Portugal Country Report

enisa
European Network and Information Security Agency

www.enisa.europa.eu

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details

For contacting ENISA or for general enquiries on the Country Reports:

Mr. Giorgos Dimitriou

ENISA External Relations Expert

Giorgos.Dimitriou@enisa.europa.eu

Internet: http://www.enisa.europa.eu

Acknowledgments:

ENISA would like to express its gratitude to the National Liaison Officers that provided input to the individual country reports. Our appreciation is also extended to the ENISA experts and Steering Committee members who contributed throughout this activity.

ENISA would also like to recognise the contribution of the Deloitte team members that prepared this country report on behalf of ENISA: **Marcelo Piccoli, Dan Cimpean, Johan Meire and Vincent Bouckaert**.

Legal notice

Table of Contents

PORTUGAL **4**
THE STRUCTURE OF THE INDIVIDUAL COUNTRY REPORTS 4
NIS NATIONAL STRATEGY, REGULATORY FRAMEWORK AND KEY POLICY MEASURES **5**
OVERVIEW OF THE NIS NATIONAL STRATEGY 5
THE REGULATORY FRAMEWORK 7
NIS GOVERNANCE **10**
OVERVIEW OF THE KEY STAKEHOLDERS 10
INTERACTION BETWEEN KEY STAKEHOLDERS, INFORMATION EXCHANGE MECHANISMS IN PLACE, CO-OPERATION & DIALOGUE PLATFORMS AROUND NIS 11
FOSTERING A PROACTIVE NIS COMMUNITY 12
COUNTRY-SPECIFIC NIS FACTS, TRENDS, GOOD PRACTICES AND INSPIRING CASES **13**
SECURITY INCIDENT MANAGEMENT 13
EMERGING NIS RISKS 13
RESILIENCE ASPECTS 13
PRIVACY AND TRUST 14
NIS AWARENESS AT THE COUNTRY LEVEL 16
RELEVANT STATISTICS FOR THE COUNTRY **18**
INTERNET ACCESS OF POPULATION AND ENTERPRISES 18
STATISTICS ON USE OF INTERNET BY INDIVIDUALS AND RELATED SECURITY ASPECTS 19
STATISTICS ON USE OF INTERNET BY INDIVIDUALS AND RELATED SECURITY ASPECTS 20
OTHER STATISTICS 21
APPENDIX **22**
NATIONAL AUTHORITIES IN NETWORK AND INFORMATION SECURITY 22
COMPUTER EMERGENCY RESPONSE TEAMS (CERTS) 22
INDUSTRY ORGANIZATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY 24
ACADEMIC ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY BODIES 24
OTHER BODIES AND ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY 24
REFERENCES 25

Portugal

The structure of the individual country reports

The individual country reports (i.e. country-specific) present the information by following a structure that is complementary to ENISA's "Who-is-who" publication and is intended to provide additional value-added to the reader:

- *NIS national strategy, regulatory framework and key policy measures*
- *Overview of the NIS governance model at country level:*
    - *Key stakeholders, their mandate, role and responsibilities, and an overview of their substantial activities in the area of NIS:*
    - *Interaction between key stakeholders, information exchange mechanisms in place, co-operation & dialogue platforms around NIS*
    - *Fostering a proactive NIS community*
- *Country specific NIS facts, trends, good practices and inspiring cases:*
    - *Security incident management*
    - *Emerging NIS risks*
    - *Resilience aspects*
    - *Privacy and trust*
    - *NIS awareness at the country level*
    - *Country-specific activities for identifying and promoting economically efficient approaches to information security*
    - *Interdependencies, interconnection and improving critical information infrastructure protection*
- *Relevant statistics for the country.*

This report is based on information which was publicly available when research was carried out, as well as comments received from National Liaison Officers and ENISA experts. As such, the country report presents a high-level snapshot of NIS at the turn of the year

NIS national strategy, regulatory framework and key policy measures

Overview of the NIS national strategy

Portugal finds itself in an initial phase of defining a National Information Security Policy. Currently no NIS-oriented risk management process is in place at a national level. However efforts can be noticed towards awareness and actions focusing on the development of a nationwide NIS strategy.

The coordination of the strategy for information security is the responsibility of UMIC (Portuguese acronym for Knowledge Society Agency). However this strategy is mostly aiming the public sector.

Regarding incident response capabilities, although Portugal does not have a formalized national CERT. CERT.PT acts as a de facto national CERT. CERT.PT is responsible for the network that serves universities and schools, the Internet domain .pt, the Portuguese Internet exchange point. Formal agreements have been settled between CERT.PT and major ISPs to build a cooperative environment and an information sharing platform regarding incident response, preventive measures and awareness raiding in general. The same kind of agreements are being established with Government agencies.

The information security strategy, including NIS awareness and incident response, are indirectly addressed by Portugal's Technological Plan, driven by Portugal's eGovernment. The plan is a wider effort to promote the development of the Portuguese Information Society and improve the country's competitiveness.

Presented publicly in November 2005, the plan is often referred to as the 'Technological Shock' and constitutes the central piece of the Government's economic policy. It consists in a series of articulated transversal measures aimed among other things at stimulating innovation by Portuguese companies, fostering research & development activities, improving education and training, and modernising the Public Administration.

The plan, which defines Portugal's main Information Society policy up to 2009, is comprised of the following three main axes:

- **Knowledge** - To qualify the Portuguese for the knowledge society, fostering structural measures which aim at enhancing the average qualification level of the population, implementing a broad and diversified lifelong learning system and mobilising the Portuguese for the Information Society.
- **Technology** - To overcome the scientific and technological gap, reinforcing public and private scientific and technological competences and recognising the role played by enterprises in the process of creation of qualified jobs and Research & Development (R&D) related activities.
- **Innovation** - To boost Innovation, helping the productive chain to be adapted to the challenges of Globalization by means of the diffusion and development of new procedures, organizational systems, services and goods.

Spread over the three main axes, the Technological Plan defines discrete measures to be implemented, many of which are directly related to e-Government.

