Single Information Space. It is our collective responsibility of policy-makers, industry and all other stakeholders."

The European Union needs to explain the hands-on benefits of NIS in everyday life. NIS works not only to the benefit of the economy, but also socially, to make a 'Europe of results' a reality for citizens. This could be achieved through, for example, the everyday use of RFIDs to identify lost luggage, or with the 'Intelligent Cars Initiative', potentially saving up to seven thousand lives a year. That's where and why, working in close co-operation with the EU Member States and EU bodies, all other NIS actors, such as the industry and academia, can make a difference.

Finally, I would like to welcome Dr. Panagiotis Trimintzios to the position of Editor-in-chief of the ENISA Quarterly. I am sure Panos will maintain the high quality of this publication established by his predecessor, while at the same time bring new ideas, adding to ENISA's overall outreach activities.

Andrea Pirotti
Executive Director, ENISA

A WORD FROM THE EDITOR

Over the last years we have all witnessed the changes in the area of Network and Information Security (NIS). Attacks are becoming more and more targeted, stealthy and sophisticated, with the use of advanced tools and the introduction of innovative ways to intrude. Cyber attackers' incentives are also changing considerably. Hackers are evolving into well paid professionals who sell people's private information or can be hired to launch an attack. In order to deal with this changing scene, NIS must use strategies and provide solutions that target many different facets of the problem.

In this issue we welcome articles on good practice and forward-looking insights into a number of different areas of NIS, which could help towards improving information security. Contributions include understanding the ever evolving threats, setting up appropriate procedures for dealing with new and emerging vulnerabilities, raising users' awareness, setting strategic policies and regulations, measuring the effect of policies, and the importance of having diverse solutions.

This issue opens with articles from two members of ENISA's Permanent Stakeholders Group, and one by the stakeholder member on ENISA's Management Board. Olivier Paridaens writes about the importance of decreasing response times when a new vulnerability appears in a software product. He argues that there is no such thing as 100% safe software, so the best approach is to have in place the appropriate procedures to deal promptly with the discovery of new vulnerabilities. Prof. Markatos et al provide a new insight into emerging threats that do not need to compromise a computer in order to achieve an attack. The authors demonstrate how it is possible to take advantage of the functionality offered by file sharing peer-to-peer applications to launch Distributed Denial of Service (DDoS) attacks. Finally, in a relaxed and easy to follow article, Markus Bautsch, proves the importance of raising awareness and provides ten simple rules of good practice for increased security.

Our own experts highlight some of ENISA's recent activities and results. In this issue we summarise the ENISA follow-on study in Anti-spam measures, present the unique, comprehensive, online inventory of tools and methods on Risk Management, the step-by-step guide to setting up a CERT, and the Information Package on Raising Awareness. ENISA has also recently (co-)organised a number of successful workshops; my colleagues have summarised the main findings from these events.

In addition, this issue includes accounts of activities, insights and success stories from the EU Member States. Kristiina Pietikäinen provides a strategic article presenting the view from the Finnish EU Presidency on the need for a clear and coherent Information Security Policy Framework in Europe. Martin Schallbruch advocates security through diversity, outlining Germany's Federal Government software strategy for the use of Open Source Software. Rytis Rainis introduces an example of awareness raising good practice in Lithuania, where cyber security software was distributed free-of-charge to ICT users. Finally, Bill van Mil et al describe the lessons learned from a risk analysis of the Netherlands' energy and information technology infrastructures.

We would like the ENISA Quarterly (EQ) to be a refreshing and constantly improving publication. So we are planning a number of changes. With this issue we have introduced a new numbering system that includes a volume number, so readers can easily reference previously published articles. We have also started announcing future relevant NIS events around Europe such as those organised by ENISA, by standardisation bodies, academic conferences etc.

I plan to create a web page for EQ that will include all relevant information about the publication, including objectives, scope, important deadlines, calls for contributions and special issues, information for contributors and a library of back issues. Please visit the ENISA website regularly (www.enisa.europa.eu) to access the EQ pages, which will be available online in early November 2006.

It is clear that NIS is a very broad discipline that includes a wide range of areas. Indeed up to now each issue of EQ has offered a balanced view of many aspects of NIS. In the future I would like to introduce EQ 'special issues', each focusing on a specific aspect of NIS. Some examples of the special issues that I am planning for forthcoming editions include 'Economic Aspects of NIS' and 'Early Warning and Emergency Preparedness Systems'. Watch for announcements of the Calls for Contributions for these special issues.

Finally, I would like to urge all readers to submit an article to be considered for publication in ENISA Quarterly. This is the best way for you to reach out to a wide audience in Europe. After all, it is your contributions that make this periodical a success. Please pass this message on to all your colleagues and do not hesitate to send me any ideas or suggestions that you think will make the ENISA Quarterly a better publication for you!

I hope you will enjoy reading the rest of this EQ issue, as much as I did while editing it!

Sincerely,

Panos Trimintzios,
Editor-in-Chief, ENISA Quarterly

Dr. Panagiotis Trimintzios is an Expert at ENISA responsible for Relations with Industry, Academia, and International Organisations

From the World of Security - A Word from the Experts

Good Practices for Managing Emerging Vulnerabilities

Olivier Paridaens

Over the last years, Information and Computer Technology (ICT) users from all sectors, including home users, have been hit increasingly by security-related attacks, as a result of vulnerabilities within products and software modules, such as applications, middleware and operating systems. Considerable pressure has been applied to ICT vendors to 'solve this issue', leading to efforts by major manufacturers to enhance the level of security in their products.

Such efforts basically address two major aspects of the problem:

- to ensure that security is duly taken into account during the software product development lifecycle, and
- to define the appropriate process for handling security vulnerabilities that are identified in deployed products.

The latter is essential, despite the effort that is invested in the development of secure products and software; there is no way to achieve a 100% secure system since, during the development of a large and complex product, some weaknesses inevitably will be overlooked. An ICT vendor therefore must be able to react when a new vulnerability is discovered that could impact on products which have already been deployed with customers.

Defining the Problem

In this article we are looking at the problem of reacting to the discovery of new vulnerabilities from the standpoint of a vendor who supplies either a software tool or a 'complete' product that includes hardware with embedded software.

In addition, we are focusing on vendors who provide solutions to network operators, such as telecom operators (telcos) and Internet service providers (ISPs), or large enterprises, rather than vendors of mass market off-the-shelf products that are typically sold to home users or SMEs. Indeed, the business relationship between the vendor and the customer is usually different in these two cases.

Another important aspect that we need to clarify for the scope of this article is the type of vulnerabilities we are referring to. These vulnerabilities can be of a differing nature: a flaw in the programming code of the software product, a missing security feature in the product, inherent weakness in a protocol implemented within the product, a mis-configuration, or a misuse.

> "there is no way to achieve a 100% secure system"

Most people understand a vulnerability as a flaw in the programming code of the product, i.e., a bug. A bug results from errors in programming the software that could be avoided if programmers followed a strict methodology, used code verification tools, and further proof tested the software. But today most software products have become so large and complex that there is no absolute guarantee of error-free software. Therefore, vendors and their customers must be ready to face and manage such vulnerabilities in products.

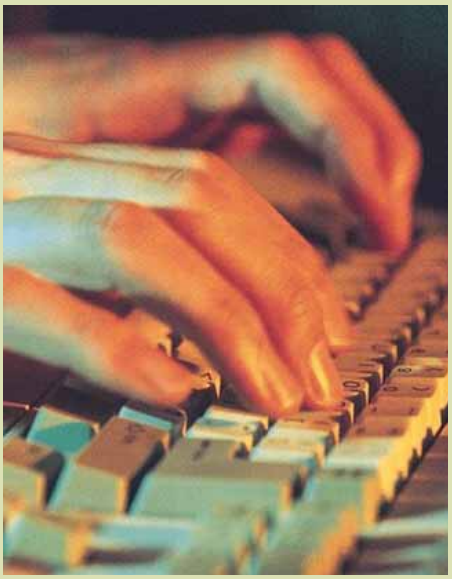
The lack of some security features in software products is usually the result of conscious or, even worse, unconscious decisions made during the design phase of the product. Inherent protocol weaknesses could also be a source of vulnerabilities. Vulnerabilities resulting from protocol security weaknesses should not be confused with vulnerabilities due to mistakes in the implementation of the protocol, which fall under the first category of programming code flaws. Finally, mis-configuration of the product or its (un)intentional misuse can also lead to the existence of vulnerabilities. The flaws created when producing software require the establishment within the vendor's organisation of an internal process for managing vulnerabilities

A Process for Managing Emerging Vulnerabilities

Why do we need a Process?

When a new vulnerability, which is linked to a flaw in the programming code, is publicly disclosed or is about to be disclosed, the time window for a vendor to react can often be quite short, and is even close to 'immediate' in cases when it is made public without any prior warning. Within such short timescales confusion and annoyance, both internally and with customers, are common phenomena. Such confusion can lead to high risks for the vendor in terms of image, reputation and penalties but also for customers, who may be at risk of malicious attacks which take advantage of the vulnerability, if the relevant means to exploit the weakness are also available.

To be best prepared for such situations, it is essential that a well-defined organisational process is in place to deal specifically with the discovery of vulnerabilities in products.



Main Objectives

Such a vulnerability management process broadly aims at:

- enabling the vendor to react on time to newly-discovered vulnerabilities that may impact its products;
- taking appropriate measures to assess the real impact of the vulnerability on the product, or several products, if the vulnerability itself is in a software component that has been used in more than one product;
- making the result of the assessment (whether and if so, how the product is impacted) available promptly;
- defining the course of action for the impacted product(s);

Product teams should assess the impact of the vulnerability on relevant products and make proposals for short- and long-term fixes.

