enisa European Network and Information Security Agency

Quarterly

IN THIS EDITION

No. 5, Jun 2006

A WORD FROM THE EXECUTIVE DIRECTOR

Boaz Gelbord and the Executive Director, Andrea Pirotti

Dear Readers,

Last month our Permanent Stakeholders' Group (PSG) presented us with a vision for ENISA. This document represents a valuable contribution to the ongoing discussion regarding the upcoming challenges in information security and the role ENISA can play in addressing them. The report (which you can read on our website) contains both interesting trends and concrete recommendations.

One important development is the move towards more targeted and stealthier worms. In the past we have seen large scale attacks with names like Slammer that have entered the common parlance. However, in the future we may yet end up being nostalgic for these easy-to-spot worms. Already we are viewing the trend towards more functional malware that tries to slip quietly under the radar, rather than the bombastic worms and viruses of the past. Fame is giving way to fortune as the primary motivation for hackers.

The PSG report highlights some new trends and also draws attention to old problems that continue to plague us – the lack of proper authentication, the multiple vulnerabilities in software, and the inherent insecurity of wireless networks, to name a few important examples. From this high level analysis of the security landscape, we must now determine how we can address these challenges within the scope of our mandate and resources.

This report is an important impetus to our continuing efforts to define a strategic vision for the future – how we can help guide towards an improved state of information security in Europe. Recently we held an informal workshop on this topic which brought together our Management Board and Permanent Stakeholders' Group. We are already active in a number of important areas but the unabated evolution of the ICT environment requires us to constantly adjust ourselves to developments.

On a final note, it is with much regret that we bid farewell to Boaz Gelbord in this issue of the ENISA Quarterly, as he leaves to pursue other challenges. Boaz has played a key role at ENISA since our first days in Brussels and he has made an invaluable contribution to the setting up of the Agency – establishing our Network of National Liaison Officers in record time and creating the ENISA Quarterly, to name but two of his impressive accomplishments. I wish to thank him very much for all of his contributions to ENISA and wish him success in all his future endeavours.

Sincerely,

Andrea Pirotti
Executive Director, ENISA

ISSN1830-3609

A WORD FROM THE EDITOR

Dear Readers,

Information security is a very broad term – covering everything from someone else reading your e-mail to a large scale cyber-terrorist attack. Indeed, the scope of this magazine is a testament to the diversity of this topic – in this edition you will find articles on policy issues such as the challenges of regulation, on technical issues such as DNS (Domain Name System) security, and on awareness-raising. But what, if anything, is the common thread that unites such diverse subjects?

One common element to all these topics is the shared challenge of securing a medium that defies our traditional concepts of physical, personal and national spaces. In the last issue, this editorial explored how cybersecurity knowledge was a factor in the digital divide – users who do not understand security issues are at a competitive disadvantage in the digital society because they cannot perform a proper risk assessment of their online activity. Framing the problem this way is an important step towards finding solutions to close this gap.

While most people are generally aware of the physical security risks they face, in the case of cybersecurity they are not able to even understand the nature of potential risks. By way of example, the average person has a general understanding of how a burglar operates and what motivates him; the hacker, on the other hand, comes across as a mysterious entity whose methods and goals are unknown. As Queen Juliana of the Netherlands is reported to have once said, "I don't understand computers. I don't even understand the people who understand computers."

This lack of understanding does not imply a lack of concern, as numerous surveys have shown that users significantly curtail their online activities due to security concerns. In the past, users may have been able to apply a blanket caution to the Internet and its use; however today's more complex ICT environment requires users to engage and try to understand how their information flows, and where it is most secure. The emergence of new architectures, devices and services is increasingly forcing end users to consider not only risks but the underlying information infrastructure itself.

A simple example of this phenomenon is ad placement within mail services such as Gmail. 'Targeted' advertising can sometimes be amusingly off-base – an e-mail starting with "Unfortunately I will never be able to travel to Iceland due to my fear of flying" may be accompanied with the offer of cheap flights – yet even the misplaced ads confront every user with the reality that his or her correspondence is being collected, analysed, and repackaged somewhere in a far-off location.

How can users make the right choices? Recently a virus hit the popular file sharing program, Winny, in Japan, which essentially made all the files on a user's PC available to anyone. For users who have their whole life on their PCs – bank statements, personal correspondence, bills and even medical files – such a virus could cause great embarrassment and loss. But the options for avoiding these attacks seem limited – keep everything offline, avoid file-sharing and other virus-prone applications, or constantly reconfigure the latest patches and warnings and employ encryption and other security mechanisms.

None of these options is very attractive. Keeping everything offline is impractical – and with many of today's devices having Bluetooth or 802.11 functionality built in – is still not entirely secure. Avoiding using downloadable applications of dubious pedigree might be fine at work, but most users would find that this seriously limits their ability to enjoy the Internet. And then the last option – constantly securing your machine – may be fine for the geeks and hobbyists amongst us, but is not really the way the average user would like to spend most of his or her time.

Which means that, in the end, all users need to become risk managers of their own systems, constantly evaluating when to avoid placing data online, which applications and activities to avoid, and how much time to devote to reconfiguration and management. What is the added value of the activity I am about to undertake online? What are the risks of something going wrong? How much will it cost me if it does go wrong? And finally – is it worth the risk?

Getting users, whether individuals or companies, to adopt this way of thinking is not easy, even though risk management is something we subconsciously practise in almost all of our everyday decisions. Within the information security community, there are a number of interesting initiatives that are addressing this issue. In this issue you can read about practical initiatives like the German Bürger-CERT (Citizen CERT) which is

trying to extend the CERT concept to the end user. This service provides citizens with information to help them make the proper risk management decisions.

Finally, a short pause to reflect on our publication – this issue marks the first anniversary of the ENISA Quarterly, and we are delighted at the positive feedback we have received from many subscribers. On a personal note, I will be stepping down as Editor-in-Chief of the ENISA Quarterly, as I leave to pursue new challenges and opportunities. I want to thank everyone for the support they have given this publication. In particular I would like to thank very much our Executive Director, Andrea Pirotti, for having given me the support and creative freedom to launch this publication and other key activities since the first days of ENISA in Brussels.

We hope the ENISA Quarterly continues to provide you with an interesting forum to read about the information security issues that matter to you. Our next issue will be coming out at the end of October 2006 so that it can incorporate the results of the ISSE conference in Rome from October 10-12.

Sincerely,

Boaz Gelbord,
Editor-in-Chief, ENISA Quarterly

Boaz Gelbord is a Senior Expert in Security Technologies at ENISA

From the World of Security – A Word from the Experts

Information Security: A Regulatory Train Wreck

Paul Kurtz

Governments around the world are responding to growing information security and privacy concerns by passing more laws and regulations. Frequently little thought is given to the global nature of the Internet as laws are passed.

Government action is based upon traditional legal institutions, local needs, customs and values. Yet action has a widespread impact transcending traditional political and legal borders. For example, California's law requiring notification of consumers in case of a breach of their personal data has had an impact across the whole of the United States. Thirty three other states have similar laws in place. The Sarbanes-Oxley Act affects any company publicly traded in the United States and beyond. The European Union's data protection and e-privacy directives affect any firm doing business in Europe. While government passes more laws, business continues to globalise. The planned merger between the New York Stock Exchange and Euronext will blur regulators' boundaries. We face a train wreck if there is not greater discourse about regulation in the Information Age. Business will be burdened by conflicting, costly regulation inhibiting innovation and growth. Consumers will be confused by conflicting privacy and security regimes.

Here is a four-step framework for addressing existing and proposed regulations:

Regulatory Information Portals

The EU and US Government should establish web-based information portals on information security regulations. The portals would include information on existing law, noting the source, purpose and scope of each law. In addition, each entry would also include widely accepted best practices to facilitate compliance. Within the EU, there are a number of bodies that could house such a service and the Department of Commerce could establish a similar service in the United States.

Voluntary Risk Management and Certification Framework

The EU and US Government should encourage business to voluntarily adopt Information Security Management System Standard 27001. The recently approved international standard provides a common, risk-based approach to security, privacy and compliance. The standard can be used to help comply with existing laws and is flexible enough to accommodate new laws, should they be necessary.

> "We face a train wreck if there is not greater discourse about regulation in the Information Age."

Regulatory Dialogue and Review

The EU and US Government should establish a strong transatlantic dialogue and review on information security law regulations. The review should identify the similarities, differences and conflict of existing and proposed law which directly and indirectly affects information security. When possible and appropriate, government representatives should seek to acknowledge equivalence of law and regulation, e.g. compliance with one country's law would be deemed acceptable to another. Business leaders on both sides of the Atlantic should be asked for their comments and recommendations.

Needs Test

Apply the following three-step needs test when government on either side of the Atlantic considers new law or regulation:

> "without a robust and ongoing transatlantic dialogue on information security law and regulation, we will soon be faced with a morass of bureaucracy"

- Whenever possible, apply existing legal and regulatory frameworks when considering passing a new law. For example, the US Congress, when addressing the need for a national data security and breach notification law, should adopt the Safeguards Rule under Gramm-Leach-Bliley Act (1999) rather than direct regulators to create a new set of rules.

- Whenever possible, legislators should offer incentives for the adoption of security practices rather than mandate specific security measures. For example, the US Congress should include a 'safe harbour' in a national law which provides that notification is not necessary in the case of a breach when the data is encrypted. A similar provision has been included in the vast majority of data breach laws passed by individual states.

- A cost-benefit analysis should accompany any proposed law. The analysis should also detail why an existing law or legal framework is not sufficient, and the costs of implementing a new law.

None of these measures would be easy to apply. However, without a robust and ongoing transatlantic dialogue on information security law and regulation, we will soon be faced with a morass of bureaucracy which is both impossible to apply, let alone untangle.

