enisa

European Network
and Information
Security Agency

ENISA – Securing Europe's Information Society

Legal notice

This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004 as amended by Regulation (EC) No 1007/2008.

This publication might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Contents

ACTIVITIES

enisa

European Network
and Information
Security Agency

About ENISA

The European Network and Information Security Agency (ENISA) is a centre of expertise for network and information security (NIS) which is bridging the gap between citizens, industry and governments by acting as a knowledge broker in NIS matters and as a promoter of good NIS practices for EU Member States.

ENISA is a decentralised agency of the European Union. It was established in 2004 and is based in Heraklion, Greece.

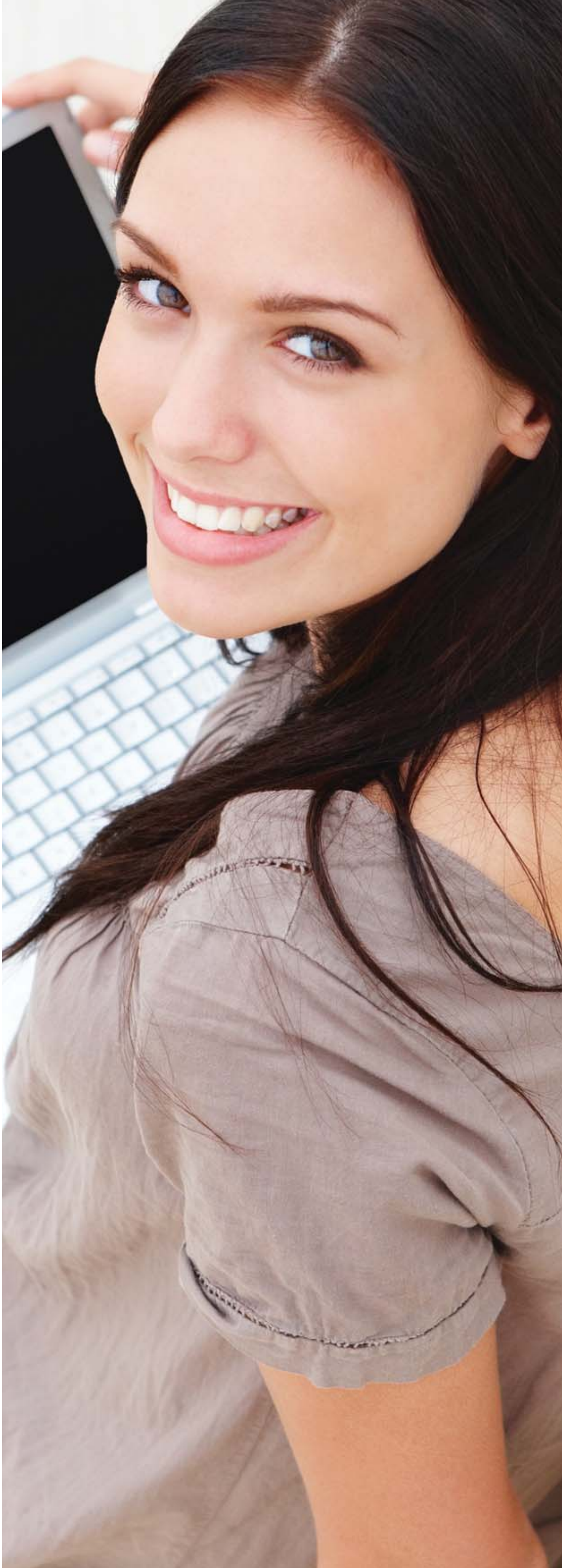
ENISA objectives are:
1. to secure Europe's information infrastructure;
2. to cultivate e-privacy, ie, trust and confidence in the use of ICT;
3. to promote information security standards, guidelines and certification schemes;
4. to educate the wider public on ICT.