- preparing coherent messages for customers, and in some cases for the press when dealing with publicly very visible vulnerabilities;
- and, last but not least, covering cases where the vendor learns about the vulnerability either from an external or internal source of information.

High-level description and some tips

Although process and its organisational structure could vary from one vendor to another, we can identify a number of major aspects that would be common to all.

One key element is obviously the ability to be aware of vulnerabilities as soon as possible. This can be achieved in various complementary ways:

- by subscribing to well-known public lists where new vulnerabilities are announced and discussed;
- by subscribing to lists and websites of the third-party software that has been used, if any;
- by subscribing to the services of one or several Computer Emergency Response Teams (CERTs) that would not only provide pre-warnings of vulnerabilities but could also play a key role in co-ordinating responses from all vendors and the public disclosure of vulnerabilities.

The interface with these external sources of information can be realised with a central team or distributed amongst the product lines.

It is important to note that customers could also discover flaws in a product. However, although these customers could be thought of as external sources of information, the vulnerability report would typically go via the internal channel of customer support. This specific case must be considered with extra care within the process so that such vulnerability reports are managed by the vendor's global management process.

Once a vulnerability report, i.e., the vulnerability description, is known, it should be passed onto one or more product team(s) that will assess the exact impact of the vulnerability on relevant products. This assessment will provide varied information, including proposals for short- and long-term fixes within already deployed products, a plan for elimination of the vulnerability in future versions of the product and advice to customers on how to detect if their product has been under attack. This assessment can be done in several phases with the aim of minimising time to the development of a short-term fix.

Depending on the severity of the vulnerability and if it is already known publicly, the time window for producing responses (to the customers and, in some cases, the press) may vary but one must be prepared to face such crisis situations.

In providing responses, care must be taken that the relevant details are included in the public response statements, in a similar way to the reports that are published on CERT websites, and they should be kept confidential for customers only. Customer support teams and the corresponding account managers play a key role in delivering the message in a timely and effective way to customers.

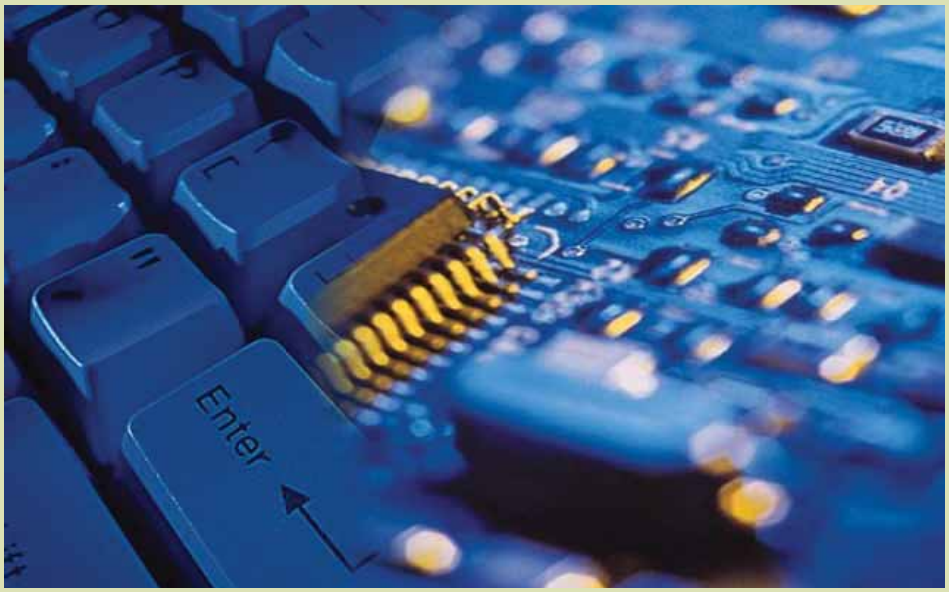
Other Issues

As a vendor, the process of managing emerging vulnerabilities due to flaws in software code is exacerbated with the use of third-party software. It is indeed common in a complex ICT product to embed both software modules developed by the vendor and third-party software modules. This mixing of software adds an extra dimension to the difficulty of dealing with vulnerabilities.

> **"it is essential that a well-defined organisational process is in place to deal specifically with the discovery of vulnerabilities in products."**

In order to be efficient, there should be a well defined list of third-party software components and protocols which the product vendor used in the development process. A careful eye should be kept on the emerging vulnerabilities of all third-party software used; and, conversely, a vendor company would be failing in its responsibility if it did not monitor third-party software it had actually embedded in its product.

Because the real impact of an emerging vulnerability in a product can depend on the deployment mode that may be specific to each customer, it may be more difficult to assess the impact for all customers and still have a single coherent message. Additionally, there may be cases where the solution to the vulnerability is made available only to users who have customer support included in their contracts. This raises the important question of whether security-related patches should be made available even to those who do not hold appropriate support contracts. ➲



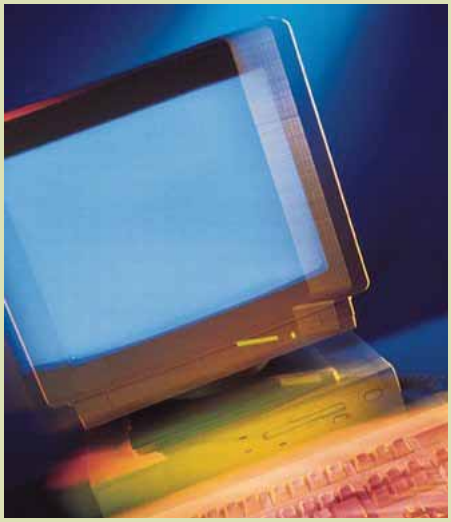
Special care needs to be taken with those customers whose contracts state that they are to be notified of vulnerabilities on an individual basis.

Disclosing Vulnerabilities

A non-disclosure approach is similar to sweeping the dirt under the carpet, hoping that no-one will notice. However, experience proves that all vulnerabilities are eventually uncovered and made public.

On the other hand, proponents of full disclosure (understood as publicly disclosing all details of the vulnerability) will claim that it helps customers to take immediate and appropriate measures. This also fulfils the ever growing demand of customers to be notified immediately of such vulnerabilities. The downside is that this obviously gives more information for potential hackers; full disclosure sometimes comes with an exploit as 'proof of concept', and it goes against the natural human instinct to keep mistakes secret.

So, to disclose or not? This question has raised hot debates in the past and will probably still do so in the future, as there



are strong arguments for both approaches. A responsible disclosure policy will combine the best elements from these two opposite approaches. Several such policies have been developed, such as that of OIS (Organisation for Internet Safety). Responsible disclosure enables us to control what, when and to whom details of vulnerability (including associated solutions) are provided, with a clear commitment from all stakeholders.

Conclusion

Managing vulnerabilities has become a major issue due to the importance of timeliness to respond. Every vendor should seriously consider defining an appropriate process to manage vulnerabilities in products that emerge after they have been sold to a customer. It is important in the definition of such a process that the relationship with customers is taken into account as, under the requirement to be notified, they may have different and sometimes conflicting demands. Last but not least, such a commitment from the vendor demonstrates to policy-makers that the ICT industry is taking positive action towards improving the security of the information society.

Olivier Paridaens is Security Solutions Manager at Alcatel, responsible for security services in IP Transformation projects, and member of the Permanent Stakeholders Group established by ENISA.

On Exploiting a File Sharing System for DDoS Attacks

Elias Athanasopoulos, Kostas Anagnostakis and Evangelos Markatos

Over the last few years we have witnessed an increasing number of Distributed Denial of Service (DDoS) attacks on the Internet. These attacks usually rely on previously compromised hosts, known in the colourful language of cyberspace as 'zombies', which repeatedly request a seemingly legitimate service from a targeted (victim) server on the Internet.

The larger the number of compromised hosts which participate in the attack and the more frequently these hosts request service from the victim computer, the larger the magnitude and ferocity of the attack against the victim. When the magnitude of this DDoS attack reaches a certain threshold, the victim's resources are overwhelmed, making it difficult, if not impossible, to serve any of its legitimate clients. Although it has been widely known that DDoS attacks are not rare, it is astonishing to learn that such attacks exceed several thousand distinct events per week, targeting all sorts of computers ranging from popular web servers to humble dial-up PCs.

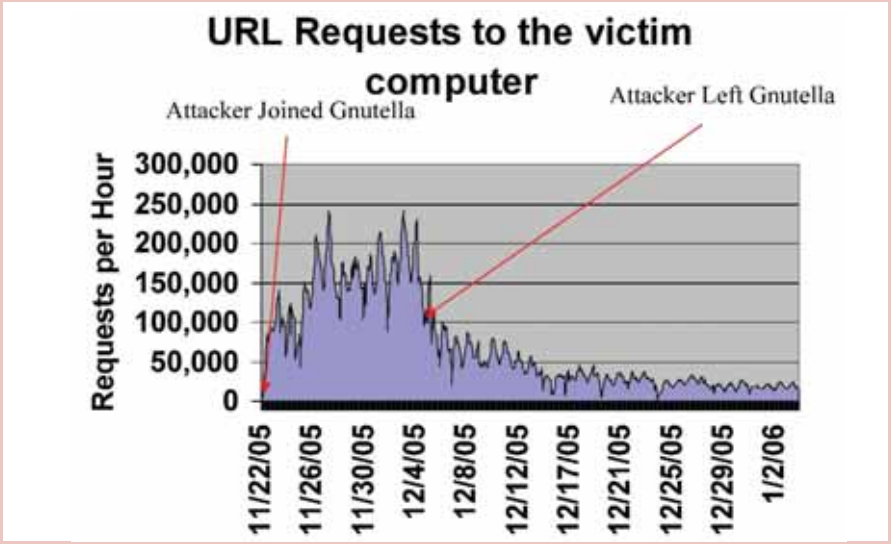
Since Denial of Service attacks require control of zombie computers, the fire power of DDoS attackers is limited by the number of compromised computers they control. Recently, however, researchers at FORTH-ICS – http://dcs.ics.forth.gr/ and http://dcs.ics.forth.gr/Activities/papers/gdos.acns06.pdf – have discovered that even non-compromised computers participating in file sharing systems can be used to inadvertently take part in such a Denial of Service attack. Indeed, by exploiting the technical details of the Gnutella protocol, a popular peer-to-peer file sharing system, it is possible to direct a large number of Gnutella peers towards an unsuspecting victim computer which may not even be part of the Gnutella network.