Paul Kurtz is Executive Director of the Cyber Security Industry Alliance (www.csialliance.org)

The International Critical Information Infrastructure Protection (CIIP) Handbook 2006

Isabelle Abele-Wigert, Myriam Dunn

Isabelle Abele-Wigert

Myriam Dunn

Critical infrastructure protection (CIP) is perceived as a key part of national security in numerous countries today and has become the nucleus of the US terrorism and homeland security debate after 9/11. A critical infrastructure (CI) is commonly understood to be a system or an asset whose incapacitation or destruction would have a debilitating impact on the national security and the economic and social welfare of a nation.

Protection concepts for strategically important infrastructures and objects have been part of national defence planning for decades, though at varying levels of importance. Towards the end of the Cold War, and for a couple of years thereafter, the possibility of infrastructure discontinuity caused by attacks or other disruptions played a relatively minor role in the security debate, only to gain new impetus around the mid-1990s, when a new, delicate problem became apparent: the dependency of modern industrialised societies on a wide variety of national and international information infrastructures.

The US was the first nation to broadly address the new vulnerability of the vital infrastructures. New risks in designated 'sectors' like information and communications, banking and finance, energy, physical distribution, and vital human services were identified by the Presidential Commission on Critical Infrastructure Protection (PCCIP) in 1997. The issue of CIIP has remained a high priority on the political agenda ever since. The events of 9/11 merely served to further increase the awareness of vulnerabilities and the sense of urgency in protecting critical infrastructures.

The Critical Information Infrastructure Protection (CIIP) Handbooks 2002-2006

Following the example of the US and driven by a growing concern for the potential vulnerability of their own networked societies, numerous countries have begun to draft protection policies of their own. The International Critical Information Infrastructure Protection (CIIP) Handbooks 2002-2006 provide an overview of these protection efforts in various countries.

The first (2002) edition of the CIIP Handbook contained an inventory of protection policies in eight countries (Australia, Canada, Germany, the Netherlands, Norway, Sweden, Switzerland and the United States) and their methods employed for CII assessment. The second edition (2004) included an update of existing surveys and covered six additional countries (Austria, Finland, France, the United Kingdom, Italy and New Zealand) as well as international protection efforts.

The 2006 version continues the tradition of the past two editions, while its scope has been extended: not only has the country survey section been further expanded with a specific focus on Asia by including India, Japan, the Republic of Korea, Malaysia, Singapore and Russia, but it also includes the CIIP policy efforts of six international organisations.

The CIIP Handbook is aimed mainly at security policy analysts, researchers and practitioners. It can be used either as a reference work for a quick overview of the state of the art in CIIP policy formulation, or as a starting point for further, in-depth research.

The CIIP Handbook 2006 with two Volumes

Volume I: Surveys of 20 Countries and 6 International Organisations

Volume I of the CIIP Handbook 2006 covers the national und international critical information infrastructure protection policies of: Australia, Austria, Canada, Finland, France, Germany, India, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Russia, Singapore, Sweden, Switzerland, United Kingdom, United States, EU, G8, NATO, OECD, UN and the World Bank Group. Each survey was reviewed by national experts in the field, either from the government or academia.

For each survey, five focal points of high importance covering conceptual and organisational aspects of CIIP are considered:

- **The definition of critical sectors:** The first section lists the critical sectors identified by the specific country and provides definitions of CII and CIIP, where available.
- **Past and present CIIP initiatives and policies:** The second section gives an overview of the most important steps taken at the governmental level since the late 1990s to handle CIIP. The focus is on initiatives and the main elements of CIIP policy. This includes descriptions of specific committees, commissions, task forces and working groups, the main findings of key official reports and fundamental studies, and important national programmes.
- **Organisational structures:** The third section gives an overview of important public actors in the national CIIP organisational framework. It only characterises the specific responsibilities or public actors at the state (federal) level (such as ministries, national offices, agencies, co-ordination groups etc.). Public actors at the lower state level and private actors (companies, industry etc.) are omitted. Due to the growing importance of public-private partnerships, the most important of these are presented.
- **Early warning approaches and public outreach:** The forth section describes national organisations responsible for CIIP early warning, namely CIIP-related information-sharing organisations such as CERTs (Computer Emergency Response Teams), ISACs (Information Sharing and

➲

Analysis Centers) etc. Moreover, public outreach initiatives are depicted.

- **Law and legislation:** The fifth section lists important legislation enacted for the promotion of CIIP. This includes acts defining the responsibilities of the government authorities in case of emergencies, as well as legislation dealing with issues such as technical IT security, data protection, damage to data, fraudulent use of a computer, the handling of electronic signatures etc.

Volume II: In-Depth Analysis and Conclusion
Volume II of the current edition ('Analyzing Issues, Challenges, and Prospects') covers some of the most important topics in more detail. Various experts express their views. Volume II has three parts:

- **Part I** deals with *conceptual issues*. Because the problem that CIIP deals with represents a highly dynamic social phenomenon, the workings of critical systems and their exact role and criticality for society are still very elusive. This might change once this area of research gains a more stable scientific and methodological base. In the meantime, basic issues need to be addressed: What exactly is CIP? What is CIIP? How do the two concepts differ? What approaches are in use to analyse these systems? What do we seek to protect?

- **Part II** deals with aspects of the *threat* to the information infrastructure, in order to deepen the understanding of issues raised in Part I. In specific, it looks at what it is that actually threatens the information infrastructure. The outline of possible actors includes hostile states, terrorist groups, fanatical religious movements, criminal organisations, and extremist political parties, as well as individuals such as discontented insiders and irresponsible hackers or crackers. In addition, complexity itself brings about the risk of a truly major, society-threatening chain reaction of IT-related events.

- **Part III** addresses three persistent policy issues identified in Volume I in more detail: public-private partnerships, national and international legal issues, and the need for international co-operation. These issues are interrelated and demand a *global* culture of cybersecurity that starts at the national level. But how does the national become global or, to put it differently, how can we move from these national approaches to a global culture? Is there some common denominator to aim for? Or does a global culture of cybersecurity already exist, at least in a rudimentary form? With these questions in mind, Part III helps to identify common themes, best practices, but especially problems and pitfalls for a future global culture of cybersecurity.

A Useful Source for all EU Member States

The CIIP Handbook 2006 also contains a chapter on the European Union. It gives an overview of EU initiatives and policies in the field, the critical sectors identified by the EU Commission, EU research and development programmes and the relevant laws and legislation.

For all experts and practitioners in the EU Member States, the extensive appendix of Volume I may prove especially useful; it contains a bibliography and a collection of links for each country and international organisations, and a list of experts involved. In addition, the 'Countries at a Glance' pages provide a comprehensive list of the most important actors and documents in each country, allowing a quick overview of EU countries' current CIIP policies and activities.

In addition, Volume II is an ideal source of information about the current challenges and prospects facing governments and international organisations when it comes to the protection of their critical information assets, and it addresses various aspects of the problem. This publication is an ideal starting point both for those previously unfamiliar with the topic and readers in search of more in-depth knowledge of the complexity and extent of the CIIP issue.

Links to the full text online version:
CIIP Handbook Volume I:
www.isn.ethz.ch/crn/_docs/CIIP_HB_06_Vol.1.pdf
CIIP Handbook Volume II:
www.isn.ethz.ch/crn/_docs/CIIP_HB_06_Vol.21.pdf

For further information
Isabelle Abele-Wigert/Myriam Dunn
Center for Security Studies (CSS)
wigert@sipo.gess.ethz.ch
dunn@sipo.gess.ethz.ch
www.crn.ethz.ch

Isabelle Abele-Wigert is a Research Fellow at the Center for Security Studies (CSS) at ETH Zurich and a member of its Comprehensive Risk Analysis and Management Network (CRN) team

Myriam Dunn heads the New Risk Research Unit at the Center for Security Studies (CSS) at ETH Zurich, and is the Co-ordinator of its Comprehensive Risk Analysis and Management Network (CRN)

The Worrisome Threat of DNS DDoS Amplification Attacks

David Piscitello

Between December 2005 and March 2006, some DNS (Domain Name System) root and Top Level Domain (TLD) name server operators were subjected to numerous denial of service (DoS) attacks. These attacks seriously disrupt name resolution service by directing an overwhelming amount of traffic at the communications links that name server operators use to provide service. This 'congestion' makes it difficult or impossible for operators to provide the function of identifying the Internet address associated with the domain name of any of the registered names in the domain under attack. The targets for such attacks are not limited to root and TLD name servers; major financial and eCommerce name servers may be even more vulnerable, and the consequent disruption to name resolution in such focused attacks have grave economic consequences. Law enforcement agencies and governments worldwide should treat these incidents as serious attacks, deliberately launched against very high profile targets, by parties who may be politically or financially motivated.

What is a DNS DDoS Amplification Attack?

The attacks against root and TLD name servers are variants of what security experts call a DNS DDoS amplification attack. The attack can be best explained by examining the elements involved in the attack. The attack targets a specific service, the DNS, and attempts to prevent or deny access to that service. A DoS is an attack whose objective is to exhaust the resources of a target host (memory, processing capabilities, or Internet bandwidth). The target can be an individual host, such as a DNS name server, or an entire name server infrastructure of a country-specific or generic TLD (com, net, org, biz). To launch an effective attack against large scale name server operations, an attacker requires a virtual army of hosts that can, at his command, simultaneously attack a specified name service target. He must thus distribute his attack.

A distributed denial of service attack (DDoS), as the name suggests, is a virtual 'attack on all fronts'. Because so many PCs, both personal and business, are poorly secured, such armies are unfortunately simple to recruit. By creating and sending an e-mail message containing a malicious programme, for example, an attacker can infect hundreds (possibly thousands) of PCs that are not adequately protected against infection. Such PCs are whimsically known as 'zombies'. To form a DDoS army, the infecting programme is written to allow the attacker to remotely control and direct to initiate a DoS attack at a specified target, at a specified time. The DNS DDoS attacks and other, similar DDoS attacks harshly illustrate that attackers can gather sufficiently large zombie armies to flood even the Gigabit per second access circuits used by TLD name server operators.