Indicatively the following measures are mentioned:

Public administration

- Creation of the Citizen Card, which aggregates in one single document the Identification, the Social Security, the National Health Service, the taxpayer and the voter cards;
- Creation of the Portuguese Electronic Passport;
- Common Knowledge Network of the Public Administration;
- Creation of the Knowledge Network of the Public Libraries (digital Libraries);
- Application of an electronic invoice control system by the Public Administration;
- Developing a computer security policy.

Public services online

- Generalisation of the use and offer of Broadband Internet;
- Creation of the Universal Electronic Mailbox;
- Promotion of the Electronic Democracy;
- Digital Libraries;
- Creation of the Training and Employment Webportal.

Enterprises

- On the spot firm Initiative;
- Creation of a national services network operated through technological centres;
- Urban Networks for Competitiveness and Innovation;
- Intelligent highway infrastructure systems. 1

Action Plan for the Information Society

The Portuguese e-Government strategy[2] for the period 2003-2006 was exposed in the e-Government Action Plan presented in February 2003 and approved by the Government in June 2003. The e-Government Action Plan has been an integral part to the Action Plan for the Information Society, which is the main instrument for the strategic and operational coordination of Information Society policies in Portugal. The Action Plan for the Information Society comprised seven pillars:

- An Information Society for all;
- New capabilities;
- Quality and efficiency of public services;
- Better citizenship;
- Health for everyone;
- New ways of creating economic value;
- Attractive content.

[1] *See: http://www.epractice.eu/en/document/288342*
[2] *See : http://www.epractice.eu/en/document/288342*

The regulatory framework

The following Portuguese national regulations have relevance and applicability in the domain of network and information security:

e-Governance Legislation

There is currently no overall eGovernment legislation[3] in Portugal. However the **Resolution of Cabinet no. 137/2005**, of 17 August, provides for the adoption of the electronic billing system for the services and organisms of the Public Administration.

Data Protection/Privacy Legislation

Law on the State Electronic Certification

Law on the State Electronic Certification[4] (SCEE from the Portuguese acronym) was adopted on 16 June 2006. The Decree-Law no. 116-A/2006, aims to ensure the integration, unification and effectiveness of a strong authentication system for the electronic relationship between companies and individuals and the state and its public entities.

The SCEE architecture is that of a reliance hierarchy that ensures electronic security for the state and the digital authentication of electronic transactions among the public administration numerous services and entities, as well as between these and citizens and companies.

SCEE is independent from other public key infrastructures; however it allows interfaces with existing infrastructures that meet the necessary authenticity requirements and EU certification policies compliance.

The referred Decree-Law entitled the National Security Authority (ANS) as certifying body, previously delegated to the Justice Institute of Information Technology.

Law on permanent certificates of people's civil status

The Portuguese Justice Ministry issued on 10 March 2010 a decree (no 145/2010) establishing permanent certificates of people's civil status. The documents became accessible online as from 20 March 2010, via the 'Civil Online' website.

The permanent certificate of civil status means the availability in electronic format of the up-to-date information contained in one's birth records. It will thus save citizens the time and procedure of visiting the competent offices to obtain a paper-based certificate. The decree also specifies that the request for access to the permanent certificate shall be made through the 'Civil Online' website "by the citizens - of age or emancipated - to whom the records relate". The applying citizens must furthermore authenticate with their Citizen Card [Cartão de Cidadão, in Portuguese], Portugal's electronic identity certificate.

In line with the decree's provisions, the transmission by its holder of the access code to another entity will correspond to the legal delivery of a birth certificate to the latter.

---

[3] *See:* http://www.epractice.eu/files/eGovernment%20in%20PT%20-%20March%20-%202009%20-%2011.0.pdf

[4] *See:* http://www.epractice.eu/files/eGovernment%20in%20PT%20-%20March%20-%202009%20-%2011.0.pdf

Law on the Protection of Personal Data

Law on the Protection of Personal Data was adopted on 26 October 1998. Law 67/98 (Personal Data Protection Law - Lei de Protecção de Dados Pessoais) governs the collection and processing of personal data and allows any person to access and correct their personal information held by a public or private body. The law transposes the Directive 95/46/EC of the European Parliament and the Council, of 24th October 1995, dealing with the treatment and circulation of personal data and enforced by the National Data Protection Commission. It should also apply in cases where there is an unauthorised access to personal data.

Additional Laws on the Protection of Personal Data

Portugal has transposed Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 in two different laws: Decree-Law n.º 7/2004 of 7 January 2004 (the e-Commerce Law - Lei do Comércio Electrónico) and Law no. 41/2004, of 18 August 2004. Under these acts, Portugal adopted a provision imposing data retention obligations on operators and service providers of electronic communication (Law no. 41/2004, of 18 Portuguese police is divided into several police entities. The police has police stations all over Portugal. All stations are competent to receive a criminal complaint. However, the Judicial Police (Policia Judiciaria) is the entity mostly specialised in these areas of crime, in particular its Central Investigations Section for IT and Telecommunications.

Cybercrime legislation

The Portuguese President has approved on 15 September 2009 the Cybercrime Law no 109/2009[5]. It transposed Directive 2005/222/JAI of the European Council of 24 February 2009, referring to attacks against information systems, and adapted the internal law to the European Council Cybercrime Convention.

The President has also decreed, in line with article 135 of the Portuguese Constitution, that the additional protocol to Cybercrime related to racist and xenophobic actions performed through information systems adopted in Strasburg in 28 January 2003 was approved by Republic Assembly Resolution no 91/2009 of 10 July 2009.

Portugal has a long tradition in the enactment of computer crime protection. In fact, Portugal has had a legal framework to be applied to criminal actions involving computers since 1991 (Law 109/91, of 17 August 1991) (Computer Crime Law – Lei da Criminalidade Informática).

The referred act follows the minimal list of Recommendation (89)9 of the European Council. In 1998, a new computer crime was added: computer-related fraud. As the scope of protection is mainly the property, the Portuguese legislator considered that this crime should be included in the Criminal Code (and not in the Law 109/91), which leads to an unjustifiable lapse: in this case, companies will not be subject criminal liability (which happens in the event of condemnations under the Computer Crime Law).

Crime (Seccao Central de Investigacao de Criminalidade Informatica e Telecomunicacoes - SCICIT). This section is based in Lisbon, and its agents cover the Portuguese territory, with the cooperation if necessary of unspecified police forces. It assists the prosecutor's department, providing technical and logistics support, and also aiding in obtaining evidence.