> **"it is astonishing to learn that such attacks exceed several thousand distinct events per week"**

Transforming the Gnutella network into a Denial of Service attack weapon against a victim computer is based on a simple observation: when a Gnutella peer searches for a file, the attacker always responds that the victim computer has a copy of this file. In this way, the victim computer becomes increasingly popular among a large number of Gnutella peers which repeatedly request all sorts of files from the victim.

➲

Denial of Service attack to a victim computer through the Gnutella file sharing network



Between 22 November 2005 and 4 December 2006 the attacker joined the Gnutella network and tricked Gnutella peers into believing a victim computer had interesting files to download. This resulted in about 150,000 requests per hour to the victim computer. After the attacker left the network in December 2005, tricked Gnutella peers continued to send requests to the victim computer for several more weeks.

Real-world experiments

A series of experiments performed in a controlled environment enabled researchers at FORTH-ICS to measure the validity, magnitude and duration of such a Gnutella-based DDoS attack. To jump-start the attack, they inserted one 'malicious' node in the Gnutella network, which, for a period of about two weeks, responded to all the queries it received, stating that a victim computer has the content requested in the query. The 'victim' computer was a carefully crafted and heavily monitored web server located at FORTH. In this way, over this period of two weeks, the 'victim' web server at FORTH became increasingly popular among Gnutella peers and was the recipient of an increasing number of requests. Indeed, as the graph above suggests, during the period of the first two weeks (when the attacker was an active member of the Gnutella network), the victim computer received an increasing number of requests reaching close to a quarter of a million per hour. Even after the attacker left the Gnutella network and stopped responding to any queries, the victim computer still continued to receive more than 10,000 requests per hour. In total, over the 6-week period of the experiment, more than 300,000 Gnutella peers connected to the 'victim' server and requested to download a file. These Gnutella peers resided in countries practically all over the world. (See diagram below, which provides a colourful and interesting mosaic. All but a handful of grey-coloured countries hosted peers which requested files from our victim server.)

The number of Gnutella peers (which requested files from our 'victim' server) hosted per country varied from low (green) to very high (deep red).

To make matters worse, if the victim computer is hosting a web server, the attacker's response can be carefully crafted so that it contains a URL that matches a file served by the victim web server, effectively deceiving the Gnutella peer into downloading an existing file from the victim computer. Therefore, by tricking Gnutella peers into requesting content from a victim web server, and by tricking the victim web server into thinking that it serves ordinary web clients, the attacker can direct a flood of seemingly legitimate URL requests to the victim computer, abusing its resources. Interestingly enough, these requests towards the victim computer continue to arrive even several weeks after the attacker leaves the Gnutella network and stops sending fake replies on behalf of the victim computer.

> **"attackers do not need compromised computers in order to launch their attacks. They have managed to effectively masquerade the attacks as ordinary activities of everyday Internet applications"**

Although there is ongoing research underway at FORTH-ICS to detect and avoid such Denial of Service attacks, the potential and effective magnitude of these incidents has yet to be fully quantified. One thing is certain though: we have now moved into an era where attackers do not need compromised computers in order to launch their attacks. They have managed to effectively masquerade the attacks as ordinary activities of everyday Internet applications.

Elias Athanasopoulos is a Research Assistant at FORTH-ICS.

Kostas Anagnostakis is a researcher at I²R and visiting associated researcher at FORTH-ICS.

Evangelos Markatos is the director of the Distributed Computing Systems laboratory at FORTH-ICS, a Professor of Computer Science at the University of Crete, and member of the Permanent Stakeholders Group established by ENISA.

Fasten Your Seatbelts, Please!

Security is not just a technical issue – Putting in a word for consumers

Markus Bautsch

A very short history of traffic

In the last one hundred years people have successfully learned how to move and travel in a safe way. Nowadays nobody would ever consider crossing a busy road without first looking in both directions. All drivers have to prove their driving skills by obtaining a driving licence. Both drivers and pedestrians are aware of most of the potential dangers. Overall, this 'system' runs well, even though traffic load is becoming heavier. This situation is due to improved vehicle safety of course, for example, the use of seatbelts, air bags and antilock braking systems and, last but not least, increased user awareness of the potential dangers.

Data traffic only now outgrowing its infancy

But what is the situation with data traffic? Since the invention of the World Wide Web in 1993, both the speed and volume of data transfers has increased enormously in a comparatively short time. Let's be realistic; users of the Internet hardly ever die during a security 'incident'! Despite this, the emerging risks in the cyber world are serious enough and financial losses can be severe, even for non-business users. Most of the time people working in organisations or enterprises are protected by their professional colleagues in the corresponding information security / technology department. However, the millions of home users, who are not fully aware of the risks in the cyber world, are the Achilles heal of the information community. Most people are not aware of the risks inherent in the new communication and information technologies they are using. Unless this awareness problem is solved, we will never get a safer data world. Therefore, educating users is of paramount importance.

Solution to the situation

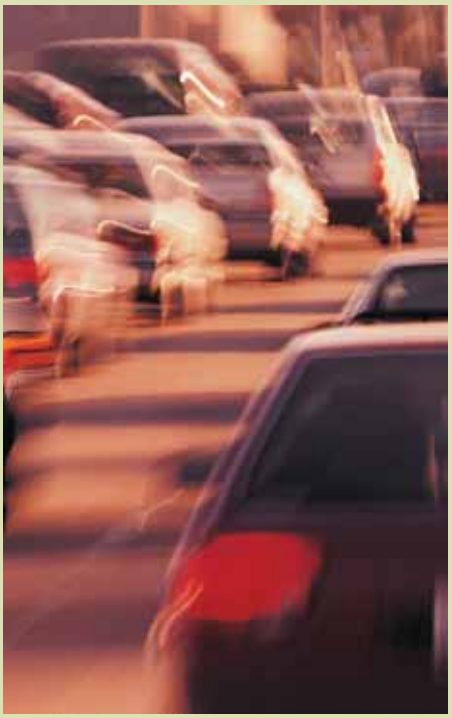
Unfortunately we do not have the same amount of time to establish safe data networking as we had to establish safe road traffic networking; time is running short! It is a pity that many people who are in charge of security initiatives, such as politicians, policy-makers, social scientists and business managers, including those employed by software manufacturers, do not act with the same degree of caution as do information technology security experts; indeed many unfortunately rank at more or less the same awareness level as most people in the private sector!

Of course a single national organisation cannot increase wide scale security awareness alone – co-operation and networking is needed. The formation of the European Network and Information Security Agency (ENISA) was a natural first step forward, as demanded by the importance of the situation. One of the tasks of ENISA is to support existing and future national organisations in their efforts to reach a large number of end users, and to increase their awareness of existing and emerging challenges and risks. ENISA is still young and its activities do not directly target the end user, but there are also a number of other related initiatives and organisations at national level, such as CASES (Cyberworld Awareness and Security Enhancement Structure) of the Luxembourgian Ministry of Economy and External Trade (www.CASES.lu), the Clubs de la Sécurité Informatique (CLUSI), the Italian CLUSIT in Milan (www.CLUSIT.it) or BSI-für-Bürger (Bundesamt für die Sicherheit in der Informationstechnik for citizens) of the Federal Institute for Information Security in Germany (www.BSI-fuer-Buerger.de), which are really worth looking at. But how many European citizens know about any of these initiatives? Not many, I would suspect. This is another symptom which demonstrates the scope of the problem.

Be wise – publicise!

We have a lot of experience when it comes to ensuring a healthy way of life. We are vaccinated, we implement many precautionary hygiene measures, we are aware of the relevance of prophylaxis. If we want to have a safe information data world, we also have to consider a number of measures which are relevant to everyone.