ENISA has published numerous reports and studies on, among many other issues, the security of USB drives, printers, spam, social networking, botnets, standards, risk assessment, risk management, business continuity, 'digital fire brigades', and how to obtain the CEO's support for awareness raising, as well as a study of the European Information Sharing and Alert System (EISAS) for SMEs and citizens.

ENISA also co-organises conferences, runs workshops, produces the ENISA *Quarterly Review* to encourage the debate on NIS matters, and publishes position papers.

As a European agency, ENISA is uniquely positioned to bring together a wide variety of crucial players in the Network and Information Society by acting as a neutral and independent advisor. With its technical expertise, its central position and its independence, the Agency is well placed to ring the alarm bells on emerging and future risks.

European legislators are currently drawing-up on a new mandate for ENISA.



ENISA – meeting the demands for a more secure Europe

In the European Union, network and information security (NIS) is a prime concern for citizens and businesses alike. Because of its importance for employment and the economy as a whole, citizens expect the EU to ensure the security of their communication networks, enforce online privacy and prevent computer crime.

> *...the Council's conclusions of April 2010 indicate closer cooperation between ENISA and authorities that fight cyber-crime*

As a result, NIS is gaining increased political attention within the EU. Indeed the Digital Agenda – one of the seven flagship initiatives of the Europe 2020 Strategy – underlines the key role secure information and communication technologies (ICT) will play in enabling Europe to achieve its economic ambitions for 2020.

The Digital Agenda recently expressed the significant degree of trust it has placed in ENISA, the European Network and Information Security Agency, when Commissioner Neelie Kroes stated:

… cooperation of relevant actors needs to be organized at the global level to be effectively able to fight and mitigate security threats. This can be channelled as part of discussions on Internet governance. At a more operational level, internationally coordinated actions targeting information security should be pursued, and joint action should be taken to fight computer crime, with the support of a renewed European Network and Information Security Agency.

In a resolution in December 2009, the Council of the European Union issued a strong statement in favour of a collaborative European approach to network and information security. This resolution marks a milestone for NIS in Europe as it reflects an identified need and the willingness of the Member States of the European Union to act in concert. In addition, the Council's conclusions of April 2010 indicate closer cooperation between ENISA and authorities that fight cyber-crime.

ENISA's work in NIS is highly appreciated. Citizens have increasing expectations of the EU on security issues and, with an ever-growing need for a safe economy, the Agency is considered a crucial asset in ensuring the overall security of Europe's network and information systems.

Who we are

ENISA was established in order to increase the capacity of the European Union, the EU Member States and the business community to prevent, address and respond to network and information security (NIS) issues.

ENISA is a **centre of expertise** in network and information security.

Its aim is to:

- Provide independent, expert advice on NIS to the European Union;
- Promote good practices in risk assessment and risk management, resilience, awareness raising and responses to computer security incidents.

The challenges facing NIS are vast, multi-faceted and urgent. They affect individual users and, crucially, they affect the economy and infrastructure of Europe. Tackling these challenges requires a systematic, coherent and integrated strategy that involves all concerned stakeholders and decision-makers and is based on dialogue and partnership.

The pace of technological development over the last few years has been unparalleled. Even the Industrial Revolution, which changed the way we live and work so dramatically, did not move this fast. Today we are surrounded by information and communications technologies (ICTs) which have become essential tools in human, business and economic relations and offer marvellous benefits to mankind.

But these technologies can also bring massive risks that could jeopardize the security of both our society and our economy. A breach in NIS can generate an impact that transcends the economic dimension and it is now widely accepted that the availability, reliability and security of networks and information systems should be of the highest concern. However, strengthening trust in the use of networks, software and services for governments, businesses and consumers remains a major task.

A culture of security

ENISA's scope of work includes ensuring a high and effective level of network and information security within the Community. The Agency is also expected to develop a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organisations of the European Union, and thus contribute to the smooth functioning of the internal market.