Even when large armies of attacking hosts are employed, an attacker will try to maximise the volume of traffic that can be directed at a target over the shortest period of time. One method of increasing or amplifying the traffic volume is to add an intermediate set of machines into the attack army by making use of public DNS servers and having these public DNS servers amplify the size of the messages coming from the zombies. In the DNS DDoS attacks, the attacker composes a DNS request message of approximately 60 bytes and causes the delivery of a response message of approximately 4,000 bytes to the target. This significantly increases the volume of traffic the target will receive, and thus accelerates the rate at which the target's resources will be depleted. Amplification of this dramatic a scale assures that an unprepared target cannot deploy countermeasures before the attack succeeds. A message of 4,000 bytes is also so large that it is almost certain to require fragmentation into multiple, smaller IP packets along the path to the target. Thus, in addition to increasing traffic volume at the target, the attack will increase the processing load by forcing message reassembly.

Deception in DNS DDoS Attacks

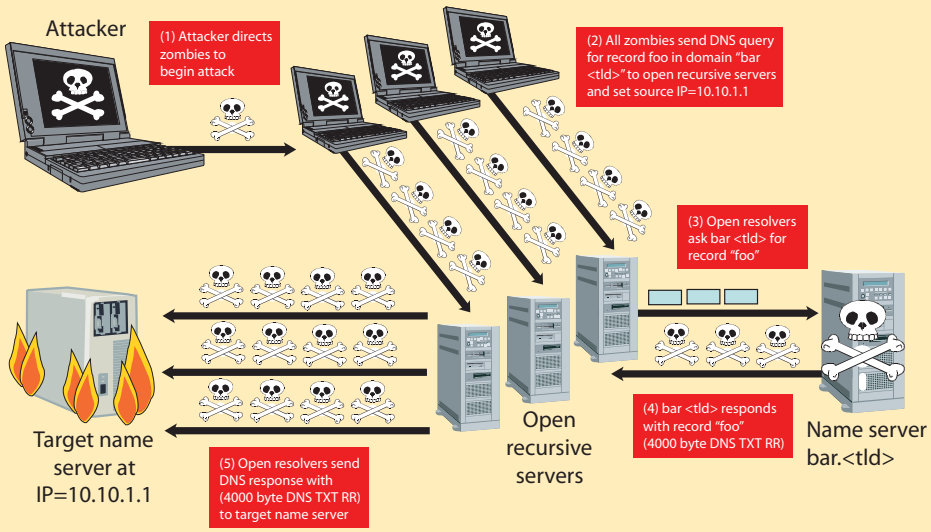
During a DDoS attack, each attacking zombie host uses the targeted name server's Internet address as its originating or source IP address, rather than its own. The effect of masquerading or spoofing the Internet address of the targeted host in a DNS DDoS attack is that responses to thousands of DNS requests will be delivered to the targeted name server operator rather than being returned to scores of spoofing zombie hosts. This is but one element of the extensive deception techniques employed in the incidents observed. DNS DDoS attacks additionally exploit name servers that allow open recursion, where a name server processes a DNS request on behalf of a PC by asking the authoritative name server, i.e., the definitive source of domain name information for a DNS name record. Recursion is typically provided for a trusted or closed set of clients, but generally, name servers can perform 'open' recursion for any host and, while estimates vary, it is possible that more than one million name servers worldwide provide open recursion.

Anatomy of the Attack

By combining IP spoofing, open recursion and amplification, attackers execute a DNS DDoS amplification attack in the following sequence. The attacker gathers a zombie army. He composes a large amplification record and inserts it in the domain name zone file of a name server (his own or one he has compromised). The attacker then commands his zombies to issue a continuous stream of DNS requests for the amplification record via name servers that provide open recursion. In the DNS requests, every zombie uses the targeted name server's Internet address rather than its own.

If an open recursive name server has not processed a previous request for the amplification record, it issues a DNS request on behalf of a zombie and retrieves the amplification record from the compromised name server. The amplification record is cached by the open recursive server, which then composes a DNS response containing the amplification record. The open recursive servers think they are returning DNS responses to the zombies that made the original request, but the responses are forwarded to the targeted name server. The targeted name server is now hammered with responses to DNS requests it never made. The large DNS responses arrive as multiple IP packet fragments, which must be reassembled. This both increases the processing load at the target and enhances the deception. Because the response spans several IP fragments, and only the first fragment contains the UDP header, the target may not immediately recognise that the attack is DNS-based.

The results can be quite devastating. Depending on the countermeasures in place and the robustness of the name server infrastructure attacked, service provided by a name server operator can be degraded, seriously impaired, or even brought to a halt.



Anatomy of a DNS DDoS Amplification Attack
(reproduced from SAC008, DNS Distributed Denial of Service (DDoS) Attacks)

Mounting an Immediate Defence against DNS DDoS Attacks

Only a handful of countermeasures are available to operators when they are targeted for a DNS DDoS attack. Note that, while the zombies employ IP spoofing, the open recursive servers do not, so the name server operators can readily identify the open recursive servers the zombies use and use this information to limit traffic from these sources, or to block traffic from these open recursive servers entirely. For the short term, name server operators can discard DNS responses that are suspiciously large. DDoS detection and mitigation techniques already implemented in commercial intrusion prevention systems and firewalls will undoubtedly be expanded to test for traffic patterns and arrival rates indicative of the types of DNS DDoS attacks that have already been executed.

The problem with all these efforts is that, while they reduce the impact to the name servers under attack, they do not quash the attack sources, and they do not reduce the load on networks and switches along the paths between the targeted name server and (all of) the open recursive servers. An undesirable consequence of temporarily blocking all traffic from open recursive servers is that legitimate attempts to resolve names through these servers become the 'baby thrown out with the bath water'. Long-term 'blacklisting' of open recursive servers will also hamper organisations that run name servers in this mode so that mobile employees can resolve from a 'trusted' name server.

Collaborative Efforts Can Thwart DNS DDoS Attacks

Security advisory groups such as CERTs, SANS and ICANN's Security and Stability Advisory Committee (SSAC) recommend widespread adoption of two measures to thwart DNS DDoS attacks. First, eliminate gratuitous and unintentional configurations of open recursive name services. By configuring name servers to only accept recursive DNS from trusted sources except where absolutely necessary, the community at large can greatly reduce the attack vectors available. (Organisations that have legitimate needs for open recursive name service should do so as responsibly as possible by implementing the DDoS detection and mitigation measures mentioned above.)

The second and most important measure is to implement source IP address validation on a broad scale. By checking that the source address in every IP packet is a validly assigned address prior to permitting traffic to enter the Internet core over any communications access link from any 'edge' device (PC, router, switch, or firewall), a wide range of IP address-based impersonation attacks can be eliminated or greatly reduced.

Currently, source IP address validation is not widely adopted. Critics claim that it adds administrative overhead and adversely affects performance. However, DDoS attacks are growing in frequency and efficiency, and the community at large should not conclude that DNS DDoS attacks against high profile name servers are the clearest and most present danger. In Europe, the RIPE community has established a task force to promote proper measures to prevent the use of an illegal address.

Public service providers and private network operators are increasingly looking to the Internet as an efficient means of deploying telephony services. Voice over IP service is currently as vulnerable to DDoS attacks as the DNS. Today, responses to terrorist incidents and natural catastrophes are dependent on the availability of cellular and PSTN networks. Telecommunications networks have been validating telephone numbers and addresses on ingress traffic for decades. It is time for IP networks to follow suit.

David Piscitello is a member of the Security and Stability Advisory Comittee and is an ICANN Fellow

ARES 2006

Louis Marinos

From 20-23 April, the international conference on Availability, Reliability and Security (ARES) 2006 took place in Vienna. The event was organised in co-operation with ENISA (see the ARES website: www.ares-conf.org).

The conference opened with a keynote speech by the ENISA Senior Expert on Risk Management, Louis Marinos, on the structure and content of deliverables in Risk Management.

ENISA also organised a workshop on 'Information Security Risk Management' (ISRM) which included presentations on policy, research and industry issues on Risk Management to about 100 attendees. This event underlined the interest in various emerging aspects of Risk Management in different sectors. Below we give some highlights of the main conclusions of the workshop for each sector:

Government: Risk Management within governments needs to support multiple methodologies. Methodologies that may be appropriate in one arena may not work for another – for example, in Austria, Risk Management is undertaken within diverse areas of public affairs, such as Quality Assurance, Emergency Precautions, Legislation and Organisation, Public Relations and Collaboration. Each one of these areas has its own regulatory and operational requirements that in turn necessitate a specific risk management approach.

Another old but still unresolved issue that was emphasised in the discussion was the importance of cross border co-operation on different levels to tackle information security problems collectively. Indeed, in the past it has been all too easy for cybercriminals to take advantage of lax cross-border co-operation to avoid detection and prosecution.

Consulting Industry: Security consultants and outsourced security service providers recognise the need to provide customers with Risk Management methodologies to apply to both IT and business processes. New legislation and standards in this domain (e.g. corporate governance, de facto industrial standards in operational processes) will further amplify this need. But providing the methodologies is only the first step – businesses must have tool suites available to transform IT risks into business language. One important development in the future will be to forge a common language to enable different companies to communicate about risks in a mutually understandable way.

National and International Activities: During the discussion on international activities in Risk Management, the results of the ENISA Working Group were presented, and the need to extend this work was identified. Activity on security at the national level was considered in the case of Austria. The generation of synergies with international organisations like ENISA to support Austria's implementation of Risk Management initiatives has proved very beneficial and augurs well for progress in the future.

The presentations from the ISRM workshop will be prepared as proceedings by the University of Vienna.