Much work is being done to increase awareness, for example in advertising campaigns with flyers and on certain websites, but the problem is that mostly they only reach the people who are already aware of the risks. One appropriate way to communicate the necessary information to everybody is still to use traditional media, which are broadly appreciated and ➲



The 10 Golden Rules

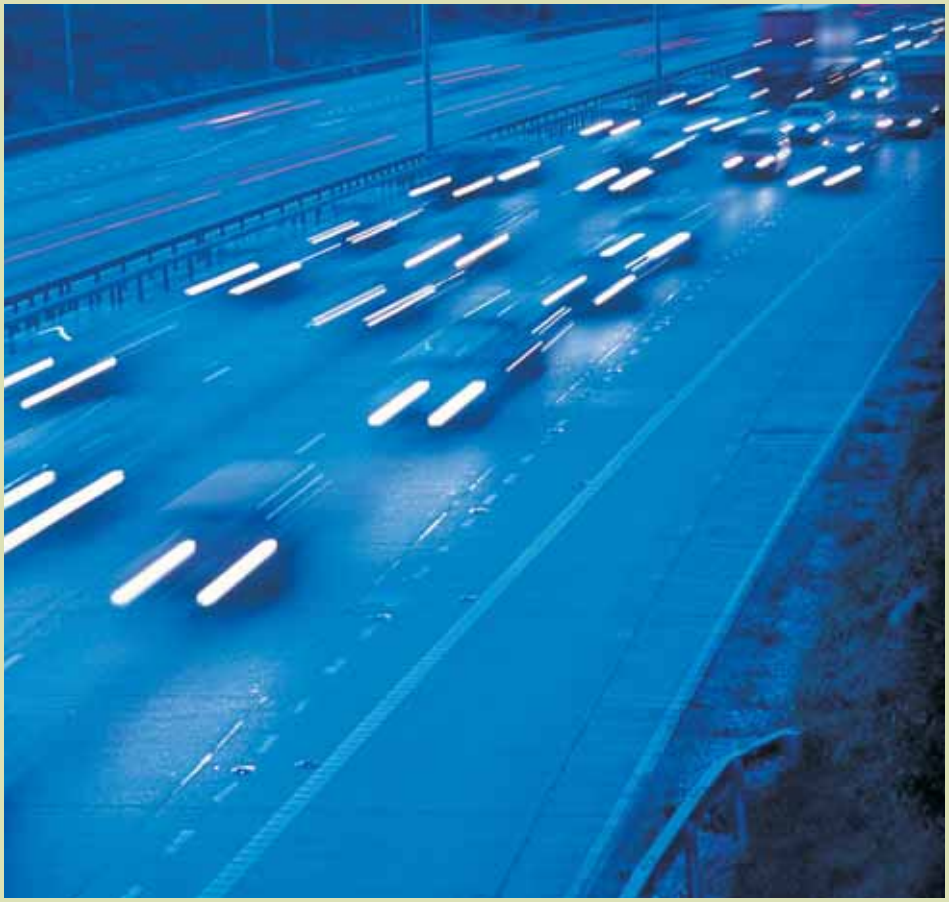
1. Use software updates, especially for widely used software, such as operating systems, browsers, electronic mail and security software.
2. Use anti-virus software and regularly update the virus definitions.
3. Diversify software; use products which are not that widespread, and try to avoid only using products from a single provider.
4. Use a personal firewall and learn how to configure it.
5. Restrict your user rights, even on your own system, and do not use the network as the system administrator.
6. Deactivate active contents, such as Java, JavaScript and ActiveX.
7. Use data encryption as much as possible, and use only secure connections and protocols for sensitive data transfers, such as credit card numbers or personal identification numbers (PINs).
8. Take back-ups of important data on a regular basis.
9. Activate relevant protocols and tools, while keeping activity logs to be able to retrace and understand unexpected abnormal events.
10. Learn to behave properly and cautiously in the field of modern communication technologies.

IST 2006 Conference 21-23 November 2006 Helsinki, Finland

Creating a virtuous cycle between ICT research innovation and socio-economic benefits.

The IST 2006 Conference Programme organised by the European Commission in Helsinki looks at one of the central questions facing European competitiveness.

IST 2006 is being held as the European Commission launches FP7, its Seventh Framework Programme for Research and Development, so one of the main themes of the event will be FP7's ICT objectives and procedures. In addition to the main programme, some purely scientific and technical subjects will be addressed in the networking and workshop sessions.



available, namely broadcasting (radio and television), magazines and newspapers. We must achieve extensive political and social consensus, while convincing media executives of the importance of the dissemination of the relevant network and information security information in a very plain and easy to understand manner.

Important issues

It is equivalent to taking coals to Newcastle for security expert readers, but ten golden rules are really important for network and information security. All users of modern information and communication technologies should be aware of them. To raise awareness, the media should try to emphasise these rules to a wide audience concisely, so that they are easy to digest by all people. Some rules are simple messages which are easily understood by non-expert users; others are more complicated and must be presented carefully in order to be widely accessible.

Going beyond users

Of course users are not the only ones responsible for their own security; software and network providers are also responsible. Unfortunately, many executive managers do not know enough about network and information security. Their actions and decisions are mainly driven by financial considerations. The decision-makers should also be aware of potential security risks and how to avoid them. They should seek to train their staff and hire well-trained entrants to the profession. Therefore graduate schools and universities have a responsibility too, to provide appropriate education in all subjects, not only in terms of technical content, but also security awareness. Last but not least, the pursuit of information security can create new job opportunities!

Are we ready?

As mentioned above, it is essential to offer a broad and comprehensive – but at the same time careful – 'education' for all citizens. Of course this requires great effort, but the result – the achievement of a more secure world – is certainly worth it. Information technology and security experts can contribute a lot, but they cannot succeed only with their ideas, their daily tasks and technical solutions, unless politicians, social scientists and industry decision-makers also recognise the seriousness of the situation and both support and promote the aims of a safe information security.

There is a German saying which is particularly relevant: "The cow is not off the ice, yet!" Let us all pull its halter in the same direction...

Markus Bautsch is deputy head of department at the German consumer organisation Stiftung Warentest, and the stakeholders' representative on ENISA's Management Board.

From our own Experts

Study on Security and Anti-spam Measures (part 2)

Pascal Manzano and Carsten Casper

ENISA has published two reports focusing on developments and trends in security and anti-spam measures taken by network service providers to comply with national implementation of EU Directive 200/58/EC on Privacy and Electronic Communications. The reports confirm that Internet Service Providers (ISPs), telecommunication companies and content providers largely comply with European laws.

The latest report from ENISA contains a synthesis of key facts and conclusions gathered from relevant studies, workshops and conferences, together with proposals to improve the situation that could be implemented by Member States, providers, the European Commission and ENISA. In this article we summarise the main findings of our study.

The report is divided into three parts: increasing transparency, defining appropriate security and setting standards.

Increasing transparency

Reporting of security breaches – While reporting is to some extent mandatory in the USA, reporting in the EU is mostly on a voluntary basis. Meaningful metrics and shared data on security incidents are necessary to increase the transparency of information security and to plan for appropriate and efficient countermeasures.

Becoming aware of a security or spam problem – Many security problems go unnoticed. While the visible level of spam continues to be very high, the nature of the threat changes. More and more spam is unknowingly sent from citizens' computers as so called zombies. Brand names are hijacked and dubious registrars fool domain holders. Some providers see data on threats as proprietary information that gives them a competitive advantage. Furthermore, many still rely solely on complaints from customers rather than proactive network monitoring. They also fail to inform customers about the cost of countermeasures. Providers have to deepen their analysis of incidents, while Europe in general needs a warning mechanism to identify and address upcoming threats.

Defining the appropriate security

State of the art and cost of implementation – Most providers follow so called industry best practice. Many offer free spam filtering or hotlines, sometimes at great cost to themselves. Reported data on damage caused by security incidents are rare, making a cost-benefit analysis difficult. Providers also have to improve customer confidence, for instance by showing compliance with security certificates. Further EU research is necessary.

E-mail security versus privacy – Providers see a conflict between delivering secured services and protecting privacy. Opinion 118 of the Article 29 Working Party on Privacy helps establish the right balance between these conflicting goals. Still, the cost of widespread customised filtering is prohibitive and further dialogue is necessary between privacy and security proponents in the future to improve this situation.

Setting the standards

Technical and organisational security measures – The goal is not to find, but rather to refine, security measures. Quarantining infected computers, securing the Domain Name Service and protecting neighbouring networks should be on the technical agenda. Providing clear contact details, offering detailed guidance to subscribers and raising awareness for identity theft help secure communications from an organisational perspective. Consumer training could be provided in public-private partnerships. Measures depend on the type of business, the size and the maturity of the provider.

Measures to fight spam – In the EU, various anti-spam laws are in place. The challenge is to enforce them, both in Europe and beyond. The Organisation for Economic Co-operation and Development (OECD) Anti-Spam Toolkit, codes of conduct for providers, sender authentication techniques, fines for spammers and initiatives on collecting data on spam all have a role to play. Fear of counter-lawsuits from spammers, the prospect of additional income from dubious e-mail marketing services and the burdensome reporting of spam cases continue to challenge some providers. Awareness of spam and related security threats must remain high.

For more details, please download the ENISA study:
www.enisa.europa.eu/doc/pdf/deliverables/enisa_security_spam_part2.pdf

Pascal Manzano is an Expert in Network and Information Security Policy at ENISA

Carsten Casper is a Senior Expert in Network and Information Security Policy at ENISA

ENISA Workshop on Risk Management

Louis Marinos

ENISA organised a successful one-day Workshop on Risk Management and Risk Assessment on 13 October 2006 in Rome. The objective of the event was to present ENISA's latest findings in the area of Risk Management, to identify user requirements, and to gather user feedback on the subject. The high level of interest in this area was demonstrated by the fact that more than 40 European experts attended the event.

The workshop was organised in three sessions:

- **Session 1:** Tackling present and future results of the ENISA Work Programme 2006. This session also covered the work of the ENISA ad hoc Working Group on Risk Management.
- **Session 2:** Explaining other key activities in Risk Management with speakers and representatives of major European players and initiatives.
- **Session 3:** Focusing on users' requirements. Panel session with a number of major players in the area of Risk Management and representatives of user associations. The aim was to obtain an overview of expectations, current activities and user needs.

