Czech Republic Country Report
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, please use the following details: Mr. Jeremy Beale, ENISA Head of Unit - Stakeholder Relations, Jeremy.Beale@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 the Czech Republic Country Report on behalf of ENISA: Dan Cimpean, Johan Meire and Jan D’Herdt.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. 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 does not necessarily represent state-of-the-art and it 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. Member States are not responsible for the outcomes of the study.

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.

Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA), 2009-2010
# Table of Contents

**CZECH REPUBLIC** ...........................................................................................................................................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 .......................................................................................................................................6  
NIS GOVERNANCE ......................................................................................................................................................9  
  Overview of the key stakeholders ............................................................................................................................9  
  Interaction between key stakeholders, information exchange mechanisms in place, co-operation & dialogue platforms around NIS ......................................................................................................................10  
COUNTRY-SPECIFIC NIS FACTS, TRENDS, GOOD PRACTICES AND INSPIRING CASES ........................................13  
  Security incident management ..................................................................................................................................13  
  Emerging NIS risks ..................................................................................................................................................15  
  Resilience aspects ....................................................................................................................................................15  
  Privacy and trust .........................................................................................................................................................17  
  NIS awareness at the country level ............................................................................................................................18  
  Relevant statistics for the country ............................................................................................................................20  
APPENDIX ..................................................................................................................................................................22  
  National authorities in network and information security: role and responsibilities .............................................22  
  Computer Emergency Response Teams (CERTs): roles and responsibilities .......................................................24  
  Industry organisations active in network and information security: role and responsibilities ..........................25  
  Academic organisations active in network and information security: role and responsibilities ........................26  
  Other bodies and organisations active in network and information security: role and responsibilities ............26  
  Consumer organisations active in network and information security: role and responsibilities ....................27  
  Country specific NIS glossary .....................................................................................................................................28  
References ..................................................................................................................................................................28
Czech Republic

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:
    - National authorities
    - CERTs
    - Industry organisations and associations
    - Academic organisations
    - Other organisations active in NIS
  - Interaction between key stakeholders, information exchange mechanisms in place, co-operation & dialogue platforms around NIS
- **Country specific NIS facts, trends, good practices and inspiring cases.**

For more details on the general country information, we suggest the reader to consult the web site: [http://europa.eu/abc/european_countries/index_en.htm](http://europa.eu/abc/european_countries/index_en.htm)
NIS national strategy, regulatory framework and key policy measures

Overview of the NIS national strategy

The Czech Republic adopts and improves measures for the protection and sharing of information. In the technically and financially demanding fields of communication and information security, it intends to continue enhancing the protection of important information systems and critical infrastructures and to consistently suppress information crime. Great stress is currently placed on the very sensitive areas of intellectual property protection and personnel security.

National Strategy for Information Security of the Czech Republic

The National Strategy for Information Security (NSIS) of the Czech Republic creates a platform for building a credible and democratic information society based on a legal foundation, which takes care to secure information in all areas of peoples’ activities and enables information to be used and shared freely and securely.

The purpose of the NSIS of the Czech Republic is to influence the implementation of best practises and cooperation of all sectors of society in administrating and building trustworthy information and communication systems. At the same time it sets out the role and responsibilities of central bodies of the public administration for supporting information protection. The basic priority is to protect information and communication assets from threats which are aimed at information and communication systems, and to reduce potential damage to these systems by minimising risk.

The implementation of credible information and communication systems and their operation and administration must be part of the interests and responsibility of all levels of the public administration, the private sector and the general public.

The priority areas for this strategy are:

1. Information security management and risk management,
2. Information security knowledge,
3. National and international cooperation for information security,
4. Using best practises in information security,
5. Human rights and freedoms protection,
6. The competitiveness of the Czech economy.

Each priority area contains a strategic goal. Measures are set out for each individual strategic goal, which, when implemented, will fulfil that goal. Each individual measure consists of activities which are compiled at project or task level.

- Objective I: Improving Information Security Management and Risk Management
- Objective II: Developing Knowledge of Information Security

---

Objective III: Support for National and International Cooperation in Information Security
Objective IV: Support of the Use of Best Practices for Information Security
Objective V: Support for Human Rights and Freedoms
Objective VI: Support for the Competitiveness of the Czech Economy

The National Action Plan to Combat Terrorism (current wording)

The aim is to establish a complete framework of measures dedicated to all the aspects of potential risks related to terrorism (International Policy Aspects of the Involvement of the Czech Republic in the Current Global Efforts to Combat Terrorism, International Commitments of the Czech Republic and Internal Legislative Arrangements Related to the Fight against Terrorism, with Special Regard to the Agenda of the Fight against Financing Terrorism,


The regulatory framework

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

Data Protection/Privacy Legislation

The Data Protection Act (No.101/2000) was adopted in April 2000 with the aim to protect the citizens’ right to privacy. To this end, it regulates the rights and obligations regarding the processing of personal data, and moreover, specifies the conditions under which personal data may be transferred to other countries. It also allows individuals to access and correct their personal information held by public and private bodies. It is enforced by the Office for Personal Data Protection.

eCommunications Legislation

The ‘Act on Electronic Communications and on Amendment to Other Acts’ was adopted by the Czech Parliament on 22 February 2005 and became effective on 1 May 2005. It transposes the EU Regulatory Framework for Electronic Communications into national law.

eSignatures Legislation

The Electronic Signatures Act (No. 227/2000) was adopted on 29 June 2000 and amended in 2004. Together with several ordinances, this Act transposes the EU Directive on a Community framework for electronic signatures (1999/93/EC) and

amends several provisions of the Civil Code, so as to expressly provide legal value to electronic signatures.

