enisa
European Network and Information Security Agency

Newsletter

06/2005

IN THIS EDITION

A WORD FROM THE EXECUTIVE DIRECTOR

Dear Readers,

I am delighted that you are reading the first issue of the ENISA newsletter. ENISA is a new Agency but we have been working very hard to make an impact and we are sure this newsletter is a step in that direction.

I would like to thank all of you who have been so enthusiastic and positive in helping ENISA in its first steps. We have received tremendous support from Member States through the ENISA Management Board and network of national liaison officers. We have also developed excellent relations with industry through our Permanent Stakeholders' Group, working groups, and direct contacts with many companies and organisations. Lastly we have maintained an active dialogue with international bodies and concerned organisations and users. The interest and support for ENISA amongst all of you has been of great importance and we intend to carry this momentum forward as we continue along our path.

ENISA has developed a number of channels for exchanging information – through our website, through conferences and events, and now – through the ENISA quarterly.

The newsletter is meant to share information on NIS-related news, best practices, and activities across Europe. The primary audience is policy and technical experts dealing with NIS both in EU institutions, Member States, and the private sector. But the newsletter could potentially be of interest for anyone dealing with information security in Europe.

To keep the level of the content high, it will be aimed at the informed community and not the average person; it is not meant as an awareness campaign aimed at the average person. On the other hand, the newsletter will not contain highly technical articles that deal very in depth in one particular topic. On very specific technical topics, the purpose of the articles will be to explain to a more general informed audience what the significance of the development is.

Our first edition will give you a peek into what we are doing and also contains some

Ā

ISSN 1830-3609

CIIP LONDON CONFERENCE GETS ENISA INPUT

The UK's National Infrastructure Security Co-ordination Centre, which is tasked with defending the nation's critical computer networks from electronic attack, is organising a Critical Infrastructure Information Protection (CIIP) Conference in London this October.

As more and more critical infrastructure networks become interdependent, the threat of external attack increases. This event will look into how these complex issues are being addressed.

The event, at Greenwich, is an 'invitation only' conference for government. It aims to highlight CIIP issues across the globe.

NISCC already maintains a CIIP contact directory on behalf of the G8 group of nations.

The conference will feature keynote contributions from senior figures. Plans are also in hand for a number of workshops. ENISA will play an important role in driving forward the event agenda.

It also marks the UK's presidency of the EU and chairmanship of the G8 group. |

valuable contributions from industry and Member States. Eventually, we look forward to bringing you these and other topics:

- Technical developments in NIS.
- Policy developments in NIS.
- Conferences/events/workshops in the area of NIS.
- European and international developments in NIS (while focusing on European ones initially).
- Trend watching, particularly for new technologies.
- Sharing experiences, mistakes made, best practices, etc.
- Providing a bird's eye view of what is going in NIS.
- ENISA's own activities.

Although a newsletter may seem quaint in our age of always on, always new information, we hope that this newsletter will allow you to take a step back and get updated on ENISA from the train, over your morning coffee, or over lunch. We promise to continue doing our utmost to provide you with a quick and valuable look into the world of information security from the unique vantage point of ENISA's scope and mandate.

ENISA is entering a challenging and exciting period as we seek to fulfil our mandate as a unique European entity dedicated to network and information security. We are also currently in the midst of our transition to Heraklion, Crete. This move poses numerous, logistic and technical challenges but with the enthusiastic help and support of the Greek authorities we are sure that Crete will become a warm and productive home for our Agency.

We look forward to an exciting exchange of ideas, information, and thoughts in the newsletter forum.