Numerous issues were addressed in intensive discussions during the sessions. The following are the highlights:

- Participants emphasised the importance of emerging risks in their work and encouraged ENISA to further elaborate on this issue.
- Participants appreciated ENISA's presentations and underlined the need for the Agency to continue in this direction by adding more examples and best practices, both for current and emerging risks.
- ENISA should provide guidance for SMEs based on size considerations and on the level of confidentiality of the processed information. This could be expressed through profiles, outlining specific threat and protection levels.
- ENISA should act as a catalyst to encourage best practice in Risk Management. Similarly ENISA should participate in the dialogue for balanced regulatory activity within Europe in this field.
- As well as the technical details of Risk Management and Risk Assessment, attention has to be paid to issues of organisational integration. This would increase the effectiveness of methods and procedures introduced in an organisation.
- ENISA should continue with the generation of a knowledge base on Risk Management and with the collection of data on Risk Assessment. This would help both non-experts and experts in applying Risk Management and Risk Assessment methods in their daily businesses.
- In co-operation with other initiatives and relevant bodies, ENISA should participate in the identification of new issues of Risk Management and Risk Assessment as subjects for European research and development.
- In the long term, this workshop should be regarded as a forum to communicate new developments, events and ENISA's findings in the area of Risk Management and Risk Assessment.

Additional information and copies of the slides from all the presentations given at the workshop are publicly available at ENISA's Risk Management website (www.enisa.europa.eu/rmra/events.html).

Dr. Louis Marinos is a Senior Expert in Risk Assessment and Risk Management at ENISA

ENISA Delivers a Comprehensive Online Inventory of Methods and Tools for Risk Assessment and Risk Management

Louis Marinos

A year after beginning work, ENISA is now in a position to present to the public its first deliverable in the area of Risk Management, as described in the ENISA Work Programme 2006.

In 2006 ENISA's activities in the area of Risk Management and Risk Assessment are targeted towards solving problems such as:

- the low awareness of Risk Management activities within public and private sector organisations
- the absence of a 'common language' in the area of Risk Management to facilitate communication among stakeholders
- the lack of surveys on existing methods, tools and good practices.

To meet these needs, especially for the presentation of a common language and inventories of methods and tools, ENISA has

➲

made available substantial information by means of a dedicated, publicly available website (www.enisa.europa.eu/rmra). The site is an extensive knowledge base that covers numerous aspects of Risk Management and Risk Assessment gathered from the experience of many organisations.

More specifically the inventory provides the following:

- A visualisation and detailed presentation of phases and activities of Risk Management and Risk Assessment
- The positioning of Risk Management within an Information Security Management System
- An inventory of 13 Risk Management and Risk Assessment methods used in Europe, with extensive information about each method
- An inventory of 12 Risk Management and Risk Assessment tools used in Europe, with a description of their functionality
- Comparison functions for methods and tools
- A detailed road map for next steps in Risk Management
- A glossary of terms
- Downloads of available reports and description templates for methods and tools.

While all aspects of the inventory are important, we would like to highlight the functions for comparing tools and methods. These functions are customisable according to individual needs.

In the future, ENISA intends to expand this repository of information, adding new methods and tools, examples and demonstrators.

For further information, please contact:
Dr. Louis Marinos, Senior Expert in Risk Management, ENISA
e-mail: louis.marinos@enisa.europa.eu

Sarah Capogrossi, Press and Communications Assistant, ENISA
e-mail: sarah.capogrossi@enisa.europa.eu

Dr. Louis Marinos is a Senior Expert in Risk Assessment and Risk Management at ENISA

Information Security Solutions Europe (ISSE) 2006

A thousand threats, many solutions, one conference

Panagiotis Trimintzios and Andreas Mitrakas

The ISSE2006 conference, held on 10-12 October in Rome, Italy, was one of the most successful to date, with some 350 delegates from 36 countries taking part in over 70 panel debates, discussions and workshops. The event focussed on opportunities, challenges and progress in international information security.

The conference was co-organised by eema, a European e-business industry association, and ENISA. The importance of the event was demonstrated by the wide support of 19 of the world's key IT product and service providers and other industry bodies which participated as sponsors or exhibited their latest products and solutions.

One of the opening keynote speeches was given by Viviane Reding, European Commissioner, Information Society and Media, who pointed out that all of us live in a society based on information and knowledge, and network security is the basis for its trust and expansion. She said that, in order to address security challenges and ensure that Europe gains maximum benefit from legislative and non-legislative actions, all stakeholders should be involved. However, bringing them all together is no easy task. New partnerships are needed to ensure that everyone works together to promote network and information security, and she has therefore asked ENISA to develop a framework of trusted partnerships for data collection.

ENISA's Executive Director, Andrea Pirotti, followed Ms Reding with a brief outline of some of ENISA's work and the scope of its activities. He stressed that the Agency's role is to act as a centre for information sharing and a focal point for network and information security in Europe. Commenting specifically on initiatives mentioned by Ms Reding, he said that a feasibility study was underway into a multi-lingual portal for information sharing and alerts on security issues, and that the terms of reference had been agreed for a data collection framework between trusted parties.

Other highlights for ISSE2006 delegates included keynote speeches from best selling author, and founder and CTO of Counterpane Internet Security Inc, Bruce Schneier, who introduced four core principles of economics in IT (The network effect; High fixed costs, Low marginal costs; Switching costs; and The market for lemons!). In addition, Michael Howard of Microsoft gave delegates exclusive insight into the security challenges and functionality of Microsoft's forthcoming new operating system.

The ISSE debate on 'How do open, closed and commercial security measure up?' concluded that the preference for open or closed software systems is equally divided. Other discussion panels included success stories from national initiatives and, of course, ENISA's information package on Awareness Raising. The panel discussion, 'Bringing security to the end user' which was moderated by ENISA's Ronald de Bruin, offered diverse views on the issue from industry, academia and other security experts.

The technology track included contributions on RFID and data protection, e-ID and smart cards, biometrics and two-factor authentication, face recognition systems for mobile phones, advanced certificate validation for secure, service-orientated architectures, validation for federation and enhanced digital signatures to capture secure document processing requirements. This track also looked at case studies from the USA, IT Grundschutz, and a range of interoperability measures, including those provided by the standardisation body, ETSI.

The legal, data protection and compliance track included discussions on awareness-raising and incident response, IT security vulnerability, early warning systems, critical infrastructure protection, compliance and governance, and privacy aware information lifecycle management. During this session the thorny issues of Internet surveillance, regulatory compliance, the legal aspects of secure grid computing environments, and the impact of the law on monitoring technology were debated. Other presentations considered national e-ID solutions and e-signatures.

During the security management track, we heard about patterns of federation, the Liberty Alliance model, deflecting active directory attacks, the effectiveness of identity management in delivering security, Role-based Access Control (RBAC) and the management of authorisation repositories for identity and access control. This track also examined mobile and wireless, with a look at secure personal end-to-end communication for handhelds and unauthorised wireless connectivity.

At the trusted computing and DRM tracks, the sessions included hardware security embedded devices, next generation electronic devices for consumers, and security architectures for device encryption.

The conference closed with a panel discussion on the ICT security lifecycle. Though many different views were presented, the panel predicted that the most pressing security concerns by 2015 would be privacy, the economics of security, interoperability and how to manage the ubiquitous society.

ENISA will continue to support ISSE, and we look forward to welcoming even more people to ISSE2007, in September in Poland.

Europe Meets to Raise Information Security Awareness

Report from the 2nd 'Awareness Raising' Dissemination Workshop of ENISA

Isabella Santa

On 4 October, the Awareness Raising unit of ENISA organised its 2nd Workshop on Awareness Raising Dissemination to share its findings within the EU Member States.

The workshop brought together policy-makers who are responsible or involved in awareness raising activities in their home countries. Through a combination of presentations, case studies and panel debates, participants explored cutting-edge topics, key issues and emerging good practices in the awareness raising field. Particular focus was placed on public-private partnerships, Small and Medium Enterprises (SMEs), children, and recent and successful government collaborative initiatives with Internet Service Providers (ISPs) aimed at raising awareness among users. In addition, the issue of appropriate metrics to evaluate the effectiveness of awareness programmes was discussed in depth.

The workshop included several speakers who have provided some of the material used for the compilation of ENISA's deliverable, the 'Information Security Awareness Programmes in the EU – Insight and Guidance for Member States'. The findings of this report are the result of an analysis of successful practices and measures already underway in the awareness raising field in Europe.

While presenting and analysing the initiatives and efforts of the EU Member States in awareness raising, a number of similarities and trends were identified:

- The total number of awareness raising initiatives in the EU has risen slightly over the last year
- As in the past, the difference in the nature and number of awareness initiatives derives from the different levels of understanding about information security and the culture of the countries concerned
- Almost every programme in EU countries targeted the SME and Home User groups
- Awareness raising collaboration with ISPs is growing
- Awareness raising subjects that are growing in coverage include the use of mobile devices and WiFi
- Websites and training remain the most widely used communication channels to deliver the message as part of any awareness raising initiative
- Media is still primarily being used as a channel of communication, and not as a target.

The workshop delegates identified the following key prerequisites and necessary action required for a successful awareness raising initiative:

- The message to be delivered has to be appealing and perceived as 'of value' to the target group – the audience should be properly evaluated with interests, needs and knowledge identified
- Communication channels should be analysed to identify and then use the optimal delivery mechanisms – preferred communication channels per target group should be understood and utilised
- Public-private partnerships should be used to leverage synergies to help ensure that the initiative has the resources and expertise to deliver the right message to the right people, using the most effective channels
- Multipliers such as teachers and the media should be used to help increase the scope and coverage of any awareness raising initiative
- Appropriate metrics and Key Performance Indicators (KPIs) should be used to measure the effectiveness of an awareness initiative – lessons learnt through the analysis of quantitative and qualitative data can be used to help improve future campaigns.

