies. The important task for the ENISA will be to **gather all the relevant information** and to be able to analyse it and **disseminate the knowledge** to those who need it.

ENISA's independence should promote trust and favour the direct involvement of industry, in both identifying and solving security problems in Europe.

We will also soon have the results of a **study carried out by Deloitte**. This is a study commissioned by the European Commission in order to find out who the contact points in the Member States are and to make an inventory over measures that have already been made. The result of the study will be published also on the ENISA web page. It will then be possible to use this site to find out whom to contact in each Member State on a certain topic. We further expect to be able to publish some **examples of good practices in various areas**, e.g. awareness raising actions so that others can use them as a starting point for their awareness raising. This information will be very important for ENISA as one of the main goals for the Agency is for various stakeholders to start co-operating and exchanging information on this.

The identification of stakeholders and building up the networks will be on-going and I will have national experts seconded from Member States to help me during the first months of2005.

One particular area that we see as particularly important for the information exchange and cooperation is the area of Computer Emergency Response Teams – CERTs or similar organisations. These are organisations to which incidents can be reported and handled.

Today in Europe not all countries have CERTs. It will therefore be a task for the ENISA to ensure that Member States who want to set up CERTs can get help from experiences in those countries that already have such organisations. It is also important to facilitate that these organisations know about each other so that they can establish the appropriate contact networks and exchange information on their activity.

Awareness raising

A basic feature of the culture of security is that all stakeholders are aware of the risks and what they can do, to be secure, when using the new communication networks.

A lot of work has been done in this area, so we should not have too much difficulty in identifying good practices that we can use for ideas and inspiration.

A special project I myself would like to highlight as an example is from Norway called SAFT (Safety Awareness Facts and Tools). This is a project aimed at increasing awareness about security among the younger users. The SAFT project was presented at a conference arranged by the Dutch presidency in October last year which I attended, and I think we have two important lessons to learn from this project:

1. It is **necessary to address different user groups in different ways** – children and young people use computers and the networks in a radically different way than I do or than e.g. users in a company do.

2. The **message should be positive** – it is important not to frighten people, but to give some positive tips so that users feel that they know what to do. Users don't need to be scared, but they need to know what the risks are and how to handle them.

This is only one example, but I think we have to identify a number of user groups and what the needs are in these special groups. Besides children and youth, I think about "old people": this is another target group. The group of people, that never had computers as a natural tool when they attended school or in the work place, needs a basic knowledge also about information security in order to be able to access these systems today.

SMEs is another important group as they rarely have the resources to invest in adequate knowledge on e.g. how to protect their networks and valuable company information. Awareness campaigns can also be directed to different sectors, such as banks and public authorities.

Part of this awareness raising will also be to know whom to turn to if problems arise and to make ENISA known in Member States. For this ENISA will provide an inventory of all active organisations in Member States and what they do and how they can help and assist users.

Dialogue with industry

As I mentioned before one of the important features of the ENISA is that we will be able to bring all stakeholders together in a public private partnership. **Industry involvement is of**

utmost importance when it comes to network and information security. Many of the networks are privately owned, software development is carried out by private companies and industry is a big user of ICT. Without involving industry, governments will not achieve secure networks and information systems….as simple as that!

One example is the use of risk assessment methods that are necessary for well-developed security policies. Another area is standardisation. In both of these areas, **industry is in the lead** and there are many more examples. Still there will be a role also for governments and public authorities in promoting and supporting such methods or standards. ENISA provides one important means to **develop dialogue with industry** on these issues and to come up with a set of best practices.

We also have to realise that **information security often provides business opportunities**, e.g. in virus protection and fire wall software. Where this is the case, ENISA's involvement should not overlap what industry is doing, but rather fill in the gaps.

The existence of generally recognised **standards is an important prerequisite for obtaining secure and interoperable products and services**. Although standardisation is a task for industry, ENISA can nevertheless track the development of standards in the area of information security and make available a list of available security standards and facilitate further work in the standardisation organisations.

Global perspective

Stepping up co-operation means working not only with EU Member State governments and industry, but also **with third countries and the global community.** As network and information security is a global issue, there is a need for cooperation worldwide, to improve security standards and information exchange and promote a common global approach. Such co-operation will help us to develop a culture of network and information security that is understood worldwide.

To this end, ENISA will contribute to Community efforts to co-operate with third countries and with international organisations.

Future work

ENISA will not manage to take on all its tasks in the first year, but it will have to develop gradually. In the area of Network and Information Security the development is quick and I

also foresee further tasks for ENISA in the coming years, and maybe I should mention a couple of what will be the future tasks.

A) We need to help the development of **risk assessment methods** for both public and private sectors. Such methods are the base of all effective security policies and it is a problem that there is at present no consensus on best practice in this area.

B) As the information networks are becoming one of our critical infrastructures, we also need to look into what the dependability and interdependencies mean for the **critical communication infrastructure.**

All in all ENISA shall develop to a centre of expertise in Europe and shall be able to advice the Commission on research in the area of network and information security and to provide opinions and advice to Member States and European bodies.

CONCLUSIONS

I would like to conclude by making the following three points.

Firstly, network and information security affects everybody, in all countries and across all user groups and we all need to get involved. I'm very happy about the great willingness to co-operate that has been shown already by Member States and industry and I hope that the trust ENISA will build up can be used to improve the security all over Europe…

Secondly, risk preparedness and compliance with risk management standards will increasingly become an economic factor in the global supply chain. Ensuring business continuity will become an increasing challenge for corporate governance. This is what ENISA will aim at doing by helping Member States and Member State's organisations to support European users and European industry to handle security risks and vulnerabilities.

Finally, I want to stress again that the messages from ENISA shall have to be positive, we are not there to frighten people or to make people stop using the Internet – on the contrary.

We want help making the Europeans into advanced and security aware Internet users in order to be able to make full use of the advantages of the information society.

Thank you!