Wishing you a very pleasant read,

Yours Truly,

Andrea Pirotti

ENISA update – what we've been up to

ENISA is a small agency which began operational work at the beginning of 2005 with a small number of seconded national experts. However, we are proud to report that we have been able to:

- finalise the work programme for 2005 and discuss the draft 2006 work programme through a solid discussion with Member States and industry.
- create and convene the Permanent Stakeholders' Group (PSG). The PSG brings together experts from industry, academia, and users' groups, and has been an invaluable tool for ENISA in liaising with these communities.
- create and convene three working groups in the areas of CERT cooperation, awareness raising, and technical and policy aspects of risk assessment and risk management.
- forge strong links with the European Commission in areas such as security research.
- collaborate with international organisations such as the ITU in the preparation of security related conferences (most recently ENISA cooperated in the ITU/EU (ENISA) regional seminar on cyber security for CEE, CIS and Baltic States held in Riga, Latvia).
- prepare work in tracking standards and technical developments.
- create a network of national liaison officers. This network helps ENISA liaise on a day-to-day basis with Member States. ENISA held successful meetings in London, Paris, Budapest, Berlin, Copenhagen, Madrid, and Warsaw, where all 25 Member States were represented.
- complete the first wave of recruitment.
- prepare the new ENISA website and country pages. |

OPINION AND COMMENTARY

By Nick Coleman

DO WE NEED TO BE MORE PROFESSIONAL?

Let's face it – if we were doctors, lawyers, accountants or even airline pilots we would have to sign up to a code of conduct, pass recognised qualifications, and get some proper experience before we could 'fly solo'.

However as information security professionals we don't need to do any of that.

In most arenas anybody can be a consultant, conduct a risk assessment, or manage a security incident if the organisation is willing to pay them.

This is quite understandable: industry has grown up in a random, organic manner, without much structure, and without any formal professional requirements for those working in the industry.

Might it be time for that to change?

The cost to business of getting it wrong is getting substantial both in terms of damage to brand reputation, as well as operational expense.

Independent market researchers NOP estimated during the last 12 months alone electronic attacks cost large UK businesses 2 billion euros.

The spate of blackmail and extortion attempts, as well as viruses and phishing scams, have increased business focus on IT security, and today the worldwide market for information security services is estimated at USD 15 billion.

Governments have also increased their focus on IT security, with the creation of ENISA and new regulations extending to IT Security such as Sarbanes Oxley and the data protection directive being clear signs of this.

As regulations come into force directors and executives in organisations are asking for their staffs to be able to certify that they have adequate protection systems in place.

But how do people demonstrate they are competent to certify the systems are adequately protected?

Is it the length of time you have been in the job, or that you have passed a technical qualification? Doctors, accountants, lawyers, surveyors, architects, psychologists all have professional institutions to guide them.

Has the time come for information security professionals to also go down this route?

How can we evaluate the need for a profession?

Is it more than just regulation which is driving us to look at professional standards?

There could be other drivers as well as the regulation:

- getting adequate financial remuneration, a recognised pay scale, with a way to benchmark people and skills levels
- dealing with the issues of skills shortages
- removing/marginalising the 'incompetents' that drag down the industry?
- creating a career in information security
- being able to influence the future direction of the industry, and give informed opinions on key issues

But it might be that regulation is a good opportunity to get professional standards work further developed.

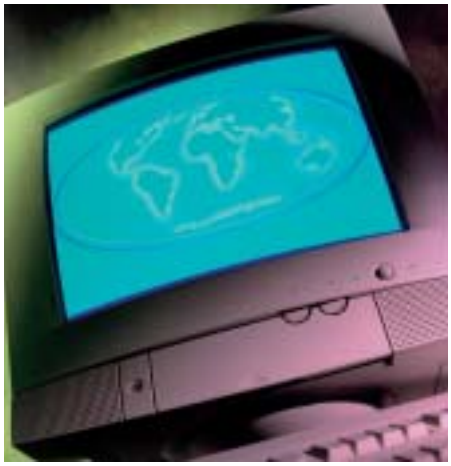
Even if the regulation does not specifically ask for it at this time, it may do so in the future.

Is it a national or international issue?

The world of business going global means regulation not only has to be implemented worldwide, but that IT security also needs to be done on a global basis.

Looking at my fellow members on the Permanent Stakeholders Group at ENISA it is perhaps no surprise that most have a large international perspective to their careers.

The technical qualification CISSP also bears out this international dimension: 33,000 have now passed the qualification, be they in Singapore, Brazil or one of the EU countries.