It has been concluded that it is crucial to:

- Draw from the experience of other countries as awareness training and campaigns around Europe present many similarities
- Share knowledge as to how to raise information security awareness, and
- Review and re-use material available in different countries.

To this end, ENISA will continue to promote the exchange of information and provide material that could be customised and presented to the EU Member States to facilitate their work on awareness raising. ENISA and the EU Member States will intensify their efforts to influence the public's behaviour towards information security positively, changing the mindset of the human element in order to achieve greater self-awareness.

Isabella Santa is a Senior Expert in Awareness Raising at ENISA

‘CERTs in Europe’

The 2nd ENISA Workshop on CERTs

Marco Thorbruegge

For the second time ENISA gathered together more than 35 participants from the EU Member States and the European Computer Emergency Response Team (CERT) communities for its one-day workshop, ‘CERTs in Europe’, which took place in Brussels on 5 October.

Supported by presentations by well known experts such as Georgia Killcrece from the CERT Co-ordination Centre (CERT-CC) at Pittsburgh USA, ENISA presented its latest deliverable, the ‘Step by step approach on how to set up a CSIRT’. This deliverable is also available online on ENISA’s website: www.enisa.europa.eu/cert_guide.

How to set up a CSIRT?

This concise but nevertheless comprehensive document describes the setting up of a Computer Security and Incident Response Team (CSIRT, a synonym for CERT) from scratch, and sheds light on all relevant processes, both technical and management-related. The work is complemented by many unique illustrations, references, examples, exercises and a sample project plan that can easily be used in one of the available project management tools. Both the guide and the project plan are available for download from the ENISA website.

Discussion, discussion, discussion!

The audience was well balanced between experts from the various CERT communities in Europe and beyond (TF-CSIRT, FIRST, CERT/CC) and project managers who are charged with the setting up of such a team in their home countries. Besides the valuable information that was shared with the expert presentations, project managers had a unique opportunity to discuss their concerns, problems, expectations and plans with the experts who were there.

Two of the most important findings of these discussions were:

- there are no two identical CSIRTs anywhere in the world, but there are core processes in the setting up and the operational phases that are common to all of them

- ‘Think big, but start small’ is good advice for new teams, especially when it comes to the selection of the basic set of services to start with.

New year, new workshop

The evaluation of the feedback forms completed by the participants gave the workshop excellent marks for both organisation and the presentations.

But is there room for improvement? The participants almost unanimously asked that even more time should be devoted to discussions rather than presentations, a demand that ENISA will of course have to meet next year!

The workshop proceedings are published on ENISA’s website: www.enisa.europa.eu/pages/04_01_2nd_cert_ws_2006.htm

Marco Thorbruegge is a Senior Expert in ENISA’s unit for Computer Incident and Response Handling

Information Security Awareness Programmes in the EU: Insight and Guidance for Member States

‘The Information Security Awareness Programmes in the EU: Insight and Guidance for Member States’ details the awareness raising initiatives either undertaken or underway within EU Member States. The information has been compiled based on the responses from the countries and Permanent Stakeholders Group (PSG) members to the ENISA Questionnaire. This data has been supplemented by interviews, research and additional material. ENISA has also constructed good practice recommendations and offered guidance on running awareness raising campaigns. A roadmap has also been created to show a holistic progression of awareness raising initiatives.

The electronic version of this report is available online on the ENISA website and can be downloaded from the ENISA Library, Publications & Deliverables
www.enisa.europa.eu/pages/05_01.htm

For further information please contact Isabella Santa, Senior Expert in Awareness Raising
e-mail: awareness@enisa.europa.eu

From the Member States

The Need for a Clear and Coherent Information Security Policy Framework in Europe: A View from the Finnish EU Presidency

Kristiina Pietikäinen

Since the end of the 1990s, our way of thinking about network and information security has changed considerably. Information security had been viewed mainly as a technical challenge. However, the changeover to an economy based on Information and Communication Technologies (ICT) has meant that information security is now primarily an economic and political challenge. Only very recently have we begun to look systematically at the significance of the economic factors of information security.

An *economic analysis* is often more accurate than a purely technical one, in explaining why information security fails or why there is insufficient contingency for it. The fact is that the level of information security within a business is typically determined by the resources available for it, rather than by what is actually needed for absolute protection against the risks. Investing in information security clearly costs, and will have an impact on competitiveness. However, anyone who would ultimately suffer the potential losses that come with inadequate information security would probably be more ready to invest in increasing levels of information security. An understanding of this raises the political significance of information security and the level of interest in it.

In Finland, network and information security has been high on the top 10 list of important issues, ever since the Finnish Government made a Resolution on a National Information Security Strategy in September 2003. The growing dependence of our society on networks and Information Technology (IT) systems forces us to create policy guidelines and to take part in political debate. Against this background it was predictable that we would choose network and information security as the priority of the Finnish EU Presidency. We feel that there is insufficient discussion, especially on new aspects of network and information security, such as emerging technologies and increased and more sophisticated risks. We feel it is time to revitalise the discussion on these issues.

Indeed, we are also very happy to see what has been happening so far in network and information security at the EU level. The European Commission launched a Communication on 'A Strategy for a Secure Information Society – Dialogue, Partnership and Empowerment' at the end of May 2006. In this Communication, the Commission has taken a holistic approach towards information security, clearly emphasising the economic aspects too. The European Council has also been very active. The Transport, Telecommunications and Energy Council discussed network and information security issues in June 2006 during the Austrian Presidency of EU. In the European Information Society Conference, 'i2010-Towards a Ubiquitous European Information Society', at the end of September 2006 in Espoo, Finland, network and information security issues were the subject of a lively discussion. The Finnish Presidency closed the i2010 Conference, summing up the main findings. Inter alia, one of the conclusions was that it is vital to develop a European-wide vision for a secure information society involving all relevant stakeholders, including the European Network and Information Security Agency (ENISA).

To that end, the Finnish Presidency of the EU has prepared a draft Council Resolution on information security. This will hopefully be adopted at the Telecommunications Council in December 2006. The aim of the Resolution is to recognise the vital role of network and information security for the development of the European information society and the competitiveness of the European economy. The emerging ubiquitous information society provides a new 'threat landscape', which is more complex and difficult to tackle than the current one. At the same time, it recognises that the information society that is evolving offers a long list of possibilities for the European economy.

From the citizen's perspective, the significance of trust should be emphasised, as well as the importance of awareness raising. The respective roles and responsibilities of the various stakeholders should also be recognised. In addition, an important part of the EU's information security policy should be security-related research and innovation, together with standardisation and the certification of products. Last but not least, the European Union must be able to participate fully in combating global information security threats, such as spam and virus attacks, and must be prepared for even worse threats, such as targeted and well planned identification thefts. Overall we must understand that security problems are not only technical, but also social and economic.

From the Presidency's point of view, Europe now needs a clear and coherent security policy framework. Electronic communications technology is taking a major leap towards IP-based and open infrastructures, where security plays a major role. In the near future the European Commission will address new security-related topics such as RFID, spam and cyber crime. In addition, the legal framework of electronic communications will be reviewed over coming years. This also includes reviewing the security provisions in the privacy directive for electronic communications. All these planned actions show that there is still much work to be done in the future on the policy-building area of network and information security.

Finland is strongly committed to enhancing the European information security policy. ENISA should be one of the key players in the European information security field; indeed ENISA was set up to deal with European-wide information security problems. The Agency's tasks and duties are listed in Regulation 460/2004 of the European Parliament and of the Council. The legal basis of the Regulation was confirmed earlier this year by the European Court of Justice. ENISA will be evaluated in the coming months, which has attracted considerable interest amongst many, including the European Parliament. The findings of the evaluation report will give an excellent opportunity to reconsider ENISA's role and status within European security policy. Whatever ENISA's future role, one thing is certain – information security should be an integral part of the political debate around the world. The discussion must go on.

Kristiina Pietikäinen is the Deputy Director General of the Communications Department of the Ministry of Communications in Finland, and the Chairperson of ENISA's Management Board.

Germany's Federal Government Software Strategy and Aspects of Open Source Software

Diversity in IT within the German federal administration through the use of Open Source Software

Martin Schallbruch

The IT systems of governments and administrations today are both vital and sensitive elements of a nation's overall infrastructure. Decisions on software policy are hence not a matter of day-to-day business. Instead, an intelligent strategy with a long-term perspective is crucial for success. This is why the Federal Ministry of the Interior (BMI) in Germany has been pursuing a determined software strategy for many years.

The central aspects of BMI's software strategy include support for open standards and the creation of *diversity*. This approach is not simply a matter of choosing between the world of large commercial manufacturers and the seemingly commerce-free communities that develop Open Source Software (OSS) products in a joint effort. The German federal administration instead advocates *openness* and *diversity* in its IT landscape – in terms of both software products and manufacturers alike.

The reasons are numerous. Software openness and diversity counteract the emergence of monocultures. Dependence on a single manufacturer should be reduced or, better still, avoided altogether. Public agencies must be able to understand and verify the security of their systems. Interoperable processes are a precondition for the interaction needed between public agencies, but also for electronic co-operation with the industry and the business community. Openness and diversity support competition and promote economic efficiency.

Open Source Software

In accordance with its strategic aims, BMI has recognised the enormous potential of OSS and has started implementing OSS products in numerous projects and supported programmes at a very early stage. Besides reducing the dependency on commercial vendors, another important benefit was the increasing security assurance through the use of OSS that has been produced in-house, customised or inspected. Software diversity and the use of open standards could be the basis for IT security. The purpose of software diversity is to avoid monocultures which are easy to attack. Software diversity could also lead to a wider choice of software and thereby reduces dependence on individual manufacturers.