[5] http://www.rand.org/pubs/technical_reports/2006/RAND_TR337.pdf

The Secção de Investigação de Criminalidade Informática e Telecomunicações (SCICIT) should be alerted in all cases of computer crime, where the victim is considering to file a complaint.

Self-regulations

Self-regulatory Code of Conduct for activities involving the provision of content services

The Portuguese mobile telecom operators have adopted a code of conduct that describes duties of the signatory members in ensuring minimum protective measures for safer use of the content provided on the mobile phone. The code has been tailored to the needs of the Portuguese mobile electronic telecommunications market and complies with applicable European and national legislation.

eIdentity

General overview

Portugal is in the process of deploying an electronic ID card for its citizens over the age of 6, as well as for Brazilian citizens covered by the Treaty of Porto Seguro.

A central database containing the attributes of the e-ID card holders is used as an authentic source. The authentication certificate contained in the national e-ID card is issued through a PKI based system and relies on two different CA for its creation. Both Certificate Revocation Lists (CRLs) and the Online Certificate Status Protocol (OCSP) can be used for validation/management of the certificates' lifecycles. Other systems are also available and rely on PKI systems (e.g. for law profession orders – lawyers, solicitors and notaries) or single factor authentication (for the Citizen's Portal and for a variety of tax/social security systems).

A specific middleware is being developed for the Portuguese government and will constitute the application level interface for e-Government applications that use cryptographic operations from the smart card and PKI services.

E-Signatures Legislation

The Decree-Law on Electronic Signatures no. 62, of 3 April 2003, aims to align the legal regime for digital signatures established in a previous Decree-Law (Decree-Law no. 290-D/99, of 2 August 1999) to Directive 1999/93/EC of the European Parliament and the Council of 13 December 1999, on a Community framework for electronic signatures. The Decree-Law no. 165/2004, of 6 July and the Regulatory Decree no. 25/2004, of 15 July constitute further legislation in this area**.**

NIS Governance

Overview of the key stakeholders

We included below a high-level overview of the key actors with relevant involvement, roles and responsibilities in NIS matters.

National Authorities	• ICP-Anacom • UMIC (Knowledge Society Agency) • Comissão Nacional de Protecção de Dados (CNPD) – National Data Protection Commission
CERTs	• CERT-IPN - Computer Security Incident Response Team integrated in the Computer Science Laboratory • CERT.PT - the Portuguese CERT • CSIRT.FEUP - Computer Security Incident Response Team for University of Porto
Industry Organisations	• ANETIE (Associacao Nacional das Empresas das Tecnologias de Informacao e Electronica) • APRITEL (Associacao dos Operadores de Telecomunicacoes)
Academic Organisations	• Fundação para a Computação Científica Nacional (FCCN) - Foundation for National Scientific Computation
Others	• Instituto Portugues da Qualidade (IPQ) • DECO (Associacao Portuguesa para a Defesa do Consumidor)

For contact details of the above-indicated stakeholders we refer to the ENISA "Who is Who"[6] – 2010 Directory on Network and Information Security and for the CERTs we refer to the ENISA CERT Inventory[7].

NOTE: only activities with at least a component of the following eight ENISA focus points have been taken into account when the stakeholders and their interaction were highlighted: CERT, Resilience, Awareness Raising, Emerging Risks/Current Risks, Micro-enterprises, e-ID, Development of Security, Technology and Standards Policy; Implementation of Security, Technology and Standards.

[6] *The ENISA Who-is-Who Directory on Network and Information Security (NIS) contains information on NIS stakeholders (such as national and European authorities and NIS organisations), contact details, websites, and areas of responsibilities or activities. Ref. code: ISBN 978-92-9204-003-1 - Publication date: May 12, 2010*

[7] *http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country/*

Interaction between key stakeholders, information exchange mechanisms in place, co-operation & dialogue platforms around NIS

Information exchange managed via ICP-ANACOM

Overall, information exchange mechanisms are not yet very mature in Portugal. A key driver for the information exchange is the **National Authority for Communications** (**ICP-ANACOM** as an acronym from the Portuguese title). There is limited exchange of information between providers and it appears that the initiative for standing committees that will institutionalize exchange and collaboration will have to come from ANACOM. ICP-ANACOM's website features a thematic area dedicated to Information Systems and Networks Security. However ANACOM is still trying to work/verify, and measure how the operators have worked to address general security issues and how to collect related information.

Other co-operation of NIS stakeholders to combat spam and malware

Cooperation between governmental bodies: no information is available that a formal, institutional and systematic cooperation has been implemented between the competent authorities. A first approach has been taken by the national telecom regulator and the DPA, who organise meetings to analyse future actions, together with the foundation for national scientific computation. This project is still in an early stage but it is expected to lead in the future to a cooperation protocol.

Cooperation between government and industry[8]: CERT.PT is starting a program with ISPs in order to cooperate within the scope of reported illegal activities. This may constitute a first step for a new approach of ISPs in order to adopt preventive measures against malpractices of their clients, in particular in relation to spam.

CERT.PT has formal agreements with major ISPs establishing a cooperation environment and an information sharing platform.

Cooperation at international level: The national telecom regulator participates in the CNSA, the LAP and the OECD on behalf of Portugal. Additionally, the foundation for national scientific computation always attends the ICANN's worldwide meetings to ensure the exchange of information and cooperation on spam.

[8] *See* *http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/spam_spyware_legal_study2009final.pdf*

Fostering a proactive NIS community

As from the end of February 2010, several **Portuguese and Spanish** eGovernment services will be interconnected, thus allowing any citizen of one of the two countries to access and use the services of the other country. This development has been made possible under the framework of a collaboration agreement concerning the validation of their respective electronic identity certificates, which Portugal and Spain signed in September 2009.

Under the first stage of the collaboration, the Portuguese businesses operating in the field of civil construction in Spain will be able to register their workers with the Spanish Ministry of Employment and Immigration online, using a citizen card [Cartão do Cidadão in Portuguese]. Likewise, the Spanish citizens will have the possibility to set up a company online through the Portuguese Enterprise's Portal after identifying with their national eID card [DNI electrónico in Spanish].