What does it take to be a professional?

Knowledge, integrity and judgement, says Paul Dorey, fellow member of the PSG at ENISA and Head of Digital Security at BP.

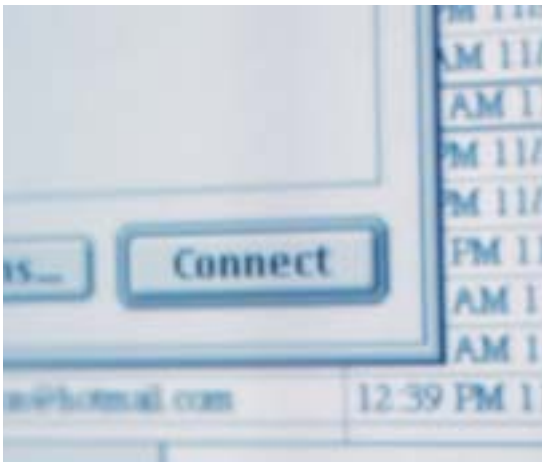
Judgement may actually be the hardest to evaluate, but still no less crucial, called upon for example to decide the right level of security for the organisation.

In the words of one chief security officer – get it wrong, at best you have wasted money, and at worst you could create a corporate catastrophe.

What is going on to address the issue?

In 2004 a group of 15 people got together, including people from academia, industry, industry groups, vendors and government.

The group published a blueprint; a copy of the blueprint is available at www.uksaint.org (SAINT is just hosting content for the group).



This then led to the creation of four working groups looking at the different areas around professionalisation:

- running an institute
- body of knowledge
- code of conduct
- skills & education

The results of the working groups will be published by the end of July; what is clear is that this is an international issue.

Across the EU and other parts of the globe there has already been lots of interest.

It is early days, but at the very least we are getting close to defining the requirements for professionals in our industry, something we have not done before.

The critical next step will be to have the community comment on the outputs from the working groups.

How will we know when we have got there?

If there is development and the profession moves forward, we should see that the challenges we had before are no longer challenges.

Paul Dorey relates this to being able to tackle new challenges, and seeing the things that used to be problems become routine.

Comments / Further information

The group have encouraged people to input; in fact they feel it is essential that this happens.

You can comment, have more information, or get involved in the work around professionalisation.

Visit www.uksaint.org or contact Barrie Wyatt (Barrie.Wyatt@nottingham.ac.uk), who runs the secretariat for the group. |

This article was written by:
Nick Coleman,
Ukcolemannick@aol.com
Member, Permanent Stakeholders Group, ENISA

European Network and Information Security Conference

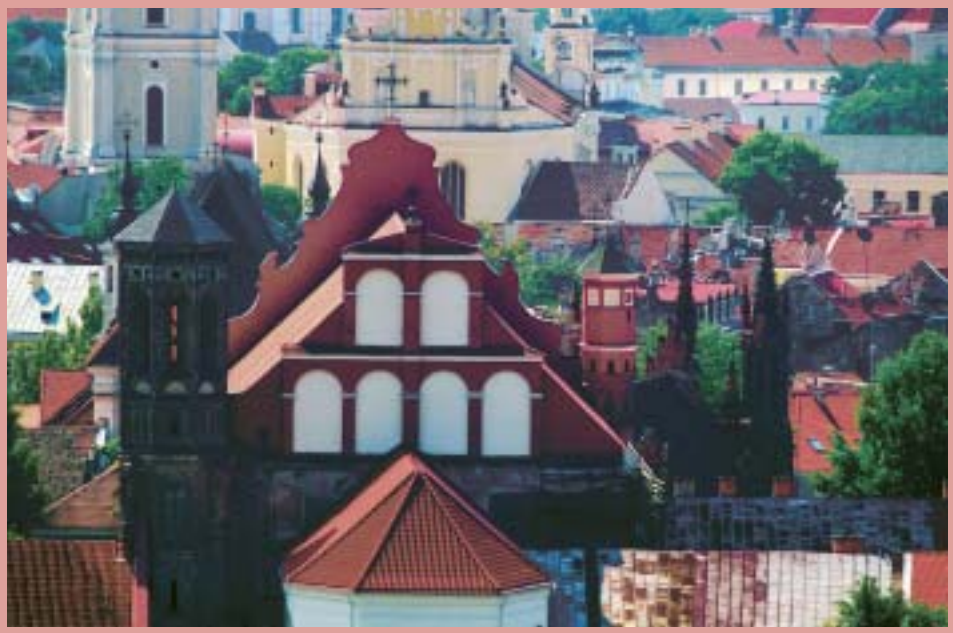
Readiness for Handling Network and Information Security Incidents