ENISA's scope of work includes ensuring a high and effective level of network and information security within the Community

All Stakeholders have a key role to play in network and information security (NIS):

- **Public administrations** need to make informed policy decisions and to address the security of their own systems, not just to protect public sector information, but also to serve as examples of good practices for all players.
- **Enterprises** increasingly see NIS as a critical element in their success or failure, and also as an element of competitive advantage rather than as a 'negative cost'. They need to be given the tools to exploit information technologies securely.
- **Citizens** are the targets of malware and extortion through botnets, and suffer real economic and emotional damage as a result of poor NIS practices. Users must be made aware of how they can and must protect themselves and the security of the network as a whole.

Pooling information, facts and knowledge

To expand and improve the opportunities for EU Member States to share information, ENISA is developing various models of cooperation in areas such as awareness raising, incident response and electronic identity (eID). The Agency has established a European NIS good practice brokerage, along with supporting tools such as an online platform, the *Who-is-Who Directory of Network and Information Security* and 'country reports' of activities in the Member States.

ENISA conducts surveys and produces position papers, reports and studies on the current state of play in NIS in Europe. Over the last five years these have included – among many others – issues such as the risks to children on the Internet, the security of USB drives and printing devices, information sharing, exercises in critical information infrastructure protection (CIIP), incident reporting mechanisms, spam, standards, risk assessment, risk management, certification schemes, eID, security economics, business continuity, and computer emergency response teams (CERTs).

Recognising the importance for the economic growth of Europe's small and medium enterprises (SMEs), which represent 99% of all enterprises in the EU and around 65 million jobs, ENISA is addressing the specific problems of SMEs and distributing relevant information to these businesses. As such, the Agency is the 'hub' for knowledge and good practices in network and information security across Europe.

> *ENISA is the 'hub' for knowledge and good practices in network and information security across Europe*

ENISA assists EU Member States and institutions with specific security problems, ranging from help with training to advice on Internet security.

Social networks and Web 2.0

Web 2.0 is sometimes called 'the read-write web' because it enables ordinary users to contribute content to the web instead of just being passive consumers of information. Perhaps the most important application of the read-write web is the social applications which the European Commission predicts will be used by over 100 million Europeans by 2012.

ENISA has been active in this area since 2007 when it published its widely cited position paper *Security Issues and Recommendations for Online Social Networks*. The report was one of the first to publicise many of the information security and privacy issues relating to online social networks, such as inappropriate disclosure, privacy issues concerning image tagging and face recognition technologies, the difficulty of account deletion and the dangers of data lock-in for privacy and security.

In 2008, ENISA published a related report on privacy and security risks in Web 2.0, highlighting inter alia the technical and systemic risks of access control in the new breed of web applications and the reasons for the clear increase in the distribution of malware (such as viruses, worms, Trojan horses, spyware, etc) via web browsers. This report also describes the problems in establishing trust in user-generated content, which make it easier to promote fraudulent information for criminal purposes. ENISA has also published a report on security and privacy in gaming and virtual worlds, which describes the very real financial and privacy risks inherent in these activities.

ENISA continues to promote the results of its studies in invited contributions to safer internet fora and to the Economic and Social Committee at the European Parliament. ENISA will continue to monitor emerging risks in this area, particularly as social networks and Web 2.0 move into the mobile and smartphone space.

Cloud computing

Cloud computing is Internet-based computing whereby shared resources, software, and information are provided to computers and other devices on demand. It is a new way of delivering computing resources – it is not a new technology.

Computing services ranging from data storage and processing to software, such as email handling, are now available instantly, commitment-free and on-demand. This new economic model for computing has found fertile ground and is seeing massive global investment.

ENISA has been studying the cloud model in order to identify, on the one hand, the most prominent risks and most critical vulnerabilities and, on the other, the main information security benefits of cloud computing. The final goal has been to provide decision-makers and potential and existing users of cloud services with useful support for making informed risk-based decisions.

The key conclusion is that the cloud's economies of scale and flexibility are both a friend and a foe from a security point of view. The massive concentrations of resources and data present a most attractive target to attackers, but cloud-based defences can be more robust, scalable and cost-effective than conventional computing.