The initiative was presented on 2 February 2010 at the Presidency of the Council of Ministers in Lisbon, in the presence of the Portuguese Secretary of State for Administrative Modernisation, Maria Manuel Leitão Marques, and the Spanish State Secretary for the Public Service, Carmen Gomis Bernal.

Country-specific NIS facts, trends, good practices and inspiring cases

Security incident management

In Portugal, ISPs are not obliged to report security incidents. For the general public, every operator has an abuse e-mail or web form to report specific security incident information. For the CSIRT environment there are specific PoC and incidents are handled in the context of the national CSIRT network in coordination with CERT.PT. Incident statistics and trends are being gathered within this network.

The Secção de Investigação de Criminalidade Informática e Telecomunicações (SCICIT) should be alerted in all cases of computer crime, where the victim is considering to file a complaint.

Emerging NIS risks

No consolidated list of emerging NIS risks that are officially considered by the Portuguese authorities has been identified.

Resilience aspects

Compared with 2010, no major changes have been implemented regarding Portugal's resilience aspects. Portugal faces a May 2011 deadline set by the EU in order to establish detailed network resilience related legislation. The current network resilience related legislation is still expressed in general terms, which makes enforcement problematic – as such, the key responsibility on network resilience stays with the telecom operators that manage the respective networks.

ICP-ANACOM's CSO was established in March 2007. Presently CSO staff is composed of two engineers, one economist and the head of the office. Currently, it conducts various studies and interviews with stakeholders to allow it to take an inventory regarding e-communication networks' resilience. Regulation of resilience and security was recognized by ICP-ANACOM's Board as an issue last year resulting in the establishment of ANACOM CSO.

In its review of the regulatory framework, the EU published a set of proposals for the regulatory framework for eCommunications in November 2007. ICP-ANACOM organised three workshops during January 2008. The objective was to raise awareness and promote a public debate regarding the proposals presented by the European Commission with respect to this review and to cooperate in defining the position of ANACOM in this respect. Beyond these activities there is no additional legislation in the works. ICP-ANACOM has launched several studies that are the beginning of its activities to provide additional guidance and regulation if needed. The studies will allow ICP-ANACOM to conduct a systematic inventory on what are the issues, what are the problems and potential risks and where do operators, users and other stakeholders see a need for improvement.

Studies will be the starting point for determining if there are further guidelines to be developed based on these data and analyses thereof. ICP-ANACOM expects first results around the end of 2008 – 2009.

As regards to future strategies, the existing research projects and findings thereof will provide the basis for developing a strategy for security of public communication networks (resilience). Responding to the above survey during data collection period is a mixture between voluntary,

required and so on. Some people do it voluntarily. Voluntary participation is most effective because it generally occurs when stakeholders have come to the conclusion that participation will be beneficial. Step 8 will contain suggestions for possible regulatory changes or the development of new guidelines. Such changes, if approved by the Government, will then have to be implemented.

ICP-ANACOM does not yet conduct audits pertaining specifically to network dependability and reliability / resilience issues regarding public e-communication networks. Because there is no specific regulation pertaining to resilience, there is no legal foundation for conducting a formalized audit. Neither do we have a regulatory basis to demand an operator response when finding shortcomings through an audit. In turn, we could not demand remedial work to rectify the problem be taken within a certain timeframe and following a specific procedure.

Privacy and trust

Status of implementation of the Data Protection Directive

Directive 95/46 has been implemented by the Portughese Law 67/98 of 26 October on personal data protection (the "DPA"). The competent national regulatory authority on this matter is the Comissão Nacional de Protecção de Dados (the "CNPD").

Personal Data and Sensitive Personal Data

The definition of personal data in the DPA is similar to the standard definition of personal data. In particular, it should be noted that the DPA only applies to individuals as opposed to legal entities.

Under the DPA, sensitive personal data means data on philosophical or political beliefs, political party or trade union membership, religion, privacy and racial or ethnic origin, and concerning health or sex life, including genetic data. Therefore, the concept of sensitive personal data under the DPA is largely similar to the standard types of sensitive personal data but also includes genetic data and data on the private life of the data subject.

Information about illegal activities and offences is also subject to additional restrictions.

The processing of sensitive personal data is permitted if it: (i) is necessary to protect the vital interests of the data subject or of another person; (ii) is carried out with the data subject's consent by a non-profit seeking body; (iii) relates to data made public by the data subject; (iv) is necessary for the establishment, exercise or defence of legal claims; (v) relates to health and sex life, including genetic data, and is necessary for medical reasons.

The authorisation of the CNPD is needed in any other case (including where processing is based on the consent of the data subject). Authorisation will only be awarded: (i) when such processing is essential for exercising the legal or statutory rights of the data controller; or (ii) when the data subject has given his/her explicit consent for such processing.

The processing of personal data relating to illegal activities or offences is also subject to prior authorisation. Furthermore, central registers relating to persons suspected of illegal activities or found guilty of offences, may only be created and kept by public authorities vested with that specific responsibility.

Information Security aspects in the local implementation of the Data Protection Directive

The data controller must comply with the general data security obligations. A data controller who processes sensitive personal data under an authorisation of the CNPD or who processes personal data relating to illegal activities or offences must take additional measures. These additional measures require the data controller to:

(i) prevent unauthorised access to the premises used for processing such data;

(ii) prevent data media from being read, copied, altered or removed by unauthorised persons;

(iii) prevent unauthorised input and or control over inputs;

(iv) prevent unauthorised use of processing equipment;

(v) prevent unauthorised access to data;

(vi) confirm the details of the persons to who the data is transmitted;

(vii) keep an audit trail of all inputs;

(viii) protect information while it is being transmitted (which at the CNPD's direction may include encryption).

Furthermore, the systems used must guarantee the logical separation between data relating to health and sex life, including genetic data, and other personal data.

Data protection breaches

The Portughese DPA does not contain any obligation to inform the CNPD or the data subjects of a security breach.

Enforcement

The CNPD has the power to investigate data controllers, including by carrying out dawn raids. Following an investigation it can apply fines. Data controllers can appeal against those fines to the courts.

NIS awareness at the country level

In Portugal, NIS awareness raising measures are undertaken by both competent authorities as well as by private companies, academic bodies and NGOs.