2005 Vilnius, Lithuania

The Communications Regulatory Authority of the Republic of Lithuania (RRT) in cooperation with the European Network and Information Security Agency (ENISA) and Ministry of Transport and Communications of the Republic of Lithuania (MoTC) are organising a European network and information security conference 'Readiness for Handling Network and Information Security Incidents'.

Objective of the conference

The main objective of the conference is to provide a forum for the discussion of ensuring user readiness for network and security incidents. A particular focus will be on the preparedness of service providers, SMEs, and residential and business end users.



Main topics of the conference

- NIS incidents: perspectives from the user
- The cost of security incidents
- Advanced technological solutions for handling NIS incidents
- Advanced organisational models of NIS incidents handling on the national level and CERTs
- Organisational, administrative and managerial aspects of coordination of activities related to incidents, in business enterprises, network providers, and other institutions

Target audience of the conference

- Representatives of governmental institutions of EU Member States working in the field of NIS
- Representatives of business and users organisations dealing with NIS in general and incident handling readiness in particular

Date and location of the conference

The conference will be held on 23 and 24 November 2005 in Vilnius, Lithuania.

Vilnius, the green capital city of Lithuania, located close to the geographic centre of continental Europe, is fast becoming one of the most popular destinations in eastern Europe. Although Vilnius is often called a baroque city, there are many examples of gothic, renaissance and other styles of architecture. Because of its uniqueness, the old town of Vilnius was inscribed on the UNESCO World Heritage list.

Mr. Valdemaras Šalauskas, Under Secretary of the Ministry of Transport and Communications, says, 'Information security is not only about preventative measures, but also about readiness for when incidents do occur. This is especially important for end-users and SMEs who do not always have the expertise or tools to quickly respond to incidents. We are delighted to be hosting a conference on this important topic in Vilnius, and look forward to welcoming you here'. |

Contact:
Mrs Diana Korsakaitė
Email: dkorsakaite@rrt.lt
Tel. (370-5) 210 56 88
Algirdo street 27, Vilnius, Lithuania,
Communications Regulatory Authority

ENISA proud to announce ISSE 2005

Mark the date on your calendar – from 27 to 29 September, ENISA will be co-organizing the annual ISSE (Information Security Systems Europe) event in Budapest, Hungary.

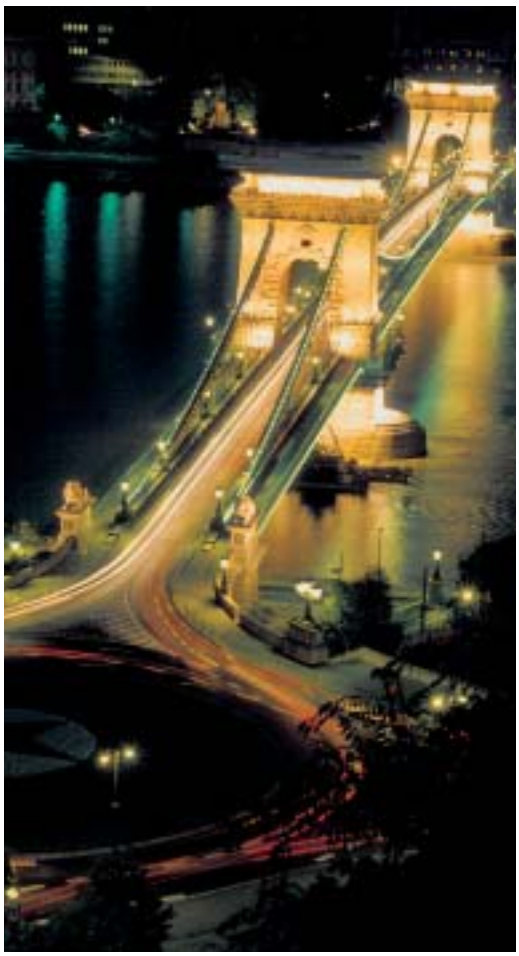
IT security breaches can have a damaging impact on organisations' customers and suppliers, lead to system downtime and loss or theft of company data – indeed, in today's world it is more important than ever that organisations are aware of security threats and have systems in place that keep their data as secure as possible. But when time is at a premium, how can IT staff keep up-to-date on the latest developments and technology in this ever-evolving area of IT?