In 2010 ENISA is following up these studies with two further activities in the area of cloud computing. The first is a study of the impact of cloud computing on the security and resilience of services offered by governments and public administrations. The second project, called CAMM (Common Assurance Maturity Model), involves an evolution of the Information Security Framework.

Helping European citizens to protect themselves

The economy, businesses, and citizens at work and at home are part of the Digital Economy and Information Society and are dependent on the use of computers and mobile phones in everyday life. Given its importance for society and citizens, the European Commission identified the need to address the issue of 'effective responses to existing and emerging threats to electronic networks' in Europe. In order to develop 'informed, proactive and vigilant' citizens, an activity called EISAS (European Information Sharing and Alert System) was launched to better reach out to home-users and micro-enterprises.

> *...the goals of EISAS's activities are more important than ever*

ENISA carried out a feasibility study on a Europe-wide system for sharing NIS related information with end-users, citizens and micro-enterprises that would raise IT security awareness and close gaps in the coverage of such information. The study concluded that the most effective way for the European Union to establish and operate an information sharing system for its home-users and micro enterprises would be to undertake the role of mediator and a 'keeper of good practices'.

Considering that the majority of computers that can be misused in botnets (ie, nets of computers controlled remotely by criminals) do in fact belong to home-users or micro-enterprises, the goals of EISAS's activities are more important than ever.

ENISA will soon publish a roadmap on how two piloted projects can be transformed into tangible results in the Member States.

Computer Emergency Response Teams – CERTs

A computer emergency response team (CERT) is a team of IT security experts whose main business is to respond to computer security incidents. The name explains what makes these entities so special; like a fire brigade, they are the only ones who can react when a security incident occurs. A CERT provides the necessary services to handle these incidents and supports its customers so they may recover from security breaches.

Besides reactive services (incident response), CERTs also usually provide a comprehensive portfolio of other security services for their customers, such as alerts and warnings, advisories and security training. Over the past 22 years, CERTs have evolved into premium providers of security services.

The European Commission stated recently that a well-functioning national or governmental CERT plays a major role in protecting critical information infrastructure in Member States and that it is mandatory for each Member State to maintain such teams.

ENISA supports Member States and their CERTs by providing help with the establishment and general training of teams. ENISA, together with stakeholders in Member States, has also defined so called ‘baseline capabilities’, a set of de facto standards for the operation, technical equipment and mandates for new and established teams. ENISA also helps CERTs to enhance their capabilities, by providing advice on good practices and support in cross-border cooperation or by establishing new services.

ENISA has become the *de facto* centre of CERT competence in Europe, a place to which Member States can turn for support. One very recent example comprises the activities around EISAS, a framework aiming at helping national CERTs to better reach out to the citizens they protect with information sharing and security alerts.

ENISA is also available to close operational gaps at the European level. If called upon, ENISA can deliver valuable work by providing CERT services for European institutions that do not yet have their own CERTs.

Secure and resilient communication networks

Reliable communications networks and services are critical to public welfare and economic stability. Attacks on the Internet, disruptions due to physical phenomena, software and hardware failures, and human error all affect the proper functioning of public communications networks.

Such disruptions reveal the increased dependency of our society on these networks and their services. This experience shows that neither single providers nor a country on its own can effectively detect, prevent and respond to these threats. The EU Commission's *Communications on Critical Information Infrastructure Protection* (CIIP) highlighted the importance of network and information security and resilience for the creation of a single European information space.

> *The Agency will contribute, and lead where necessary, to a European-wide public private partnership for resilience*

ENISA has launched a multi-annual programme which delivers stock takings, analysis and recommendations on the policies of Member States, and on the regulatory and operational environments of various technologies (such as IPv6 and DNSSec), as well as on measures that service providers should take. The programme also makes proposals for research priorities and recommends areas for standardisation.