Like in almost all EU Member States, Portugal has several informative website and one or more complaint channel to present NIS awareness actions. Most of these websites are related to spam and/or malware, including advice on how to best protect against them.

Last year's ARECI study gave the country the opportunity to discuss with various stakeholders the issues pertaining to resilience of public e-communication networks. Information included from Portugal in the final report of the study included input from operators and infrastructure owners. The public concession was a Public-Private Partnership (PPP) in its beginning. The concession does encompass security-related matters that the operator must take care off. Working groups exist on security planning. They meet regularly; an example is the working group for civil defense. One goal of the working groups is to come up with requirements for network security issues.

Security awareness aspects are also, in general, published on the web sites of the Portuguese banks and they cover aspects related to basis information security aspects relevant for public: antivirus software, firewalls, security updates, use of passwords, rules concerning providing personal or confidential/ sensitive information by electronic mail or by any other means, etc.

Awareness initiatives

A number of initiatives have been undertaken in Portugal with regards to awareness on web security, namely "Internet Segura[9]", "Linha Alerta[10]" and "Segurannet[11]".

Internet Segura (meaning "Safe Internet") is a consortium of entities combined in a project for awareness on web security. It was created within the scope of the European 'Safer Internet plus' programme and has the following four main strategic goals:

- Fight against illegal content;
- Minimise the impact of illegal and harmful content on citizens;
- Promote safe Internet usage;
- Raise awareness about the risks of using the Internet.

The Internet Segura consortium consists of the following members: UMIC (National Agency for the Knowledge Society); Ministry of Education; FCCN (Foundation for National Scientific Computing); Microsoft Portugal.

Linha Alerta[12] is part of Internet Segura and was co-funded until December 2008 by the European Commission under the 'Safer Internet plus' programme.

The hotline service is managed by FCCN within its security services group CERT.PT.

Seguranet's[13] main goal is to promote Internet use that is clarified, critical and secure among parents, teachers, children and youngsters. This portal is part of the consortium 'Internet Segura'.

---

[9] See: http://www.internetsegura.net/
[10] See: http://linhaalerta.internetsegura.pt/index.php?lang=en
[11] See: http://nonio.fc.ul.pt/recursos/pesq_seg_net/segurannet.htm
[12] See: http://linhaalerta.Internetsegura.pt
[13] See: http://www.seguranet.pt

Awareness measures to combat spam and/or malware

Measures have been undertaken in Portugal by competent national authorities[14]. However Portugal can be a seen as a state where no comprehensive information about measures against online malpractices is available.

The laws do not provide a clear understanding about the leading role of the regulators and there is no clear and concise rule on anti-spam actions. It seems plausible that the telecom regulator may act regarding spam and spyware on corporate bodies, the national DPA on spam and spyware regarding individuals and the police computer crime unit on malicious software.

The lack of clarity and coherency of the Portuguese legal framework leads to uncertainty on the competences to act against online malpractices. In fact, it may be acceptable that different authorities may act against quite similar situations, without a feasible explanation. This may be the major explanation for the absence of comprehensive actions by regulators. Apparently, the national DPA imposed some fines.

Nothing indicates that competent authorities on this matter are cooperating on the implementation of coordinated public rules. On the other side, it seems that ISPs are willing to take more proactive approaches against online malpractices. Currently, most of them already provide anti-spam filters and about half of them offer anti-virus software.

Administrative decisions – Both the telecom regulator and the national DPA can impose fines. In practice, only the DPA is said to have imposed fines so far.

Judicial decisions – There is no track record of judicial sanctions on spam and, notwithstanding the number of processes in the inquiry phase, no references have been found regarding the last two years.

Awareness measures – The national telecom regulator is expected to provide more educational information to web users on its website, including the response to a 2008 query on spam.

Complaint channels – Via the website of the national telecom regulator, communications users and subscribers can upload their complaints against unsolicited communications and other malpractices on electronic communications. Complaints are also possible via email, fax, mail or directly. Criminal complaints can also be filed on the website of the police but apparently this function has never been used by citizens.

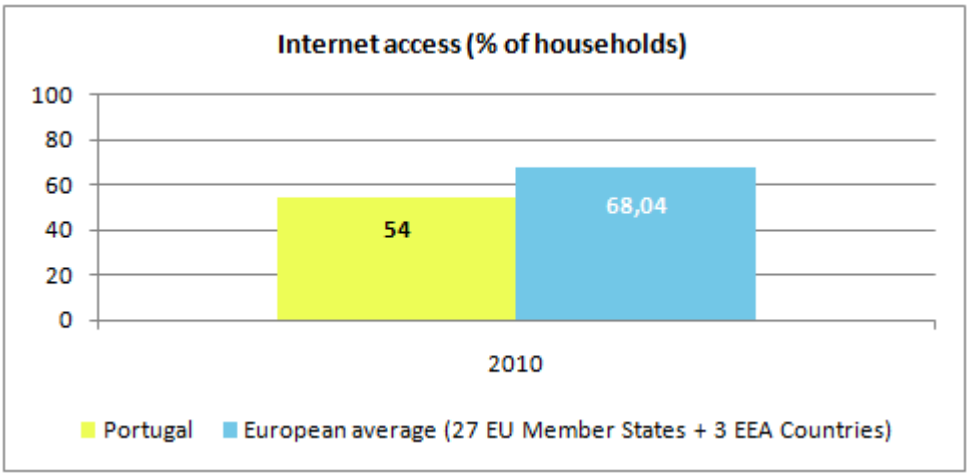
[14] *See:* *http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/spam_spyware_legal_study2009final.pdf*