The ISSE (Information Security Systems Europe) annual European IT Security Conferences have done much to address this problem. Far from being a forum for companies to sell their products and services, ISSE prides itself in being an independent conference where delegates and speakers are encouraged to present and discuss ideas and solutions on all aspects of IT security – from risk management, to data protection, to mobile security.

This year the conference is being held in Budapest, Hungary (27–29 September 2005) and will benefit from the variety of knowledge and expertise of the organisations that are supporting the event: eema (a UK independent body for the IT industry), the European Network and Information Security Agency (ENISA), TeleTrusT, the Hungarian Ministry of Informatics and Communications, and the German Ministry of Economics and Labour.

With the growing need for IT security throughout the European Union it is important to bring together knowledge from as many countries as possible – this year's partnerships will certainly help us achieve this goal, explained Roger Dean, head of special projects at eema.

ENISA is taking an active role in organising the event this year, with the full support of Andrea Pirotti, Executive Director of ENISA: 'ISSE has created an independent platform for the IT industry to bring European interests to the fore and help organisations understand and share information about information security issues. We are very proud to be part of the ISSE team for 2005 and welcome everyone to attend this conference.'



Delegates will benefit from hearing case studies of guest speakers and industry authorities from across Europe, in a variety of fields – including e-government, health care, e-business, the financial sector and enterprise security. Previous speakers at ISSE have come from high-profile international organisations such as Ernst & Young, Microsoft and DaimlerChrysler. Dr. Reimer, Manager of TeleTrusT, says, 'IT-security is essential for modern society. It can only be improved if we share our best experiences. ISSE 2005 is the appropriate platform for this vital exchange.'

ISSE 2005 is not only a unique opportunity for individuals from across Europe to share and broaden their knowledge in a critical area of IT, but also to have a positive impact on business profit.

Ferenc Suba of the Hungarian Ministry of Informatics and Communications and Vice-President of the ENISA Management Board says, 'Hungary is delighted to be hosting this conference and we expect a great exchange of ideas and experiences. We look forward to a great conference and look forward to welcoming you all to Budapest!' |

For further information about ISSE 2005 contact isse@eema.org or telephone (44-1386) 793028 or visit the ISSE website for full details, http://www.eema.org/isse.

ENISA-BSI Information Security Management Workshop in Bonn

ENISA has the pleasure to announce the ENISA-BSI Information Security Management Workshop in Bonn on 10 and 11 November. Risk assessment, one of the main tasks of ENISA, is the principal element of the security concept of every IT system. BSI has focused on this subject since its foundation in 1991.

The BSI, in collaboration with German industry, developed the methodology of IT Baseline Protection in 1994. Since then the IT Baseline Protection Manual (ITBPM) has become the security standard in industry and administration in Germany. More than 4000 registered users in Germany and in all of Europe apply the IT Baseline Protection Manual.