Security is a process that is affected by many factors. The security of a system depends, for example, on the software *implementation*, the software *architecture*, the *protocols* used and the *configuration* of the software. However, just as much as with proprietary software, OSS does not in itself guarantee a secure system. OSS does, however, offer certain technical and strategic advantages compared with proprietary software, which are due to the inherent lack of restrictions in terms of use and usability, learnability, extensibility, openness and the ability to redistribute. This freedom ensures that the software used can be subjected to thorough security checks at any point in time.

The German Federal Office for Information Security (BSI) has already carried out various security checks on open source software. With this strategy, mere trust in a manufacturer can be replaced by in-house knowledge of software security gained during security checks. Since there is no non-disclosure agreement in place to prevent publishing words of warning about security shortcomings in software, with our security checks we are able to help the wider community towards more secure software; users can be informed at an early stage about omissions in security and can take appropriate action.

➲

From Software User to Provider

The German federal government is not just a simple user; it has also become a provider of open source software. In recent years BSI has developed several OSS tools.

One example of this is the Kolab server. The collaborative Kolab software is a groupware server that provides e-mail, a directory service and web services. Modularity, flexibility and openness were central elements in the development of Kolab. Proved and tested open source software components, such as the Apache web server, Postfix e-mail server and OpenLDAP directory service, were combined to form a groupware solution. From the financial point of view, it would not have been feasible to develop such an advanced application without the ability to use existing software as a basis. By simply adding extensions and customising other open source software that was available in the Internet, we managed to complete this project at minimal cost.

In the Ägypten project we developed another open source software system for protecting communications in networks. Based on the Kontact groupware client and its further development by BSI, a secure system for e-mail communications was created using the Sphinx standard (ISIS/MTT). Besides the use of S/MIME encryption and signatures, Kontact also supports encryption using OpenPGP and Chiasmus.

Signature management and encryption compliant with the OpenPGP standard are available to users of Microsoft Windows with the Gpg4win (GNU Privacy Guard for Windows) open source software. This software package, commissioned by BSI, is based on widely used encryption components and combines these to form an easy-to-install package. Graphic user guidance in German and German user manuals, which explain how to use the software itself as well as the background to the cryptography, complete the package.

BSI also offers open source software for checking systems in a network. Although the BSI Open Source Security Suite (BOSS) was developed primarily for administrators and auditors, especially within public agencies, it is also available to companies and private users. BOSS is not only capable of checking the security of any particular computer in a network. It can also control centrally and perform local checks on GNU/Linux computers using various PSS (Production Systems Support) security tools.

Thus independence and software diversity, as well as the use of open standards, form the basis for IT security. However, security is first and foremost a process. In order to maintain IT security, those responsible need a precise knowledge of the system, they must regularly service the system and must close security gaps as quickly as possible.

However, not all of the aspects of diversity and openness discussed in this article have been fully achieved yet. The Federal Ministry of the Interior is hence determined to further promote the use of OSS. Another important issue is the flexible use of software. In concrete terms, this means that those in charge of IT decisions within public agencies must be enabled to identify and avoid dependencies.

The Migration Guide

In an effort to support this decision-making process, BSI commissioned the preparation of a Migration Guide ('A guide to migrating the basic software components in server and workstation computers'). IT decision-makers are allowed to implement the most favourable software applications and software for their particular needs in the most efficient manner possible.

The Migration Guide draws on the experience gained with our pilot projects. We describe different starting scenarios, success factors and recommendations for action needed to support IT managers in

public agencies when deciding between 'replacement migration', i.e., replacing existing licenses and products with open source software, and 'continuing migration', i.e., the continuing use of existing licenses and product lines. Comparisons of technical aspects and detailed cost estimates, evaluations of economic efficiency and a chapter on legal aspects make this 500-page document a reference book with a strong focus on practical aspects.

The first version of the Migration Guide was published in summer 2003. A second, updated version was released in autumn 2005. The tremendous demand it has elicited bears witness to its enormous impact; there have been some 100,000 downloads of the first version and translations into many languages. The publication can be found at www.kbst.bund.de/migrationsleitfaden/. It is available in both German and English.

Clearly, the trend towards greater variety in software, especially embracing OSS, is a crucial factor in the drive towards economically effective and secure government IT.

Martin Schallbruch is the Chief Information Officer at Germany's Federal Ministry of the Interior.

Reducing the Negative Impact of Security Incidents: an example of good practice from Lithuania

Cyber security software distributed free-of-charge to Lithuanian ICT users

Rytis Rainys

Apsaugok savo kompiuterį!

On 15 June 2006, the campaign 'Protect Your Computer!' was launched in Lithuania to increase network and information security in the home users' domain. As part of the campaign, the Lithuanian Communications Regulatory Authority, in co-operation with 16 partners from the public and private sectors, produced more than 100,000 CDs that contain all the essential software for protection against computer viruses, spam and harmful content on Internet websites. This material was distributed free-of-charge to ICT home users.

Recognising that robustness and trust in information and computer technology (ICT) networks and applications are crucial for the sustainable development of the information society, private and public sectors, as well as end users, are seeking to develop a strong network and information security culture in Lithuania. This special multi-partnership project was organised to raise public awareness of cyber security and to prevent the negative impact of cyber incidents on home users.

The CD offers home users advice and suggestions on how to secure the privacy of a computer and information contained in it, as well as easily installable software to combat cyber threats. The provision of a practical means for home computer users to safeguard their software and hardware against cyber attacks and incidents at no cost is intended to encourage wider usage of protection tools by the general public.

The CDs were developed and produced as a result of an extensive collaboration between the private and public sectors, with particularly significant contributions from some software vendors. The CDs were distributed at public Internet access spots in district centres and rural areas with the support of the Ministry of the Interior and the alliance, 'Window to the future', as well as through branches of the Communications Regulatory Authority in the major cities of Lithuania. The Ministry of Education and Science facilitated the distribution of CDs to all high schools in the country.

Finally a virtual CD is available for other interested parties at: www.esaugumas.lt, which is the national comprehensive website on network and information security in Lithuania. We hope that our programme of reaching out to a wide audience of end users, both raising their awareness and providing the security tools they need, will be an example that will be followed by increasing numbers of public authorities around the European Union.

To date, more than 35,000 programs have been downloaded from the virtual CD site. During the project implementation process, in co-operation with the Ministry of Education and Science, the CD was released to all secondary schools in Lithuania, which are now using it for educational purposes. Generally we have received very positive feedback. By making programs freely available on the CD, we expect now to see improved security for end users throughout Lithuania, as more people use safeguard tools.

Rytis Rainys is the Head of the Network and Information Security Division in the Communications Regulatory Authority of the Republic of Lithuania

Lessons Learned from Risk Analysis in National Networks

An Example of Best Practice from the Netherlands

Bill van Mil, Annelies Dijkzeul and Ronald van der Luit

In today's society, all sorts of products and services rely on ICT (Information and Communication Technologies) and energy networks. It is true to say that ICT and energy are the engines that drive all of society's processes today.

The Ministry of Economic Affairs (EZ) is the department responsible for safeguarding the provision of ICT and energy in the Netherlands. EZ has implemented a policy geared to ensuring continuity of supply within these two sectors that include a network infrastructure. As part of this policy, EZ regularly conducts a risk analysis at the national level. The objective of this analysis is to reveal all risks that threaten operational continuity and to evaluate whether the government must take extra measures to combat these risks.

The question is really what makes a good risk analysis? What are the dos and don'ts? To answer that question, last year EZ undertook research into relevant best practices. The results of this study are presented in the book 'Risk modelling handbook, Selection of models and methods for conducting risk analyses', which was compiled by two of the authors of this article on behalf of the Netherlands Ministry of Economic Affairs. The handbook is written in English and is available online in the publications section at: www.minez.nl/content.jsp?objectid=145247.

In this article we present the most important lessons learned from this study. We found that, while performing risk analysis at a national policy level, it is important to take into account the different perspectives of three relevant roles: the risk analyst, the policy advisor and the process manager.

The Risk Analyst

A risk analyst continuously asks him or herself how to build up the most complete image of the risks that is possible. The risk analyst wants to collect all of the information for inclusion in the analysis. For the risk analyst, mapping out risks is an objective in itself. The lessons learned for a good risk analyst are the following:

- **One should consciously choose as a starting point a scenario or an effect that must be prevented**

The first lesson is that there are two possible primary approaches for conducting a good risk analysis. The first is to specify threat scenarios and initial events, and then determine the consequences these scenarios and events would have. Based on the analysis of the consequences, measures can then be formulated. That is the standard methodology.

Another approach starts, not by determining the threat scenarios and initial events that might cause a malfunction, but by formulating situations that must be prevented: worst cases scenarios or 'situations to be prevented that have maximum effects'. Then one works backwards from the consequences, i.e. what circumstances, events or causes could create such a situation?

Finally, what measures can be used to prevent these circumstances? The second approach supports the argument that there are thousands of threat scenarios and that it would therefore never be possible to produce a complete list of all the threats. Trying to envisage all these scenarios is a time-consuming task and ultimately this approach would not result in the formulation of measures to actually prevent the worst case scenarios.

A good risk analyst should make a conscious and explicit choice between these two approaches or combine the two approaches, and justify that decision.