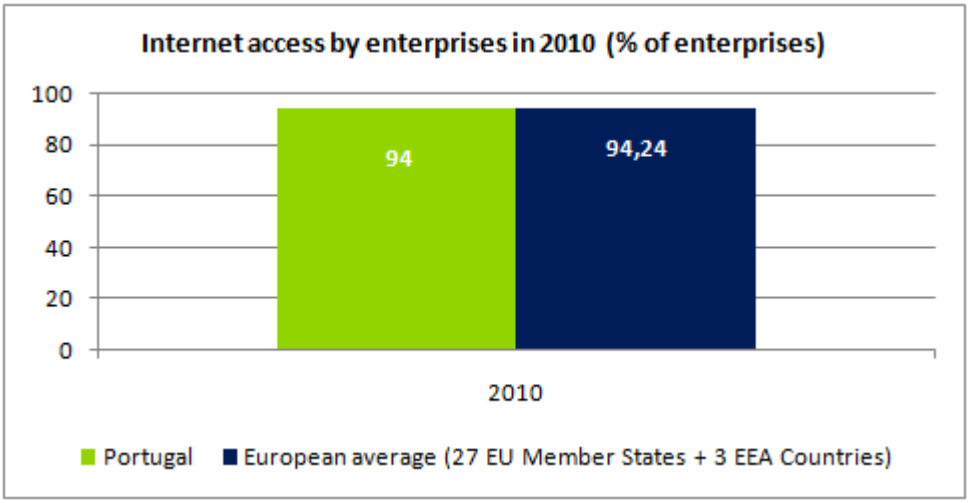
Relevant statistics for the country

In order to provide the reader with additional information about the relative stage of NIS development in Portugal, a series of relevant statistics are included in this section. Some of them indicate that this country still needs improvement to be made while others show progress and interesting trends.

Internet access of population and enterprises

The following graphs provide an overview of the situation[15] of Internet access in Portugal for enterprises and respectively households, relative to the European average.



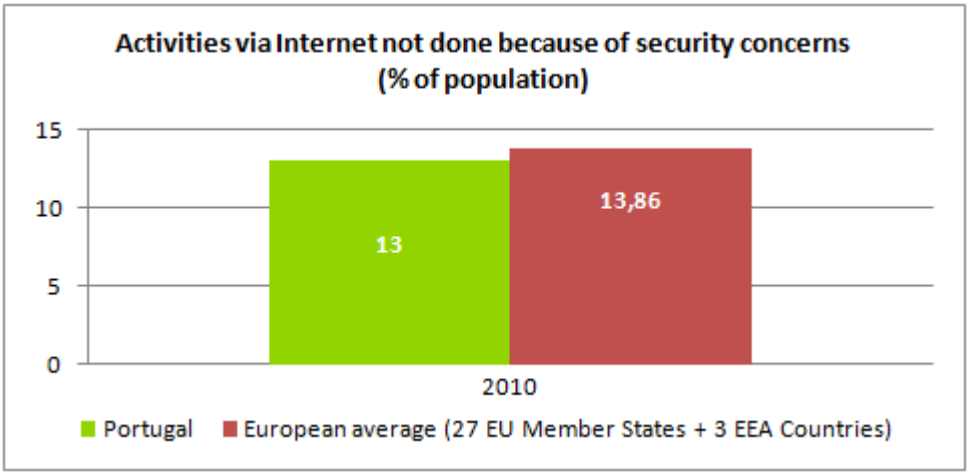


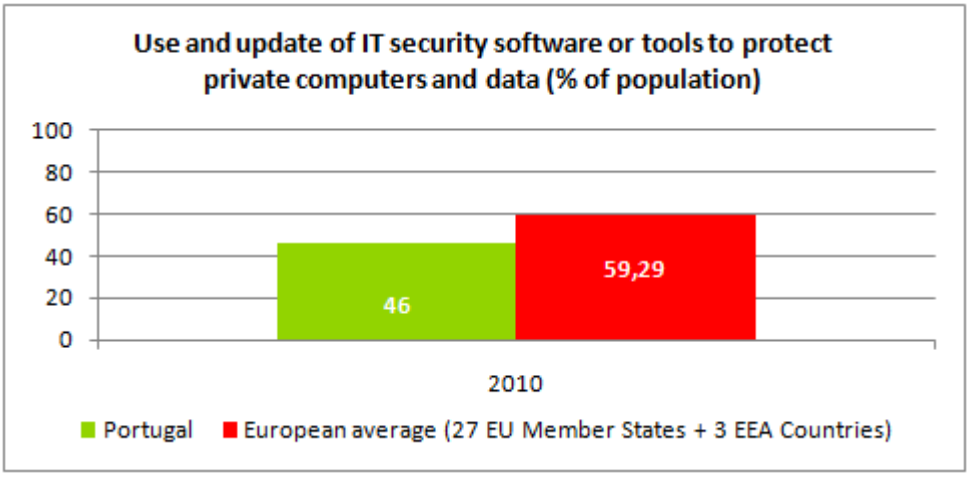
In 2010, the statistics indicate that the enterprises in Portugal have the same level of Internet access as the European average, while efforts are needed to narrow the gap on households.

[15] *Source: Eurostat*

Statistics on use of Internet by individuals and related security aspects

The percentage of population in Portugal that is reluctant in performing activities via Internet (e.g. e-banking, purchases of goods and services over Internet, etc.) because of security concerns is slightly below the European average:

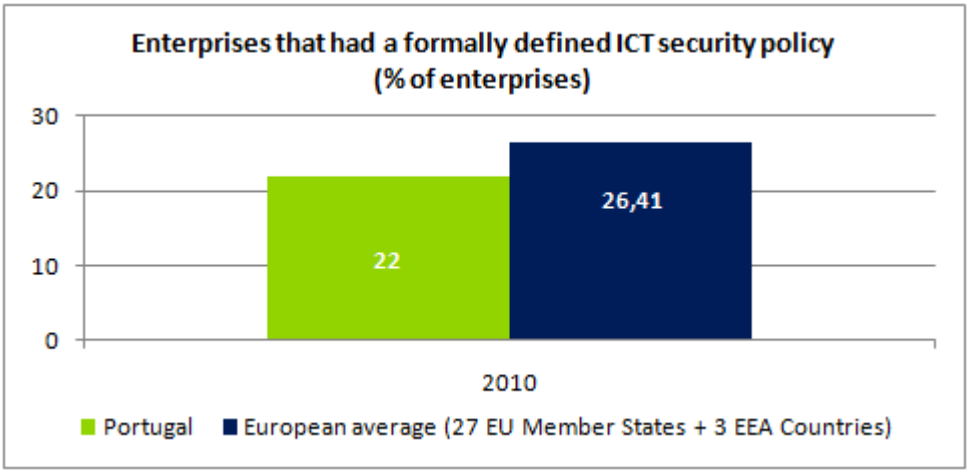




It also appears that the use of security tools to protect private computers and data is below the European average.