The Agency will – together with Member States and private stakeholders – contribute, and lead where necessary, to a European-wide public private partnership for resilience (EP3R), develop national information sharing exchanges and, in the future, a pan European platform. Furthermore, ENISA will develop good practices for measuring, disinfecting and defending against botnets, develop guidelines for implementing article 13a of the New Telecom Package including measures for reporting incidents to ENISA annually in an aggregated manner, and develop guidelines for interconnected networks and interdependencies among networks.

Trust and privacy – enduring challenges in an evolving networked world

The Digital Agenda identified the key actions needed to assist the viable economic growth of the European economy and to provide Europeans with a better quality of life (ie, through the use of e-services such as e-health and e-invoicing).

The identified objectives cannot be achieved without trusted information infrastructures and services and without protecting the privacy and personal data of individuals. ENISA contributes to the accomplishment of these objectives by addressing them in its work on, for example, improving resilience in European e-communication networks, trusted identification mechanisms (eID), secured and privacy enabling online services, the integrity of the supply chain for electronic components, and the legislation required for the protection of personal data in the context of the new technologies.

A good practices guide for deploying DNSSEC and a study on the costs of its deployment have been published. Other studies covering the principles of end-to-end resilience as well as secure routing technologies and their deployment are being undertaken. Such technologies are expected to enhance the resilience and security of networks and enable citizens to trust communication infrastructures.

ENISA plays an active role in tracking standards. In this context, the Agency has analysed the gaps in current standards related to the resilience of communication networks and provided the community of standard developing organizations with five key recommendations in this area.

In February 2010 ENISA analysed the current situation and assessed the security risks of electronic authentication in cross-border solutions.

Since then it also launched new activities in the area of ‘trust and privacy on the future Internet’. One example is a study covering European requirement for the notification of data breaches for the telecommunications sector. Based on the contributions of well known experts in their respective fields, ENISA published *Priorities for Research on Current and Emerging Network Technologies*.

Over the next few years ENISA will continue to address the challenges of trust and privacy in a networked world that is evolving continuously.

Reporting security incidents

Incident reporting plays an important role in enhancing the security and resilience of communications networks.

In a number of key policy documents, the Commission highlighted the importance of getting reliable, up-to-date and comparable data on security incidents in order to develop a clear understanding of the nature and extent of the challenges at stake. Such an understanding is needed for effective and informed policy making and business decisions.

The recently adopted reform of the Telecommunications Regulatory Package specifies that Member States must ensure that telecom operators notify the competent national regulatory authority of any breach of security or loss of integrity that has had a significant impact on the operation of their networks.

ENISA will establish a permanent communication platform to engage Member States

ENISA carried out an extensive stock-taking of the activities of Member States with the aim of identifying and analysing existing practices in the procedures for the reporting of incidents. The main objective was to identify good practices and to share them with Member States. Such a stock taking of good practices serves as a basis for the overall discussion on how Member States may best implement the provision on the notification of breaches contained in article 13a of the revised Framework Directive.

ENISA will establish a permanent communication platform to engage Member States and the private sector in the establishment of a framework for how the Agency will collect and analyse the information reported by the Member States.

First pan-European exercises on resilience

Exercises are an important tool to assess the preparedness of a community for natural disasters, technology failures and emergency situations.

Exercises enable competent authorities to target specific weaknesses, increase cooperation across a sector, identify interdependencies, stimulate improvements in continuity planning, and generate a culture of cooperative effort to boost resilience.