The organisers of ARES and ENISA have agreed to co-operate for future events.

Louis Marinos is a Senior Expert in Risk Management at ENISA

A Users' Guide: How to Raise Information Security Awareness

Isabella Santa

As part of ENISA's 2006 Work Programme, the Awareness Raising Unit of ENISA has compiled 'A Users' Guide: How to Raise Information Security Awareness'.

This Guide provides practical advice for Member States to help them prepare and then implement awareness-raising initiatives related to information security, recognising that awareness of the risks and available safeguards is the first line of defence for the security of information systems and networks. The information covered within the document features step-by-step advice which could form the basis of an effective awareness campaign targeted at different audiences, such as public and private organisations.

Specifically, the Guide achieves the following:

- Illustrates a sample strategy for how to plan, organise and run an information security awareness-raising initiative
- Highlights potential risks associated with awareness initiatives in an effort to avoid such issues in future programmes
- Provides a framework to evaluate the effectiveness of an awareness programme
- Offers a communication framework
- Contributes to the development of an information security culture in Member States by encouraging users to act responsibly and thus operate more securely

Strategy for Executing Awareness Initiatives and Programmes

The Guide identifies the main processes and activities necessary to run an awareness campaign. The processes have been defined as follows: plan and assess; execute and manage; evaluate and adjust. For each process a few activities have been identified. A series of steps and recommendations have been included in this section to help the reader implement awareness initiatives and programmes.

In particular, the Guide emphasises the importance of:

- **Effective Communication Planning**
  A communication strategy is at the centre of any effective awareness programme, but the strategy needs to be adapted to a specific context, i.e. it must:
  - be based on communication goals and principles
  - be aligned with target group needs
  - take into account different target groups
  - cover both regular and situational communication needs
  - be adapted to target group feedback
- **Change Management Approach**
  Applying a change management approach to an awareness initiative is crucial as it helps close the gap between a particular issue and human responses to the need to change, even in the case of a cultural change.

  Using the main principles of change management (targeted communications, involvement, training and evaluation) helps ensure that awareness initiative objectives are met as well as providing a sound platform for future or follow-up programmes.
- **Measurement of the Value of Awareness Programmes**
  The need for security awareness is widely recognised. However, not many public or private organisations have tried to formally quantify the value of awareness programmes. Evaluation of a campaign or programme is essential to understand its effectiveness as well as to make adjustments based on what has been learned to date. Evaluation

metrics cannot be universally applied to all target groups since needs and situations differ greatly.

Four headings have been identified under which security awareness can be measured:

- Process Improvement
- Attack Resistance
- Efficiency and Effectiveness
- Internal Protections

Conclusion

Up to now, awareness-raising has been done in a variety of different ways in different Member States; this guide offers a unique product to help Member States both start new programmes and improve old ones.

The Guide will be available shortly in print and online on the ENISA website.

Isabella Santa is a Senior Expert in Awareness Raising at ENISA

Other Topics Covered in the Guide

Obstacles to success
Implementing a successful security awareness programme may seem a difficult task. It is therefore helpful to understand some common obstacles and to take steps to overcome them during the planning and implementation phases of the initiative. The Guide identifies potential barriers and suggests how to deal with them.

Critical success factors
Success factors for awareness campaigns are identified and described in detail in the Guide.

Templates and samples
To help the reader while planning, managing and executing an awareness campaign, the Guide suggests using a number of tools for which templates and samples have been included in the document (e.g. a lessons learned template; a work plan sample; a target group data capture form etc.).

Study on Security and Anti-spam Measures

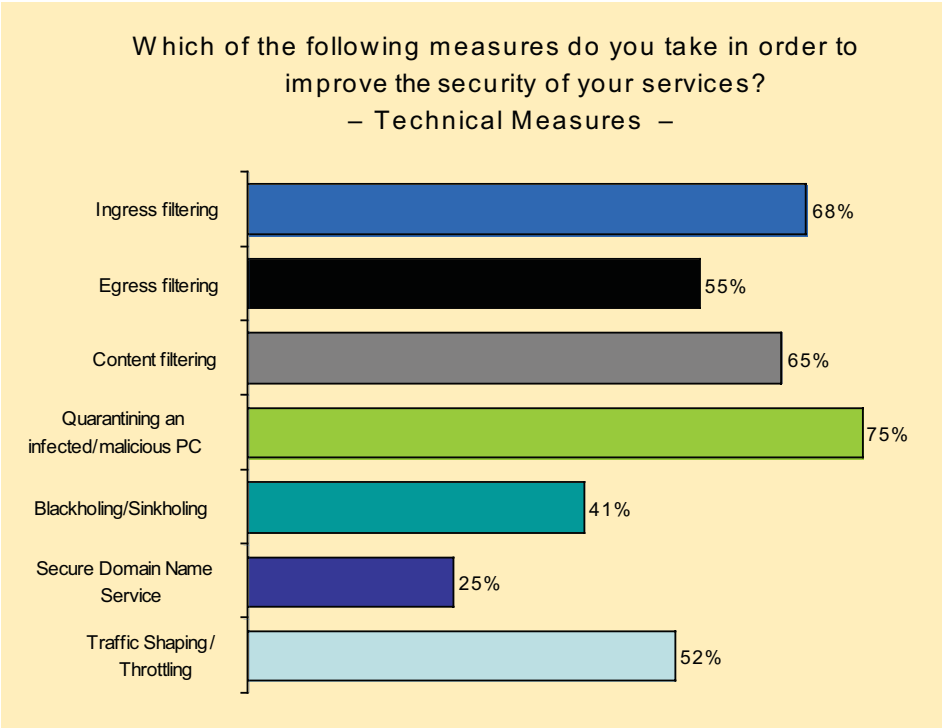
Carsten Casper

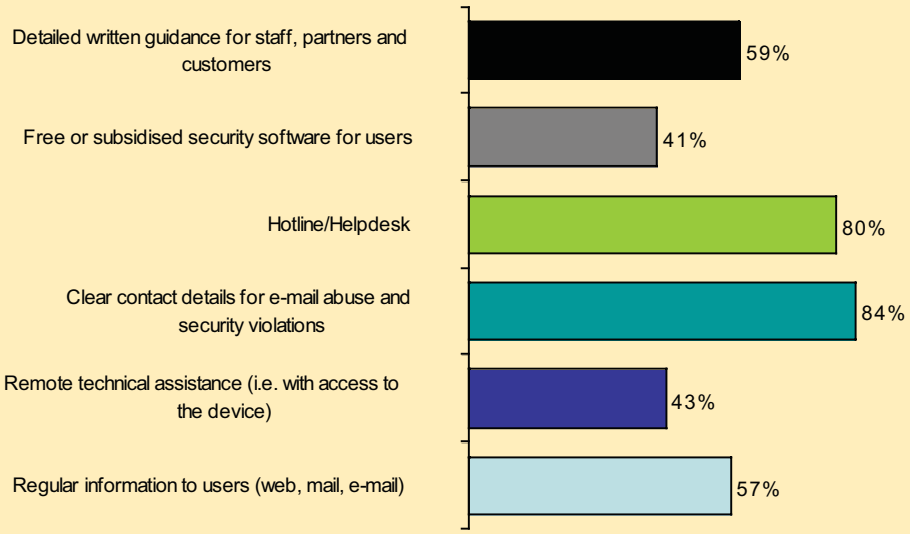
EU Directives have to be transposed into national law by the Member States. These laws are then binding for organisations and citizens in that country. After some time, the Commission evaluates the impact a Directive actually has. In this context, ENISA conducted a survey on measures taken by electronic communication services providers (ISPs, telcos and others) to comply with national requirements implementing provisions of EU Directives, in particular Directive 2002/58/EC.

This Directive, also called the 'Directive on Privacy and Electronic Communications', outlines measures on security in Article 4 and measures on unsolicited commercial e-mails (spam) in Article 13. ENISA's study addressed both. The analysis of the data gathered from the more than 90 respondents led to the following conclusions.

Measures taken by providers

Measures depend on the type of threat against which each provider focuses its defence, and the specific nature of the business the provider is in. This applies both to technical measures and organisational measures.





Technical Measures – There are a number of activities that would help improve technical security measures. For example, providers could be required to report on the technical measures which they implement to secure their services, in order to increase transparency and enable comparisons. There should also be an incentive for providers to contribute to the overall security of interconnected networks rather than merely protecting their own resources. Moreover, providers need to be more proactive and monitor their networks for risks of security breaches, and could also be asked to report which networks they monitor.

Organisational Measures – Clear documentation and regular communications on information security, as well as collection and dissemination of best practices should be emphasised. This includes guidance to consumers as well as guidance to the provider's staff, in particular with regard to incident response and emergency planning. Moreover, providers should publish contact details for e-mail abuse and security violations.

Appropriate Security and Reporting – One article of the Directive 2002/58/EC asks providers to take into account the state of the art and the cost of security implementations. As many responses have indicated, interpretation and additional guidance is necessary to promote this objective. National Regulatory Authorities and other national bodies, as well as ENISA itself, could play an active role in this. Another article of the Directive demands that providers report on the risk of security breaches. According to the providers, this happens on a case-by-case basis, and only voluntarily. While it is certainly important to get an overview of the risk that can be expected from a particular problem, only reporting actual security breaches (an emerging requirement in the US), rather than reporting the mere risk of a breach, would really improve the situation.

Spam – From a technical perspective, there is no 100% protection against spam. Though in the past technical measures made significant inroads into reducing incoming spam (many of the providers even offer spam protection free of charge), it appears that more technologies deployed by individual providers would have only a marginal effect. This is due to the underlying economic model for spam and the fact that most spam originates outside the EU. Reporting large scale e-mail abuse and international co-ordination of anti-spam measures should be encouraged, e.g. via the Contact Network of Spam Authorities (CNSA) and the London Action Plan (LAP).