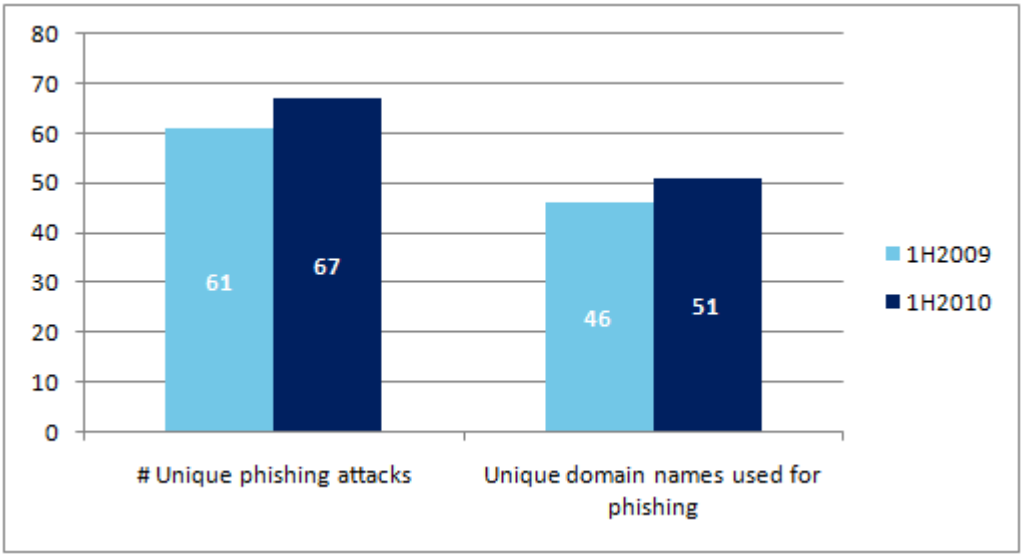
Statistics on use of Internet by individuals and related security aspects

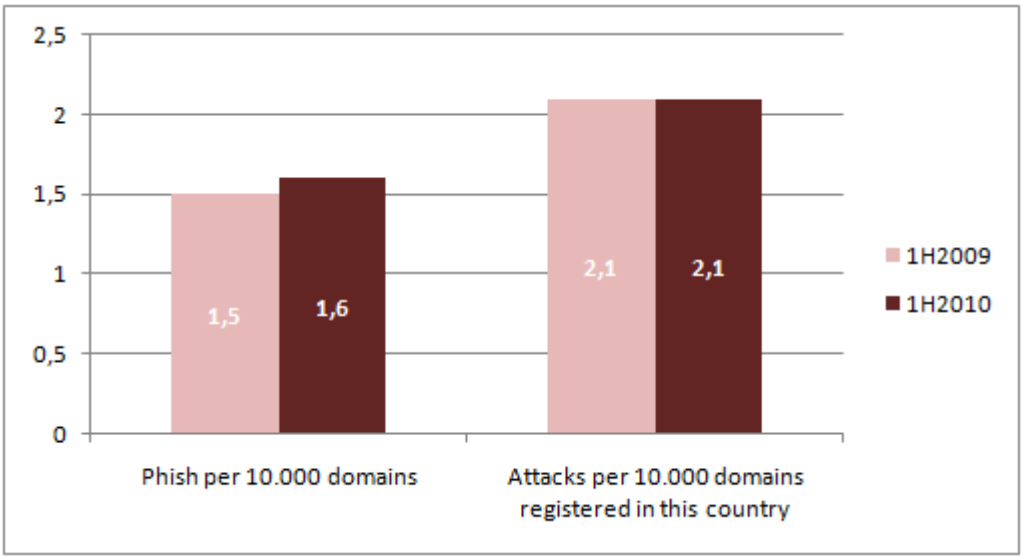
Fewer enterprises in Portugal have a formally defined ICT security policy, compared with their European peers. See below:



Other Statistics

It is interesting to also mention that during the 1st half of 2010, and respectively for the 1st half of 2009, Portugal was mentioned in the global report[16] published by the Anti-Phishing Working Group (APWG) with the following relevant statistics:





[16] *See: Global Phishing Survey: Trends and Domain Name Use 1H2010, available at: http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_1H2010.pdf*

APPENDIX

National authorities in network and information security

National authorities	Role and responsibilities	Website
1. ICP-Anacom	The National Communications Agency (ANACOM) is the regulator, supervisor and representative of the communications sector in Portugal. The authority is responsible for ensuring compliance with the Electronic Communications Law.	www.anacom.pt
2. UMIC (Knowledge Society Agency)	Portuguese public agency with the mission of coordinating the policies for the information society and its mobilisation through the promotion of dissemination, qualification and research activities. Among other tasks, it is in charge of promoting security and privacy in the use of the Internet and ICT.	www.umic.pt
3. Comissão Nacional de Protecção de Dados (CNPD) – National Data Protection Commission	The National Data Protection Commission (CNPD) is an independent body, with the power to supervise and monitor compliance with the laws and regulations in the area of personal data protection.	www.cnpd.pt

Computer Emergency Response Teams (CERTs)

CERT	Role and responsibilities • FIRST[17] member • TI[18] listed	Website
4. CERT.PT	CERT.PT is the Portuguese CERT. CERT.PT has a mandate to support the Portuguese society in working with protection against IT incidents and be the central report and coordination point for relevant security incidents for the government. CERT.PT's priorities include: offering technical support to computer users in resolving security incidents, advising on best-practices, analysing artefacts, and coordinating actions with the parties involved; gather and disseminate a set of information about vulnerabilities and recommendations, pertaining to potential security risks and ongoing malicious activities; gather from accredited sources information related to security vulnerabilities, and act on the community with the goal of minimizing impact at the National level; and, promote the creation of new CERT/CSIRTs in Portugal, and raise awareness of security issues on computer users. CERT.PT coordinates the Portuguese CSIRT network. CERT.PT is: • Not FIRST member; • TI listed.	www.cert.pt
5. CSIRT.FEUP	CSIRT.FEUP (Servico de Resposta a Incidentes de Seguranca Informatica da Universidade Porto) is the Computer Security Incident Response Team (CSIRT) for University of Porto. The scope of CSIRT.FEUP is the ssers of systems connected to the network of the —Faculdade de Engenharia da Universidade do Portoǁ (University of Porto),	http://csirt.fe.up.pt