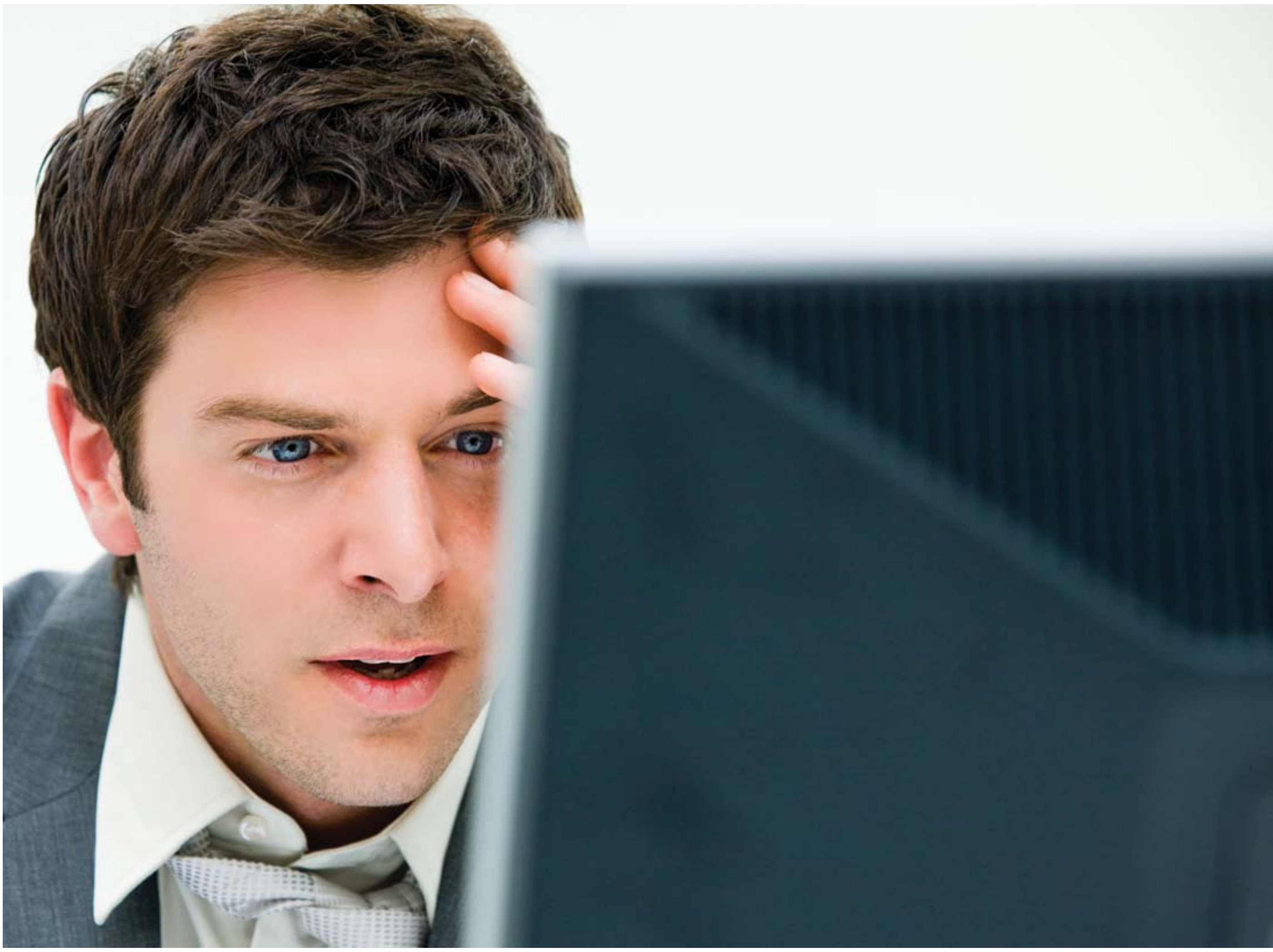
ENISA has developed a good practices guide on planning and conducting national exercises and is preparing to conduct such training at EU-level

In an effort to support Member States to enhance the resilience of critical information infrastructure, ENISA has developed a good practices guide on planning and conducting national exercises and is preparing to conduct such training at EU-level – as called upon by the Council and the Commission.

The exercise scenarios encompass incidents that involve the resilience of the Internet. Such incidents would affect all participating countries.