Conclusion

The study gives a snapshot of how providers are coping with the requirements imposed by Directive 2002/58/EC. ENISA has found that providers are indeed taking these into account, although to varying degrees. Adjustments of legislation will be necessary, for example making some voluntary measures mandatory, to further improve the information security posture of providers in Europe.

Information Security Certificates – Invitation to Participate

Certificates attest to a certain level of information security for people, technologies and organisations. ENISA will bring together those who establish certification schemes and those who use them.

Comprehensive security requires secure technologies, secure organisational processes and people with the necessary background and skills. All these should work hand in hand, using well-defined interfaces and a terminology that is understood by all parties. During the coming months, ENISA will collect information on knowledge certifications (e.g. CISA, CISSP), technology certifications (e.g. Common Criteria) and organisational certifications (e.g. ISO 27001). In a workshop at the end of 2006, relevant players will be invited to present their certification scheme and its use. ENISA will moderate the discussion to identify commonalities and differences. A plan to improve certification schemes and to promote their use will follow soon after, laying the ground for future ENISA work in 2007.

An initial list of certificates will be available on the ENISA website (under 'ENISA Library'). A continuously updated version will be discussed in an Interest Group on http://circa.europa.eu/enisa (registration necessary).

ENISA is looking for experts in this field and is inviting national and international certifiers to participate. If you would like to know more about this project, please e-mail: Carsten.Casper@enisa.europa.eu

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

CERT Staff Training is in High Demand

Mehis Hakkaja

Participants at the recent TRANSITS training in Vilnius

Since the early Internet was practically brought to its knees by the first network worm just under two decades ago, security services provided by CERTs have been set up across the world. CERTs (Computer Emergency Response Teams), also known as CSIRTs (Computer Security Incident Response Teams), were first established in the US, but this time-tested model has spread throughout the world, and over 100 teams exist in Europe now.

CERT Coverage

There are many CERTs but their number is still small compared with the rapidly growing array of networks and information systems in Europe. By February 2006 when ENISA revised its 'Inventory of CERT activities in Europe' (www.enisa.eu.int/ pages/0501.htm), 22 Member States out of 25 had at least one CERT established, with a total of 92 active EU and 12 other European teams. But even the highest scoring countries, with up to 20 teams, could not claim perfect coverage – as CERTs have been established mostly in the private sector by research and education network organisations, commercial network operators and vendors. Specifically, the ENISA ad hoc working group of CERT experts concluded at the end of 2005 that small to medium enterprises (SME) and home users were the least addressed groups. Even government and national CERTs, where coverage is better, have only been getting more attention in recent years.

Training is Essential

The need for CERTs to grow and for new CERTs to be set up is hampered by a shortage of qualified personnel, as a high level of technical and security skill is required to operate a CERT. To address this issue, the European Commission funded a project called TRANSITS (Training of Network Security Incident Teams Staff) from July 2002 to September 2005. The main goal of this project was to promote the establishment of new CERTs and the enhancement of existing CERTs by addressing the problem of the shortage of skilled staff.

The TRANSITS Project

The TRANSITS consortium involved TERENA (the Trans-European Research and Education Networking Association) and UKERNA (the United Kingdom Education and Research Networking Association). During its three years of operation, the TRANSITS programme achieved the following:

- Two-day training courses were developed to cover the organisational, operational, technical, market and legal issues involved in providing CERT services.
- 7 TRANSITS training workshops were organised during the lifetime of the project.
- These 7 workshops provided training to 153 people from 32 countries.
- The course materials have been put in the public domain.

While the project officially ended in 2005, the initiative continues to provide benefits as two post-project workshops have trained 53 additional people, and course materials have been used by CERTs internally. The TRANSITS consortium partners have taken responsibility to ensure that training materials are regularly updated and courses are continued. FIRST (the Forum of Incident Response and Security Teams) has joined forces with TERENA, commiting resources for the further maintenance and updating of the course materials. FIRST also continues to organise training workshops outside Europe, in particular in Latin America and the Asia-Pacific region.

ENISA – Supporting the European CERT Community

The TRANSITS training initiative continues to be in high demand in Europe. At the end of March 2006 ENISA co-organised a TRANSITS course in Vilnius, Lithuania, following a request by the Lithuanian authorities for help in setting up a national CERT.

The training involved participants who were new staff of existing CERTs, as well as people involved in setting up CERTs. 25 participants from 13 countries from the public and private sectors took part in this course: Lithuania (7), Estonia (3), Poland (1), Finland (2), Austria (1), Netherlands (2), Portugal (1), Germany (1), UK (2), Belarus (1), Azerbaijan (2), Kyrgyzstan (1) and even Afghanistan (1).

Bringing TRANSITS to the region has assisted both Lithuania and Estonia in their work to establish operational national CERTs by the end of 2006 and hopefully these will not be the only new European teams established this year.

Towards the Future

ENISA very much values the opportunity to support and co-organise such training sessions. Participation not only helps to ensure there are more trained and certified CERT staff across Europe; it also allows ENISA to identify potential new teams and to make new contacts with emerging teams outside of Europe. And perhaps most importantly, such events allow new teams to integrate into the European CERT community at a very early stage in their development.

ENISA has produced an overview identifying gaps in CERT coverage. Such co-organised events have proved an efficient and cost-effective way to address these gaps and make a direct impact on the European CERT community.

ENISA will be co-organising another TRANSITS training event with TERENA in the last quarter of 2006; details will be published soon on the TRANSITS website at www.ist-transits.org/.

For countries and regions still in the early stages of planning a CERT, please contact the author (mehis.hakkaja@enisa.europa.eu) if you would like to discuss the possibility of hosting a CERT staff training event in 2007.

Mehis Hakkaja is an Expert in Computer Incident and Response Handling at ENISA

From the Member States

Market Penetration of Common Criteria Certification: the Italian Perspective

Luisa Franchina, Marco Carbonelli, Laura Gratta

Despite increasing awareness about the importance of security in the ICT context, the use of Common Criteria system/product certification is not yet as widespread as one would expect. This article continues the discussion of the subject opened by the French certification body in the last issue of the ENISA Quarterly.

Factors Limiting the Use of Certification

The Italian information security certification body, Organismo di Certificazione della Sicurezza Informatica (OCSI), was established in 2004 and is currently preparing the actions needed in order to be accepted as a certificate authorising body according to the Common Criteria Recognition Arrangement. To boost the use of Common Criteria certifications in Italy, we have tried to analyse the current application of CC certification, learning from the experiences of certifications made under foreign schemes, and comparing this situation with the Italian market.

In our opinion, besides the criticisms reported by the French certification body (costs, delays, abuse of certificates, obscurity of the criteria), certain other issues should be taken into account. These are:

- the scope of certifications
- the role of the end user in the certification scenario
- the nature of the majority of security incidents
- the effectiveness of certifications in a rapidly evolving ICT security scenario.

We analyse each of these issues in turn below.

The scope of certifications

The weakest link principle suggests that the use of very secure, certified products in an insecure context does not provide a global benefit. Consequently, certification does not make much sense if a common level of overall security is not guaranteed.

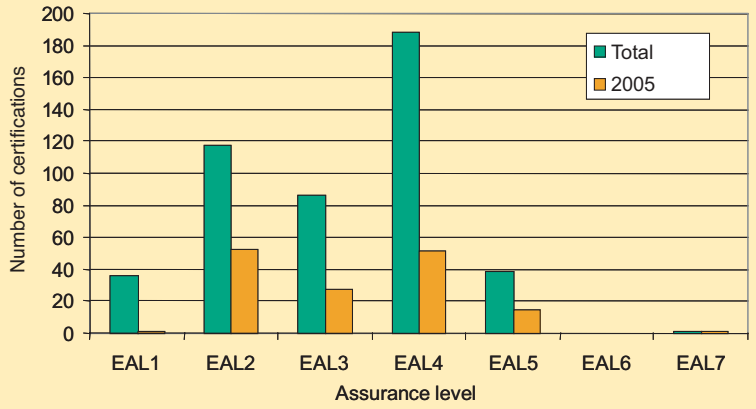
In many cases only a small part of a whole system is certified as a product. In these cases, a certification of the entire ICT system, even at a low assurance level, would be of benefit for the end user. This would guarantee that the security features of the whole system had been tested, including operational aspects like configuration. This has a major impact since, in the operational phase of a system life-cycle, many security holes arise from poor attention to a hardened configuration.

A further increase in overall system security would be achieved if the CC certification process were synergic with the ISO 27001 process certification, leading to full management of all the security aspects of the system life-cycle.

The role of the end user in the certification scenario

Until now, the certification market has been driven mainly by developers, with only marginal involvement of end users. Often certification has been conceived as a marketing tool for products. This approach has pushed up product certification; moreover, in order to achieve greater marketing revenue, developers often preferred high assurance levels (at times restricting the scope of certification to minor security functions), with an accompanying increase in delays and costs.

Number of certifications at different EALs



data from www.commoncriteriaportal.org

Consider the number of EAL (Evaluation Assurance Level) certifications issued, which vary from EAL1 (the lowest level) to EAL7 (the highest level) in the CC framework. From the analysis of the data on the certifications issued all over the world (see above), it appears that the total number of EAL4 certifications ever issued exceeds that of any other assurance level. In 2005 the situation seems to have changed, however, as EAL2 and EAL4 certifications were almost equal. Hopefully, this could indicate that a new trend is in place.

As already pointed out, the security level perceived by the end user depends on the assurance he can get from the overall ICT system he is logged into. Conversely, there is a risk that certification can be seen as a decoy, due to its limits and understatements. A significant spread in the use of certification can be achieved only if end users, having a concrete perception of the advantage of certification, strongly increase their demand for it.