[17] *www.first.org/members/teams/*
[18] *www.trusted-introducer.nl/*

CERT	Role and responsibilities • FIRST[17] member • TI[18] listed	Website
	users of systems inside the fe.up.pt namespace. It is a member of the Portuguese National CSIRT Network. CSIRT.FEUP is: • Not FIRST member; • TI listed.	
6. SONAECOM	SONAECOM is the sub-holding of the Sonae group for the telecommunications, media and information systems software areas. It is a member of the Portuguese National CSIRT Network since January 2008 and it aims to support the integrated management of business entities in the telecommunications, media and information systems software areas. SONAECOM is: • Not FIRST member; • TI listed.	www.sonae.com
7. Cabovisao	Cabovisao is a telecommunications service provider that became a member of the Portuguese National CSIRT Network in March 2008. Among its services, it provides VPN and Domain Name registration. Cabovisao is: • Not FIRST member; • TI listed.	www.cabovisao.pt
8. CC-CRISI (EMGFA)	CC-CRISI (EMGFA) is the CSIRT for the Portuguese Armed Forces. It is a member of the Portuguese National CSIRT Network since November 2008. CC-CRISI (EMGFA) is: • Not FIRST member; • TI listed.	www.emgfa.pt
9. Portugal Telecom	Portugal Telecom is a large telecommunications service provider in Portugal which actively engages in Cyber security education. It interacts with Portuguese and international academic organizations for that matter. It is a member of the Portuguese National CSIRT Network since March 2009. Portugal Telecom is: • Not FIRST member; • TI listed.	www.telecom.pt
10. Claranet	Claranet is an ICT integrated services provider in Portugal which provides its clients with the implementation of preventive IT security measures as well as incident response and support to legal actions arising from security incidents. It is a member of the Portuguese National CSIRT Network since March 2009. Claranet is • Not FIRST member; • TI listed.	www.claranet.pt
11. ONI Communications	ONI communications is an ICT integrated services provider in Portugal which provides its clients with IT Security services among others. It is a member of the Portuguese National CSIRT Network since March 2010. ONI Communications is TI listed.	www.oni.pt
12. Refertelecom	Refertelecom is a telecommunications service provider that became a member of the Portuguese National CSIRT Network in March 2010. Refertelecom is • Not FIRST member; • TI listed.	www.refertelecom.pt
13. Milennium BCP	Millenium BCP is a bank that became a member of the Portuguese National CSIRT Network in September 2010. Milennium BCP is: • Not FIRST member; • TI listed.	www.milleniumbcp.pt

Industry organizations active in network and information security

Industry Organisations	Role and responsibilities	Website
14. ANETIE (Associacao Nacional das Empresas das Tecnologias de Informacao e Electronica)	ANETIE is Portugal's information technologies and electronics association which was created with the goal of promoting sustained growth of the IT sector. ANETIE brings together today most of the national companies active in the electronics, software, communication and information industries. Membership includes the most important companies connected with IT and electronics that develop locally, produce and/or sale products or services.	www.anetie.pt www.PortugalHighTech.com
15. APRITEL (Associacao dos Operadores de Telecomunicacoes)	APRITEL is the association of the electronic telecommunication companies operating in Portugal. Its responsibilities include to promote a legal and regulatory environment supporting investment in the industry of electronic communications and to contribute to the development of the information society including: • healthy competition; • industry's sustained development; • the competitive and economic development of the country; • the well being of consumers.	www.apritel.org
16. APB (Associacao Portuguesa de Bancos)	APB is the main entity that represents the Portuguese banking sector. It has created a working group focused on IT security and resilience .	www.apb.pt

Academic organisations active in network and information security bodies

Academic Organisations	Role and responsibilities	Website
17. Fundação para a Computação Científica Nacional (FCCN) - Foundation for National Scientific Computation	The Foundation for National Scientific Computation (FCNN) runs the research and education network and CERT.PT.	www.fccn.pt
18. Carnegie Mellon Portugal	The Carnegie Mellon Portugal is a Portuguese research program co-lead along with the Carnegie Mellon University which aims to create new knowledge in key ICT areas with focus in network and information security with a close connection with the Portuguese industry.	www.cmuportugal.org
19. PT Security Lab	The PT Security Lab is an IT Security initiative led by Portugal Telecom in connection with Carnegie Mellon Portugal. It functions as both a sponsor for CMUPortugal as an intermediate between CMU, Portuguese Universities and the telecommunication industry in Portugal.	www.telecom.pt/InternetResource/PTSite/PT/Canais/SobreaPT/Seguranca/PTSecurityLab/PTSECURITYLAB.htm

Other bodies and organisations active in network and information security

Others	Role and responsibilities	Website
20. Instituto Portugues	IPQ (standing for Portuguese Institute of Quality) is a non-lucrative association, a Portuguese private legal entity of public interest,	www.ipq.pt

da Qualidade (IPQ)	nongovernmental and apolitical, recognized as a national standards body by the Government Decision 142/2007. Main responsibilities: • To establish the principles and methodologies of the national standardization • To assure the public information in the field of standardization • To edit, publish and disseminate the standards and publications of standardization • To represent Portugal before the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC), the International Electrotechnical Commission (IEC), the Conference General des Poids et Mésures (CGPM), the International Organization for Legal Metrology (OIML), and the International Organization for Standardization (ISO).	
21. DECO (Associacao Portuguesa para a Defesa do Consumidor)	DECO is a consumer organisation, responsible for protecting and educating consumers in general.	www.deco.proteste.pt

References

- An overview of the eGovernment and eInclusion situation in Europe, available at http://www.epractice.eu/en/factsheets
- ENISA, Information security awareness in financial organisation, November 2008, available at http://www.enisa.europa.eu/doc/pdf/deliverables/is_awareness_financial_organisations.pdf
- Portugal - ENISA CERT Directory: http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country/portugal

enisa
European Network and Information Security Agency

PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280
www.enisa.europa.eu