The objectives of the exercises include building trust, increasing the understanding on how cyber incidents are handled, testing communication points and procedures between participating Member States, understanding interdependencies between key actors within each Member State, and promoting mutual support between Member States.

Participants in the exercises will be public authorities in EU Member States and the European Free Trade Association (EFTA).



Botnets

Cyber attacks, such as distributed denial of service attacks (DDoS) carried out by so-called ‘botnets’, have become one of the foremost cyber-threats of the 21st century. Criminals and terrorists gain command of networks of hundreds of thousands of compromised ‘zombie’ computers by infecting them with viruses, worms and other malware.

They use these computers to perpetrate acts of political terrorism, to overwhelm key digital services and extort money from their owners, to send spam and defraud internet advertising services (‘click-fraud’). In so doing, criminals and terrorists could successfully transform citizens into weapons without their knowledge.

No single measure is enough to counter these modern forms of warfare and crime. The European Commission has proposed a multi-stage response to these recent threats. ENISA is also actively supporting these actions in order to protect European citizens.

In 2010 ENISA conducted a study on *Botnets: Detection, Measurement, Disinfection and Defence*.

The first part of the project focused on evaluating methods for measuring the size and impact of botnet infections, with a view to providing sound advice to decision-makers on the true level and nature of these threats. The second examined the problem of defending EU infrastructures against attacks.

In both cases a broad survey of techniques and a gathering of expert opinion on good practices was conducted. All aspects of the problem, including economic, social, technical, legal and political issues, were considered.

For example, many defensive measures which are technically possible are not legal in Europe. As most botnet attacks are economically motivated, ENISA also examined the question of how to minimise the potential criminal revenues from botnets.

Awareness raising

Users' awareness is the first line of defence for a safe and secure networking environment, as humans being are the weakest link in the information security chain.

Information security tips for the general public

- Do not provide personal information online unless you initiated the contact and you are sure you know with whom you are dealing. Never give your full personal data online; in situations where you are required to provide some personal details, make sure you do so at trusted websites that have valid, trusted certificates.
- Protect your PC with a firewall, anti-virus software and anti-spyware software obtained from trusted sources.
- Check the terms of use for what you install and download and be wary of 'free' programs that offer to install additional programs.
- Make your browser safe by having the latest version installed.
- Install the latest updates for your operating system and software.
- Look for web sites that indicate that an encrypted connection is being used to communicate your data before you make any online payments — URLs that start with 'https://' rather than 'http://' and that also have a small padlock icon in the browser window.

Information security tips for employees

- Use portable devices such as laptops, USB drives, mobile phones and Blackberries in accordance with corporate security policies.
- Handle corporate information with care, carefully disposing of it, printing, copying and scanning it only when necessary, always shredding it if it contains sensitive information, storing it only on the organisation's drives and ensuring that any third party working with the company has signed a non-disclosure agreement before being given access to any sensitive data.
- Report any loss of portable corporate devices and any security breaches and/or incidents to the IT department of your organisation.
- Protect information when you are outside your organisation by ensuring you keep sensitive data and equipment secure at all times to prevent theft.

Parents and guardians should be educated, empowered and engaged to ensure a truly positive and valuable Internet experience for their children, while reinforcing safe online habits in the process.

Internet safety tips for helping parents and guardians of children

- Communicate with your child about his or her Internet experience. Discuss the importance of Internet safety and teach the basics.
- Educate yourself on the latest threats facing children online and have a good understanding of how your child spends his or her time online.
- Analyse content providers' policies. Check contractual flexibility (eg, how to delete an account) and the use of automated moderation filters.
- Tell your child to avoid using his or her full name and sharing passwords. Prevent your child from sharing identifiable personal information (eg, address, telephone number, name of school, or sport clubs). A minor should never be in a position to enter data unassisted.
- Ensure your child understands the implications of posting photographs and personal data on the Internet.