This workshop will give information security management experts from Europe an overview of the current risk assessment and management models and an easy introduction to the IT Baseline Protection methodology. The announcement of the new BSI certificate, combining both ISO 17799 and IT Baseline Protection, delivers an outlook on the answer to one of the greatest demands of the market. Presentations reflecting the experience of applying the ITBPM in both private and public institutions will serve as the basis for discussion. |

IT Baseline Protection Manual Developed by BSI is establishing itself as a standard both nationally and internationally

Baseline protection in IT is more than a mere provision of antivirus software, firewalls or backup systems. To determine the individual need for protection of the corresponding institutions and draw up relevant measures, an integral concept is required. For this purpose the IT Baseline Protection Manual (ITBPM) developed by the BSI has established itself as a standard both nationally and internationally. The ITBPM has been steadily improved since 1994 and describes potential threats and security precautions. The manual includes both systematic methods for elaborating IT security concepts and standard security measures which have been tried and tested in practice. They have already been successfully used by numerous government agencies and companies. A current version is available for downloading at the websites operated by BSI in HTML and PDF format. An English version can be found at http://www.bsi.bund.de/english/gshb/index.htm. |

CERT Bund warns of 'Surf Turbos'

The computer emergency rescue team of the CERT Bund (CERT for German federal government institutions) has issued a warning against 'surf turbos', which, in the meantime, represent a considerable security risk. The warning applies particularly to banks, which have been especially affected by this problem. However, above all, it applies to users who use the 'surf turbos' to increase the surfing rate. In the past few months offers which promise faster surfing on the Internet by installing special supplementary software on the customer's PC have increased in number at various providers. As a rule, these providers are untrustworthy market research agencies, which provide this software for downloading free of charge after registration. By installing the software, the data traffic is routed through proxy servers during surfing on the Internet by the provider. The increase in the surfing rate is to be achieved by compressing data during the transfer between provider and customer.

When using such an offer, most users are not aware of the fact that the provider can read their entire data traffic, analyse it, and link the data with the personal data delivered by the user during registration. There is a special threat in the fact that also sensitive information, such as data transfer during Internet banking (state of accounts, PINs, and TANs), can be read. In addition, data which is supposed to be protected by an SSLlink is not safe from unauthorised

reading while using the 'surf turbos' offered by several providers, because the encoded link is decoded on the provider's proxy server. Indeed, there is not any direct, encoded link between the user's browser and the server of the website visited, instead the data communication is decoded on the proxy server and then again encoded. This occurs unnoticed by the user, because with the installation of the software an additional certificate of the pro-vider is installed and automatically placed in the list of trustworthy certificates. Consequently, the Internet browser does not display any warning that the encoded link does not exist between the user's PC and the server of the web site visited (e.g. of an online-bank) but merely with the provider's proxy server.

The BSI warns against using 'surf turbos' if sensitive data such as passwords, PINs, TANs, and personal data are transferred during surfing. |

Review:

From 10 to 16 March 2005, the BSI presented itself at the world's largest IT-fair, CeBIT, whose major focus this year was, among other things, IT security. Apart from an exhibition stand with several major focuses, BSI experts informed their visitors about IT security with a series of lectures at the convention centre as well as at the public sector parc. One of the highlights was a panel discussion titled 'The Safe Country – Data Storage in the Era of Global Threat'. ENISA Director Andrea Pirotti and BSI President Dr. Udo Helmbrecht jointly participated in this discussion.

It is already the ninth time that the BSI has organised the German IT security congress, which was opened by Otto Schily, German Minister for the Interior. Under the motto 'IT Security Concerns Everyone!', manufacturers, users and service companies from industry and business, administration and the sciences met in Bonn from 10 May until 12 May, 2005. For three days they discussed the state of the art of the national and international development in IT security in a practice-oriented and open manner. Discussions focused on the subject of security in electronic passports.

Further details are available at http://www.bsi.bund.de/veranst/bsikongress/index.htm. The congress is held every second year. Even now it is worthwhile to make a note of the BSI congress for the spring of 2007. |

ENISA is moving to Heraklion!

ABOUT THE NEWSLETTER

ENISA wishes to thank all the contributors to the newsletter. 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 newsletter contents or from errors therein. |

Edited by: Boaz Gelbord.
Design by: Heimbüchel PR, Cologne/Berlin

More about ENISA

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