- **One should not hide the lack of certainty, but should make it transparent**

In risk analysis, the goal is often to achieve a uniform outcome. For example, the likelihood that a specific situation will occur must be specified. The attempt to arrive at consensus and to achieve uniformity is the focal point. The danger is that, in striving for consensus, the outcome may be a compromise between two randomly selected experts. This may result in assuming that the risk of occurrence is certain, while in fact this may not be the case at all. Failure to distinguish uncertainty may then have an undesirable effect on the analysis.

This is also referred to as the phenomenon of 'reproducibility'. If the same risk analysis is conducted twice, what is the chance of the outcome being the same, or close enough to the first outcome, that the final outcome of the risk analysis is the same in terms of possible measures? A good risk analyst should ensure that uncertainty during the analysis remains transparent, particularly if quantitative methods, that might create a false sense of security, are used.

The Policy Advisor

The policy advisor in our example continually tries to identify the role of the government in taking measures to combat risks. Moreover, the policy advisor is a political servant too and must therefore also consider political interests during the risk analysis process. This means that the policy advisor should be pragmatic, and specific risks must be mapped out within a very short time. The lessons learned for a good policy advisor are the following:

- **Links between the management of public confidence and awareness**

Policy-makers have to deal with actual risks, as well as the risks perceived by citizens and companies. There are threats and risks that are small, but which citizens and companies may regard as significant. That raises difficult questions in terms of dealing with such threats.

Increasing citizens' sense of security requires managing public confidence. The government must indicate when citizens have no reason to worry about a potential risk, for example, when the risk is rather small or when one must accept the fact that a genuine risk exists. However, the consequence of this could be that citizens become less cautious and stop taking precautionary measures which they had taken in the past. In turn, this increases the risk, which can be one reason for managing public confidence or making citizens aware of the risks.

Effective policy staff will strike a balance between the management of public confidence on the one hand and the management of awareness on the other.

- **One should work cyclically and iteratively rather than chronologically**

A strict, rigid step-by-step plan is often followed when conducting risk analyses; the first step must be completed before the subsequent step can begin. A disadvantage of this chronologically ordered plan is that a great deal of information can be lost.

When studying threat scenarios and vulnerabilities, obviously solutions for eliminating those vulnerabilities will appear. By organising these steps as separate units, one runs the risk that the only result of the vulnerability analysis is an indication of vulnerability and that all the information regarding countermeasures that was identified during the analysis will be lost. By the time it comes to formulating measures, the suggestions made during the process may have been lost, either because individuals have been replaced or because ideas were never written down. Then, in the last phase, measures have to be pulled out of a top hat. And at the same time, if a policy advisor is under time pressure and is forced to provide output in the short term, an iterative process, where analysis and formulating measures is combined, can help achieve results quickly.

The Process Manager

The process manager continually tries to specify and manage the role that various persons and organisations play in the risk analysis process. The process manager explicitly focuses on developing broad-based support. The lessons learned from our study for a good process manager are the following:

- **One should respect and anticipate 'coloured' input**

The parties involved – such as companies and public managers of infrastructures and objects – have both a role to play and an interest in the risk analysis process. What they contribute to such a process can depend in part on the role they fulfil – 'Where you stand depends on where you sit'. This can lead parties to consciously or unconsciously downgrade certain risks, while overemphasising others, for example, because other parties are responsible for those risks, or to try to have extra government resources allocated to improving the safety or security of their particular product or service (which then strengthens their competitive position internationally).

A good risk analysis process leader respects the fact that the parties involved bring their own specific interests to the task and does not attempt to prevent this, but rather tries to exploit these differences. For example, the people involved in setting the list of potential measures within a sector should not be the same as those implementing the proposed measures.

- **One should prevent 'group thinking' and consider differing opinions**

In expert meetings, the chance of 'group thinking' is high. The party who is first to say something about the nature or scope of a risk, for example, is deemed correct. The other parties involved do not have arguments at hand that enable them to enter the discussion, even though their own estimates of the nature or the scope of a risk may be completely different. A good risk analysis process leader should attempt to anticipate and prevent 'group thinking', for example by ensuring that assumptions are discussed, that counter-arguments are organised, that all sides of the question are heard and that critical questions are asked. In practical terms, this can be accomplished by involving an expert with opposing views, obtaining a second opinion, or by organising a knowledge competition, i.e., by asking two or more renowned experts or institutes to offer an option based on their vision.

- **One should view the process as the prelude to broad-based support and implementation**

In most situations, the recommendation is not to wait until the last minute to inform the parties involved of the results of a risk analysis, but to include them in the process in a timely manner and allow them to influence the outcomes of that process (naturally without jeopardising the special responsibility the government has to define appropriate measures). After all, giving parties influence over the outcome of such a process enables them to commit to the outcome at an earlier stage.

Moreover, by consciously involving specific parties in the risk analysis process, not only can broad-based support be developed for measures that may have to be taken, but the awareness of the parties regarding risks is also increased. Such awareness can already be a result in itself, for example, because parties involved take follow-up action within their own organisations. Thus, the involvement of these parties is extremely relevant. A good risk analysis process leader utilises the process as the prelude to implementation.

Conclusions

There are countless strategies and tactics for conducting risk analyses. The desired approach depends on the goal of the particular analysis, the characteristics of the service or sector, and the time and the expertise available, both within and outside the department. It is important to take into account the lessons learned for all three different roles and perspectives outlined above when applying risk analysis in the ICT and energy public networks. This will make possible a better assessment of the nature and scope of risks threatening the continuity of supply and will offer a clearer picture of the measures that must be taken, based on proper priorities. It could also help improve an organisation's risk analysis policy, ensuring it is well substantiated, understandable and based on sound argument.

Bill van Mil is a senior consultant at Berenschot and a PhD candidate at Delft University of Technology.

Annelies Dijkzeul is a consultant at Berenschot.

Ronald van der Luit is Senior Policy Advisor at the Ministry of Economic Affairs, dealing with network and information security.

What can we achieve with information security certification?

Voice your opinion on information security certifications in Europe

Call for Participation and Contributions

ENISA Workshop – 28 November 2006

Sofitel, Athens Airport, Greece

Workshop Goals

The goal of this workshop is to assemble and discuss opinions about the use of information security certifications in Europe. We invite experts on security product certifications (e.g. Common Criteria), people certifications (e.g. CISA, CISSP) and process certifications (e.g. BS 7799) as well as organisations that use, governments that promote or vendors who provide such certificates. The preparation of the workshop is important, and participants are invited to submit presentations or position papers prior to the event. A draft report will be proposed to the workshop participants, discussed and agreed upon. Where it is necessary, conflicting opinions will be noted. The report will be finalised after the event and presented to ENISA's stakeholders (e.g. the European Commission, Member States, industry and academic representatives).

Call for contributions

- All interested parties are invited to present their position in 15-30 minutes. We anticipate 6-10 presentations. The rest of the time will be reserved for discussion, working especially towards the creation of the report.
- Interested parties who are unable to attend can also contribute a one-page position paper to the event (1 page DIN A4, PDF). ENISA will screen all papers for relevance and distribute them to workshop participants prior to the event.
- An alternative means of expressing an opinion is to complete the short questionnaire on information security certification schemes that will be circulated prior to the event. Answers can be given as multiple-choice (5 minutes) or in detail (20 minutes).
- Participation in the workshop is free of charge. Presentations and registrations are due by 15 November. Please see www.enisa.europa.eu/pages/certifications for all logistical details.

Background

Europe is concerned about the state of information security. There are numerous actual and perceived IT security risks – and these risks have to be managed. To do so, organisations employ experienced staff, define processes and deploy products. But how does an organisation know that staff, processes and products are appropriate to help mitigate the risks? The use of accreditation and certification schemes is considered as one method of describing the usefulness of a product, process or person. However, a lack of general recognition of certifications hinders an uptake of this market. On the other hand, wide recognition and the improved visibility of such schemes would help providers and users of certifications and make the market more open and dynamic.

During the workshop, participants will discuss whether and how accreditation and certification schemes help to ascertain value and when a scheme can be considered successful. Participants will also discuss whether user organisations, governments and vendors need to do more – or if they should do less – with regard to such schemes.

ENISA Workshop

Finding a common language to describe security levels of authentication methods

29 November 2006, Athens, Greece

ENISA is looking for national and international experts in the field of authentication who can help identifying a common language for security levels of authentication methods. The goal is to facilitate interoperability and mutual recognition of electronic authentication schemes for the benefit of citizens and enterprises.

The group of experts will discuss ways to harmonise existing languages for the classification of authentication levels and to define a commonly accepted definition for each term and each level. If you are aware of a language or a method that could be used to describe levels of security of authentication methods – either in your company, in your administration, or in your field of research – or you want to suggest additional ideas, your input will be appreciated as well.

ENISA will invite the experts to share information on authentication methods and to discuss the different ways used in Europe to describe the level and appropriateness of such methods. The relevant players will present their views at a workshop on 29 November 2006 in Athens.

Please join this group of experts or request further information by sending an e-mail to Pascal Manzano at pascal.manzano@enisa.europa.eu .

ENISA wishes to thank all the contributors to the publication. Please remember that all contributions reflect the views of their authors only, and are not in any way endorsed by the European Network and Information Security Agency. ENISA assumes no responsibility for any damages that may result from use of the publication contents or from errors therein.

The ENISA Quarterly is published once each quarter. You may sign up to the ENISA Quarterly by sending an e-mail to press@enisa.europa.eu with "subscribe" in the subject line. To unsubscribe send a mail to the same address with "unsubscribe".

Editor-in-Chief: Panagiotis Trimintzios
eq-editor@enisa.europa.eu

More about ENISA

For the latest information about ENISA, check out our website at www.enisa.europa.eu