The nature of the majority of security incidents

The majority of security incidents are due to the exploitation of known vulnerabilities for which patches already exist. Therefore, as was pointed out by Howard Schmidt in the last issue of the ENISA Quarterly in 2005, a security policy which pays appropriate attention to the monitoring, testing and installation of patches could prevent many security breaches from being exploited.

The effectiveness of certifications in a rapidly evolving ICT security scenario

The effectiveness of system/product certification is intrinsically limited by the evolving nature of possible vulnerabilities and attacks. In principle, the vulnerability analysis and penetration tests conducted by evaluators on the Target of Evaluation (TOE) could lead to completely different results if performed the day after the certification was issued! Of course in practice, if all of the security measures and environmental hypotheses implemented in the TOE have been carefully designed and evaluated, the TOE itself would probably be able at least to limit the effects of an attack.

On the other hand, the issued certification is valid only if the TOE is configured and operated in the exact conditions under which it was evaluated – with no successive patches or bug fixes. This puts the owner of a certified system in a dilemma: whether to keep the system secure, installing trusted patches, or to leave the system with the evaluated certification and exposed to potential vulnerabilities?

It appears that a strategy must be devised to allow the security patches to be applied while at the same time maintaining the assurance provided by certification.

The Italian Perspective

In order to understand how the above mentioned issues would impact on the diffusion of certification in Italy, we must bear in mind that the Italian ICT landscape is dominated by a small number of software and/or hardware producers with many system integrators that build solutions using commercial off-the-shelf hardware and software products. This situation is similar to that in many other European countries.

We expect that a great number of such systems could be certified by the Italian national certification body, OCSI. Nevertheless, developers are not willing to incur the costs and effort needed to afford a medium/high assurance level certification. Often they would rather undergo a low cost, quick evaluation process that requires very little additional effort and provides substantial revenue in terms of quality and image.

In order to promote the effective use of certification we aim to pursue the following goals:

- to promote system certification, as opposed to product certification, in order to guarantee comprehensive security to the end user, thus further increasing end user demand for certified systems
- to promote low assurance level certification, thus cutting down certification time-to-market and costs, in order to extend the penetration of certification in the ICT market and achieve a minimum guaranteed level of overall assurance
- to promote the maintenance of certification, in order to protect TOE users from new vulnerabilities that may arise. The approach proposed by OCSI consists in providing a framework (the Certification Management Scheme) within which minor modifications to the TOE can be introduced under OCSI supervision. So, if a security patch proves to be necessary (according to a well defined patching strategy) in order to keep the security functions effective, it can be installed, after providing OCSI with a rationale for installation. Obviously, the full validity of the certificate can be maintained only after a third party validation of the modified TOE has been carried out; this will typically occur on a periodic basis, unless major modifications are applied. Still, in the period between two third party evaluations, the TOE can be updated in a supervised manner.
- to increase security awareness within public administration in order to trigger a demand for certifications by users, as has been done in the USA.

Conclusion

We have analysed the factors driving the spread and actual use of system/product security certification. We believe that certification is a useful tool to promote security in the ICT world, provided that it is used with due attention to transparency and effectiveness. This is the goal of the Italian certification body.

Luisa Franchina is General Director of the High Institute for Communications and Technologies in the Italian Ministry for Communications, and Director of OCSI

Marco Carbonelli is the head of the OCSI 'evaluation facilities accreditation' division

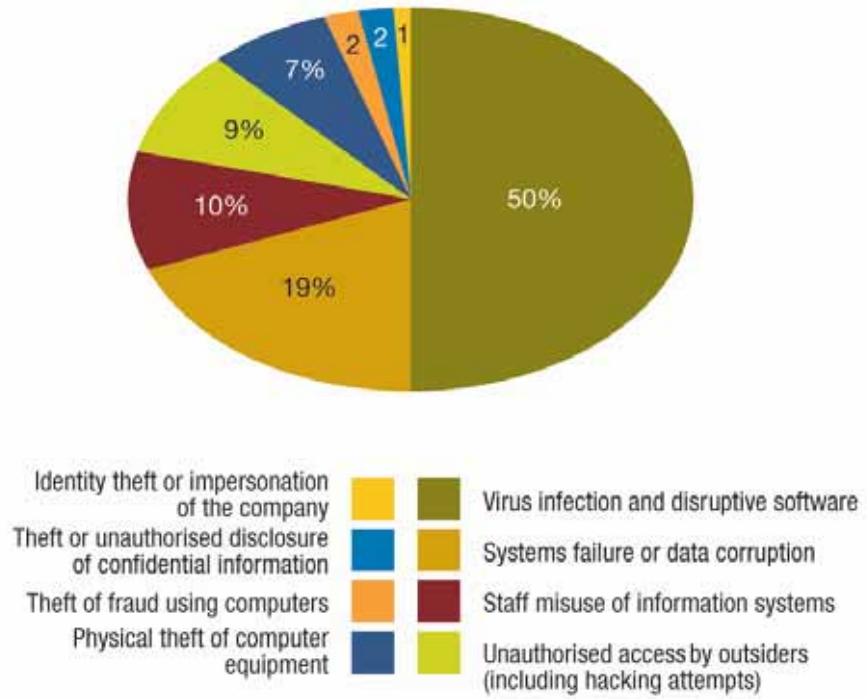
Laura Gratta is the head of the OCSI 'certification' division

UK Information Security Breaches Survey 2006

Pauline Tordoff

The UK's Department of Trade and Industry has been sponsoring research into information security breaches since the early 1990s in an effort to understand the nature of the problem and therefore help UK businesses understand the threats they face. The 2006 Information Security Breaches Survey was managed by PricewaterhouseCoopers and was sponsored by Microsoft, Clearswift, Entrust and Symantec. It is considered to be the most authoritative source on the state of information security in the UK. With over 1000 respondents, it is also the largest survey of its kind in the UK and is entirely non self-selective. The survey was conducted between October 2005 and January 2006 and is based on 1,000 telephone interviews with organisations of all sizes across the UK, plus a series of face-to-face interviews with information security officers to supplement the telephone interviews. Aside from the major sponsors, a number of organisations acted as independent reviewers.

What was the worst security incident faced by UK businesses?



The 2006 survey brings mixed news. With nearly every UK company making use of the Internet (97% have an Internet connection and 88% of these are broadband), the new business environment has brought with it new security threats.

> **"Security has a higher profile than ever before, with three quarters of UK businesses rating it as a high or very high priority"**

Security has a higher profile than ever before, with three quarters of UK businesses rating it as a high or very high priority for their senior management or board of directors. This priority status has translated into action with companies spending more on security controls, the consequence of which has been that the number of companies affected by security incidents seems to have stabilised. On average, 4-5% of IT budgets is being spent on security, three times as many companies have a security policy in place as six years ago and 98% of businesses have anti-virus software. Fewer companies had a security incident than in 2004 when the last survey was conducted. Overall, 62% of businesses suffered a security incident in the past year; this is down from 74% two years ago. Perhaps inevitably, larger businesses are more security aware and the total cost to them of security incidents has fallen by 50% over the past two years. It is the financial services sector that allocates the greatest priority to security, the retail sector the least. The 2004 survey indicated that security expenditure was treated as an overhead rather than an investment. The picture is different now and, although formal return on investment calculation in terms of security expenditure is rare, most UK companies make formal business cases and attempt to quantify the benefits of security expenditure.

The less positive news is that the burden of security incidents seems to be falling disproportionately on small businesses where security controls are less well developed. Indeed there seems to be a small core of companies which still appear to think security doesn't affect them and these companies can lack even the most basic security controls. The average number of security incidents has risen by 50% to roughly eight a year. Average financial losses are in the region of £500 - £1,000 for smaller companies, and £3,500 - £5,000 for large firms. While trying to extrapolate these figures to reach an average financial cost for the entire business community is an imprecise science at best, several thousand pounds is about as accurate as it is possible to be. Actual financial loss in fact remains a small part of the overall cost of security incidents. Damage to reputation can have a much longer lasting impact on a company's brand. Larger businesses can suffer from adverse media coverage and household names in particular are an obvious target.

Greater use of emerging technologies is changing the nature of the security threat UK businesses face. Companies are slow to adopt controls to reduce this threat – for example a quarter of UK businesses are not protected against spyware. Although more wireless networks are protected than two years ago, one in five is still completely unprotected and a further one in five is unencrypted. 55% of firms have not taken any steps to protect themselves against the threat posed by removable media devices. Two-fifths of companies that allow staff to use Instant Messaging have no controls in place over its use. Of the companies that have implemented Voice over Internet Protocol (VoIP) telephony, half did so without evaluating the security risks.

Having security controls in place is only a start. Although most companies now have anti-virus software, and patching discipline has improved, virus infection was still the biggest single cause of respondents' worst security incidents. The nature of the virus threat has changed; in 2004 a small number

of viruses such as Blaster were dominant, whereas, over the past year or so, there has been a huge number of different viruses and variants. The nature of viruses and the motivation of their writers have also changed. Viruses are now much more insidious with programmes hidden on infected machines ('bots'), gathering information and targeting valuable data.

A consequence of the high level of broadband take up in the UK is that 63% of companies, recognising the risks this can bring, have acceptable usage policies in place. 42% restrict access to the Internet to certain staff only. However, only one in six UK companies scans outgoing e-mail for inappropriate content. Those that do scan were nearly three times as likely to detect incidents of staff e-mail misuse.