References

PAGE 9

Web 2.0 Security & Privacy **(http://www.enisa.europa.eu/act/it/oar/web2sec?searchterm=web+)**
Recommendations For Online Social Networks **(http://www.enisa.europa.eu/act/it/oar/social-networks/security-issues-and-recommendations-for-online-social-networks)**
Online as soon as it happens **(http://www.enisa.europa.eu/act/ar/deliverables/2010/onlineasithappens?searchterm=social)**
Online Games & Virtual Worlds **(http://www.enisa.europa.eu/act/it/oar/massively-multiplayer-online-games-and-social-and-corporate-virtual-worlds/security-and-privacy-in-virtual-worlds-and-gaming)**

PAGE 10

Cloud Computing Information Assurance Framework **(http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework/?searchterm=cloud*)**
Cloud Computing – SME Survey **(http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-sme-survey/?searchterm=cloud*)**

PAGE 11

EISAS – European Information Sharing & Alert System, A Feasibility Study **(http://www.enisa.europa.eu/act/cert/other-work/files/EISAS_finalreport.pdf/view?searchterm=eisas)**

PAGE 12

A Step-By-Step Approach on How to Set Up a CSIRT **(http://www.enisa.europa.eu/act/cert/support/guide)**
A Basic Collection of Good Practices for Running a CSIRT **(http://www.enisa.europa.eu/act/cert/support/guide2/files/a-collection-of-good-practice-for-cert-quality-assurance)**
CERT Exercises Handbook **(http://www.enisa.europa.eu/act/cert/support/exercise)**
Baseline Capabilities For National/Governmental CERTs **(http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-for-national-governmental-certs)**

PAGE 13

Stock Taking of Policies & Regulations **(http://www.enisa.europa.eu/act/res/policies/stock-taking-of-national-policies/stock-taking-report)**
Analysis of Member States Policies and Regulations **(http://www.enisa.europa.eu/act/res/policies/analysis-of-national-policies/analysis-of-policies-and-recommendations)**
Good Practice Documents **(http://www.enisa.europa.eu/act/res/policies/good-practices-1)**
Network Provider Measures **(http://www.enisa.europa.eu/act/res/providers-measures/files/network-provider-measures)**
Resilience Features of Technologies **(http://www.enisa.europa.eu/act/res/technologies/tech/resilience-features-of-technologies)**
Study on the Costs of DNSSEC Deployment **(http://www.enisa.europa.eu/act/res/technologies/tech/dnsseccosts)**

PAGE14

Privacy Features of European eID Card Specifications **(http://www.enisa.europa.eu/act/it/eid/pet/?searchterm=privacy)**
Technology Induced Challenges in Privacy & Data Protection in Europe
(http://www.enisa.europa.eu/act/rm/files/deliverables/technology-induced-challenges-in-privacy-data-protection-in-europe)

PAGE 15

Reporting Security Incidents – Good Practices **(http://www.enisa.europa.eu/act/res/policies/good-practices-1/incident-reporting-mechanisms/reporting-security-incidents-good-practices)**

PAGE 17

Botnets – The Silent Threat **(http://www.enisa.europa.eu/act/res/other-areas/botnets/botnets-2013-the-silent-threat)**

PAGE 18

Publications of ENISA in the Field of AR – An Overview **(http://www.enisa.europa.eu/act/ar/deliverables/overview)**
Information Security Tips for Employees **(http://www.enisa.europa.eu/act/ar/deliverables/2010/informationsecuritytips-employees)**
Information Security Tips For Parents & Guardians **(http://www.enisa.europa.eu/act/ar/deliverables/2010/internetsafetytips-parents)**
Guidelines For Parents, Guardians & Educators on Child Online Protection
(http://www.enisa.europa.eu/act/ar/deliverables/2009/cop_initiative)

enisa

European Network
and Information
Security Agency

PO Box 1309   71001 Heraklion   Greece
Tel: +30 2810 391 280   Fax: +30 2810 391 410
Email: info@enisa.europa.eu
www.enisa.europa.eu