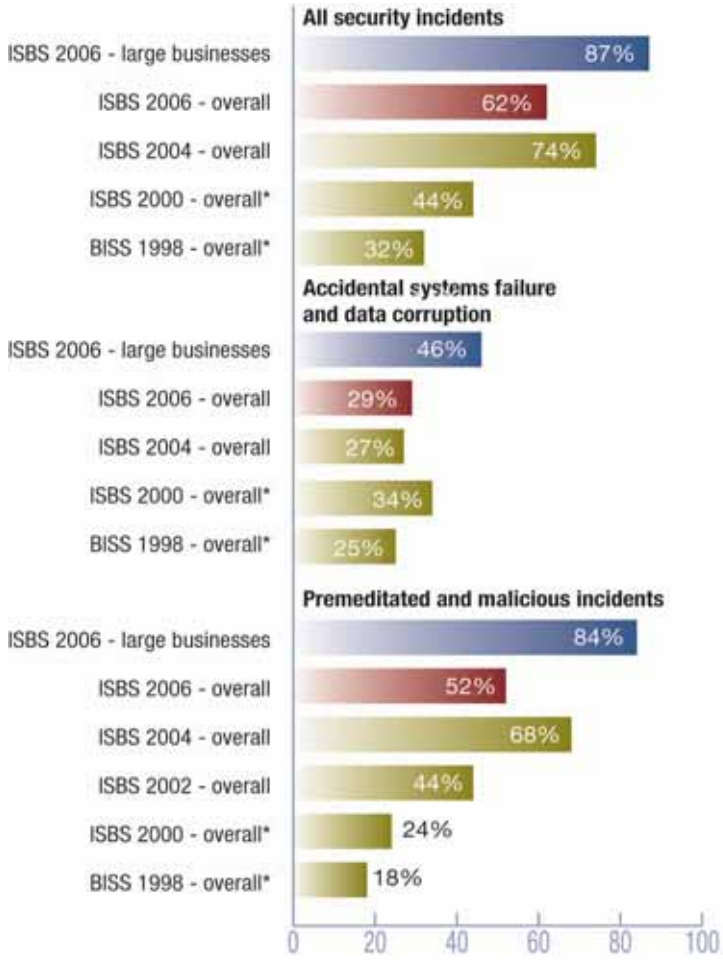
Greater adoption of transactional websites, as well as regulatory requirements (in the UK, the Data Protection Act is an obvious example) are driving the need for stronger authentication. 90% of respondents described compliance with laws and regulations as a key driver of security expenditure. Incidents of unauthorised access are low and remain consistent with figures for 2004. This type of fraud, although relatively rare, can have a serious impact however.

> "The average number of security incidents has risen by 50% to roughly eight a year."

With more consumers than ever buying goods over the Internet, the issue of trust is central to public confidence and the public remains concerned about the security of online transactions. 90% of firms considered the protection of customer data to be the strongest justification for security expenditure. Some 80% of UK companies have a website (among large firms the figure is 93%), most accept orders online and most of these use payment service providers.

There was a rise in the number of companies that reported an attack on their Internet or telecommunications traffic. Over a quarter of those affected by attempts to break into their networks said they suffered at least one significant attempt every day. The businesses attacked tended to be those that accept financial transactions online. All the websites that accept financial transactions are behind a firewall. Fewer

What proportion of UK businesses had a security incident in the last year?



* The 2000 and 1998 DTI survey figures were based on the preceding two years rather than the last year. In addition, they included operator user errors as a security incident; these have been stripped out of the totals to present on a like for like basis. The ISBS (Information Security Breaches Survey) 2002 did not cover accidental systems failure.

than two-thirds of websites accepting financial transactions encrypt the data they receive. In contrast, every transactional website run by a very large respondent uses encryption. Controls over authorised wireless networks have improved. The number of unprotected networks has halved since 2004, but there is no room for complacency – one in five firms still lacks any controls.

We have attempted to pull together some key recommendations for UK companies based on the survey findings. These are that companies should:

- Draw on the right expertise and international standards such as ISO 27001 to understand the security threats they face and their legal responsibilities
- Integrate security into normal business practice, through a clear security policy and staff education
- Use risk assessment to target their investment in security controls at the areas of maximum business benefit
- Make sure their key security defences are up to date and integrated, and address emerging technologies they are exposed to (such as spyware, instant messaging, Voice over IP etc.)
- Develop contingency plans so that they can respond to any security incidents efficiently and minimise business disruption.

The overall message of the 2006 survey is that UK businesses are more aware than ever of the risks they face from information security breaches and, whilst there is much to applaud in terms of increased security spending and better security controls, there is no room at all for complacency. Nearly two-thirds of UK businesses believe there will be more security incidents in the next year than in the last and also believe it will be harder to detect security breaches in the future. In contrast, only one in five is optimistic about the future outlook.

While we suspect that UK companies are not significantly different from other European companies, it would add considerable value to the survey to be able to benchmark against other parts of the EU (in aggregate and by sector). Of course, our focus is on businesses and there is a bigger challenge to ascertain how home users understand and respond to the changing problems – and the extent to which the perception of a security or privacy risk really determines what they are prepared to do online.

The Survey (the main Technical Report, the Executive Summary and a series of four accompanying Fact Sheets) can be found on the ENISA website at www.enisa.europa.eu (under 'Studies') or go to www.dti.gov.uk/sectors/infosec (the survey deliverables are available under 'Downloads').

Pauline Tordoff is a Senior Policy Adviser in the Information Security & Internet Policy Team at the UK Department of Trade and Industry

IT Security for the Public: A CERT for End Users

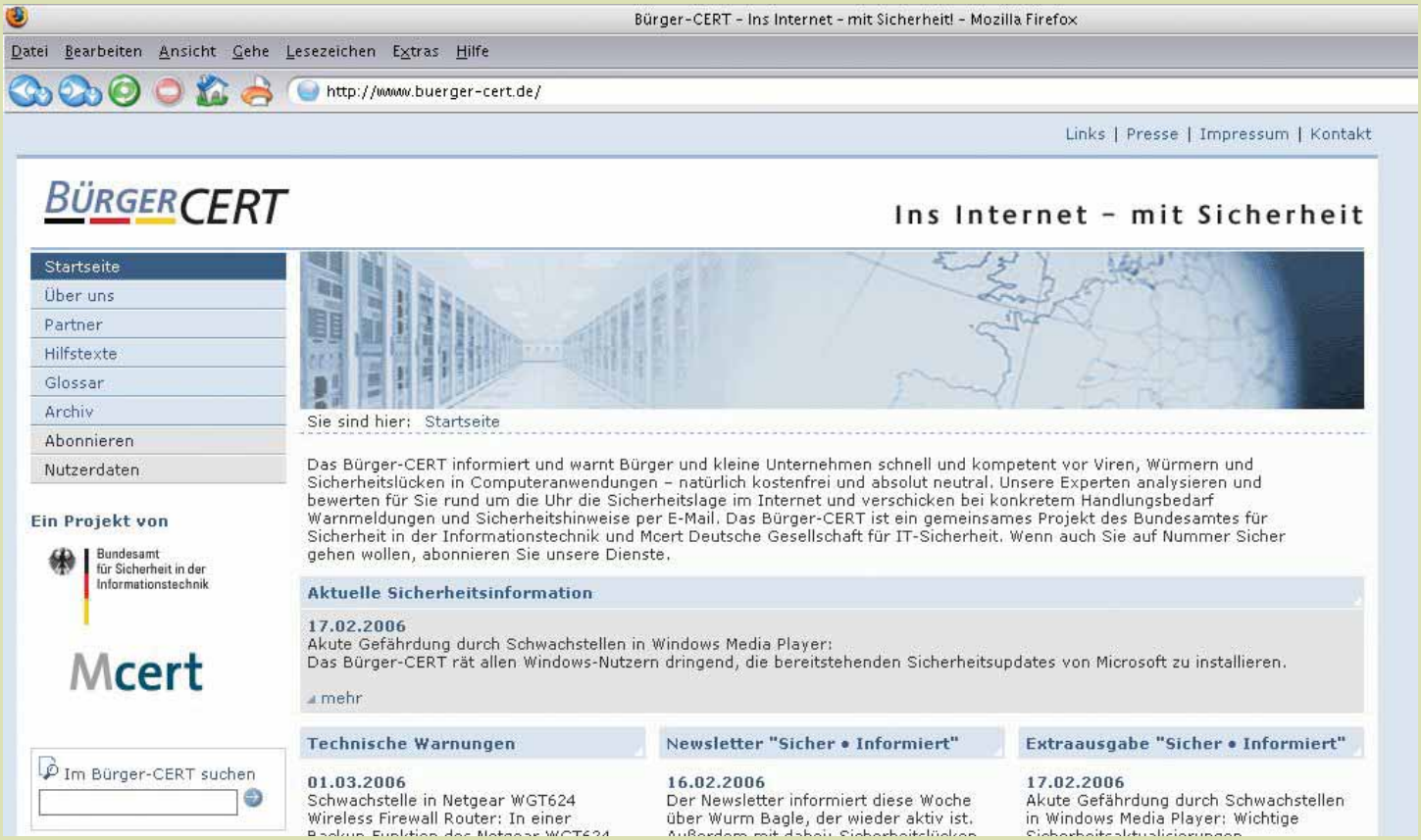
Anke Gaul

In the private and business sphere alike, IT systems are vulnerable to hackers, computer viruses, worms and other risks. As malicious software often turns victims into unwitting perpetrators, every user is responsible for making a small contribution to the overall security of the Internet. To help reach this goal, the German public initiative, Bürger-CERT (or 'Citizen-CERT' (Computer Emergency Response Team)), has been offering free information and support for effective self-help since March 2006.

In the age of phishing attacks and rapid adoption of new technologies such as VoIP and WLAN, private Internet users as a target group are an increasingly important component of online security. As the upsurge in bot networks transforms an increasing number of private PC users from mere victims into technical 'accomplices', educating private users to raise their level of security awareness has taken on added urgency.

The mutual dependence which increased networking gives rise to is still underestimated and underappreciated by the public. The individual citizen still, all too frequently, perceives his environment as a microcosm. He does not see himself as part of the Internet and therefore does not recognise his personal responsibility for the technology that he uses on his PC and in applications. This detached attitude means he invests little time or effort in IT security.

So far – so bad! Yet how can members of the public contribute to Internet security and thus to their own security? And more crucially, how can they be motivated to take responsibility for promoting Internet security? When it comes to implementing measures, if users do not know why they need to take action, the result will be indifference and a perfunctory attitude. Only when the motivation is clear can the user understand and, by implication, know and act.



Federal Interior Minister Dr. Schäuble and Dr. Helmbrecht, President of the BSI, launched the Bürger-CERT in March.

Photo courtesy BMI

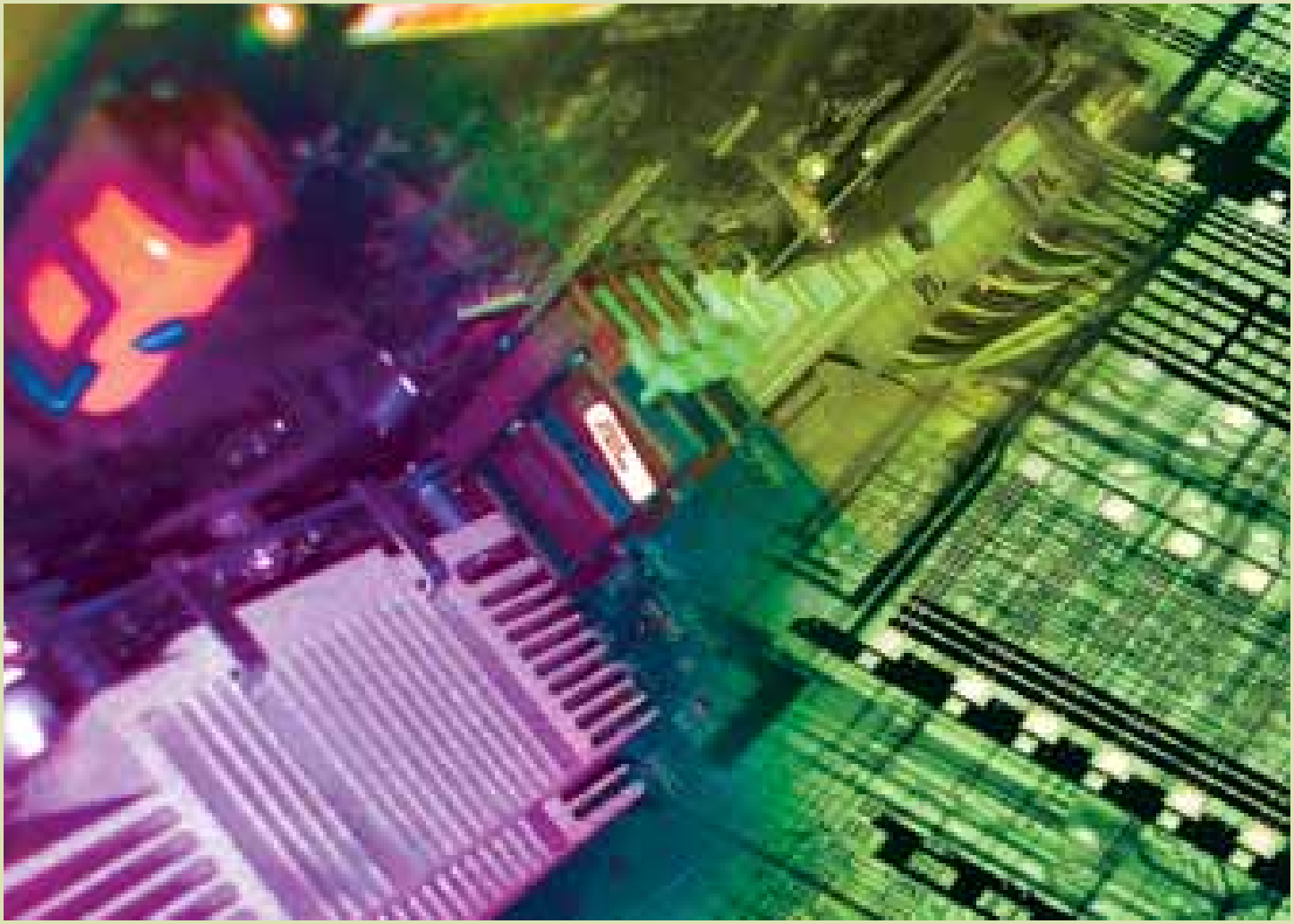
It is therefore only possible to achieve a satisfactory approach through continual education and awareness training. One major problem in this complex issue is that there is precious little 'natural interest' in the topic of IT security among the general public. Users are busy and their time is precious, so they must be given the opportunity to access information without any great commitment of time or financial outlay. A balance must be struck between avoiding information overflow while at the same time maintaining an uninterrupted information flow.

The German Federal Office for Information Security (BSI) has already been focusing on a direct approach to the public for some time. The aim is to create a security culture supported by all the social groups in Germany and, in doing so, to improve the basic infrastructure conducive to the development and use of secure information technology. To this end, as early as 2002 the BSI released the CD-ROM 'Ins Internet – mit Sicherheit' (roughly translated: 'Into the Internet – Safely!'), a guide for the public on safety in using the Internet. The portal www.bsi-fuer-buerger.de was developed as a result of the great demand and the permanent need for updating. Security programmes are also available for download free of charge.

A CERT for Citizens

Despite these efforts, it was still felt that a more proactive approach was needed. The attacks and threats emerging from the Internet today require extremely short response times. Concrete information, rapid communication and clear procedural recommendations are therefore essential – and all the more so for the general public. This basic necessity spawned the idea of setting up a CERT for citizens.

CERTs are teams of security specialists who watch the IT infrastructures in networks, publish warnings and security information, and provide support in resolving IT security incidents. In setting up the Bürger-CERT, the BSI joined forces with its IT security partner, Mcert Deutsche Gesellschaft für IT-Sicherheit, and, since March 2006, has been delivering information to Internet users who register at Bürger-CERT, (www.buerger-cert.de). The project is financed by an alliance between the public authorities and partners from the private sector. Through this alliance, the German government and the information and telecommunications industry are demonstrating that they take their responsibility for the protection of IT infrastructures seriously.



The Bürger-CERT represents a new approach in Germany – until now, the services provided by private CERTs have only been available to companies, and those provided by the BSI's Federal Computer Emergency Response Team, CERT-Bund, have only been available to the public authorities. Bürger-CERT meant providing, for the first time, impartial and free warnings and information on IT security to the general public and small companies. Through this unique service Internet users now have access to a rapid, competent and comprehensive source of information and advice on specific risks and threats.

An important feature of the Bürger-CERT service is that the business partners have no editorial influence on the independent and unbiased content the service provides. Impartiality is the key criterion for the success of the service, as this approach is the only way to foster a high degree of trust.

The Bürger-CERT provides its warning and information service in parallel on three different levels. The user can select which services to use based on his or her individual security requirements. The online newsletter, 'Sicher Informiert', is a fortnightly bulletin covering the main items of security news. 'Extraausgaben' (extra issues) of the online newsletter are published in the event of extremely time-critical security vulnerabilities which call for immediate action. Rounding out the service, the 'Technische Warnungen' (technical warnings) cater for the more technically-minded and more experienced users and contain detailed background information.

The Bürger-CERT plays an important role in helping secure the end user. However, the delivery of condensed information directly to the public's PCs in an easily-understandable form does not absolve them of personal responsibility. Countless studies have repeatedly demonstrated that the problem of security arises through misconceptions and negligence in the use of IT. Education and awareness will continue to play a key role in ensuring that users take responsibility in securing their machines by implementing the recommendations and installing security updates and patches.

Anke Gaul is an Adviser on Information, Communication and Public Relations at the BSI

2006 ISSE INFORMATION SECURITY SOLUTIONS EUROPE

Rome, Italy 10 – 12 October 2006

The Independent European ICT Security Conference and Exhibition

A thousand threats. Many Solutions. One Conference.

ISSE 2006 is the essential conference for anyone in the IT security arena, bringing together Europe's top ICT security experts, suppliers and implementers.

In three days, you can choose from over 70 presentation sessions on all the hot topics in ICT security.

Day 1 Tuesday 10 October 2006 10.00 - 18.00

Opening Plenary

Welcome Address: Andrea Pirotti, Executive Director, ENISA; Representative from the Italian Ministry

Keynote: The Economics of Information Security: Ten Trends, Bruce Schneier, Founder & CTO, Counterpane Internet Security Inc

Track 1: Technology	Track 2: Legal, data protection & compliance	Track 3: Security Management	Italian Workshop
Smart Tokens, RFID and e-ID cards	Awareness raising and incident response	Identity management, authorisation and provisioning	Security issues from an Italian perspective
	Compliance and governance		

Day 2 Wednesday 11 October 2006 08.30 - 17.30

ENISA Plenary and Panel Discussion Bringing Security to the End User

Track 1: Technology	Track 2: Legal, data protection & compliance	Track 3: Security Management	Track 4: Trusted computing and DRM
Biometrics	Data protection and privacy	Identity management, authorisation and provisioning	Trusted computing and DRM
PKI		Economics of security	

Day 3 Thursday 12 October 2006 09.00 - 15.00

Track 1: Technology	Track 2: Legal, data protection & compliance	Track 3: Security Management	German Workshop
Security Standards	e-Government applications	Web services security	Cooperative IT security solutions
Interoperability & security standards	Network security	Mobile and wireless	

Closing Plenary The Crypto Year in Review
Bart Preneel, Professor, KU Leuven, Belgium

Organised by enisa | Owned developed and run by eema | Programme compiled by | Hosted by iscom | Supported by Federal Office for Information Security, Federal Ministry of the Interior

To register for ISSE 2006 or for information visit **www.eema.org/isse**

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: Boaz Gelbord
boaz.gelbord@enisa.europa.eu

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

European Communities, 2006
Reproduction is authorised provided the source is acknowledged