Besides transposing the Directive (1999/93/EC) this act also establishes two national specific instruments - an electronic mark and a qualified timestamp token. The electronic mark is based on a qualified system certificate which can be issued both to natural and legal persons. The electronic mark is based on the same technology as the electronic signature but unlike the electronic signature the electronic mark can also be created automatically e.g. by an information system. The qualified timestamp tokens are issued in accordance with the ETSI TS 102 023.

eGovernment legislation

**Act No. 480/2004 Coll., on Certain Information Society services** was approved at the end of 2004. It addresses spam and limits liability of the providers as far the content of communicated information is concerned. The Act follows the efforts of the Government to eliminate obstacles hindering the development of electronic commerce.

Act No 300/2008 on Electronic Actions and Authorised Document Conversion was adopted on 17 July 2008 and entered into force on 1 July 2009. It accords electronic and hardcopy documents the same legal status, enables the authorised conversion of hardcopy documents and sets out provisions for the use of certified eSignatures.

The aim of the eGovernment Act is to simplify communication among citizens, businesses and public authorities, while producing significant savings. The Act first foresees the conversion of hardcopy documents into electronic format. In order for the electronic version to have the same legal status as the paper version, the texts will need to be converted by recognised authorities – notaries, regional or municipal authorities.

In addition, the Act states that each eDocument must have an authenticated eSignature, as well as a time stamp to show when the document was signed. In dealings with the public authorities, the certified eSignature will have the same value in certifying official documents as a hand-written signature.

Another innovation contained in the Act is the so-called 'Data Box' - a personal register of all electronic communications with the public authorities. All legal entities in the Czech Republic will be obliged to set up and activate their respective Data Boxes by 1 November 2009. Each Data Box is password protected and accessible only with a certified eSignature. Natural persons will be able to open their Data Boxes on a voluntary basis and use the documents they contain in their dealings with the public authorities.

**Classified Information Protection Legislation**

Act No. 412/2005 on the Protection of Classified Information. It governs the principles for determination of information as classified information, conditions for access to it and other requirements for its protection, principles for determination of sensitive activities and conditions for their execution and related execution of the state administration.

Government Regulation N. 522/2005 Establishing the List of Classified Information

Crisis management Legislation


Cybercrime legislation

A proposal for amendments in the legislation concerning the Council of Europe Convention on Cybercrime was finalized on February 5, 2005.

The following provisions of the Criminal Code may be applicable:

- Illegal access: § 257a - Damaging and misusing records in information stores. The mere access to the computer system is not a crime, but criminal responsibility may be applicable according to Section 257a.
- Illegal interception: The transmission of communication from one computer to another may be punishable according to Section 239 as violation of privacy of transmitted messages.
- Data interference, Section 257a.
- System interference, Section 257a.
- Misuse of devices: The criminalization of such conduct is limited to preparation of especially serious criminal offences, and to complicity or participation in an attempt or completed criminal offence. In the course of implementation it appears to be necessary to consider new legislative regulation.

4See: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/T-CY%202008-%20E%20-%20LONG%20REPORT%20FINAL.pdf
**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.

<table>
<thead>
<tr>
<th>National Authorities</th>
<th>CERTs</th>
<th>Industry Organisations and Association</th>
<th>Academic Organisations</th>
<th>Others</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ministry of the Interior</td>
<td>CESNET-CERTS - Czech Republic National Research and Educational Network CERT</td>
<td>The Association for Information Society (SPIS)</td>
<td>CESNET</td>
<td>Consumers Defence Association of the Czech Republic (SOS)</td>
</tr>
<tr>
<td>Ministry of Trade and Industry</td>
<td>CSIRT-MU - Masaryk University CSIRT</td>
<td>Czech Association of IT Managers (CACIO)</td>
<td></td>
<td>ISACA Czech Republic Chapter (ISACA CRC)</td>
</tr>
<tr>
<td>National Security Council</td>
<td></td>
<td>Association of Public Telecommunication Network Operators</td>
<td></td>
<td>OWASP Czech Republic Local Chapter</td>
</tr>
<tr>
<td>Civil Emergency Planning Committee</td>
<td></td>
<td>Telefonica O2 Czech Republic</td>
<td></td>
<td>CZESICON (CZEch Safer Internet Combined Node)</td>
</tr>
<tr>
<td>Office for Personal Data Protection</td>
<td></td>
<td></td>
<td></td>
<td>CZ.NIC</td>
</tr>
<tr>
<td>National Security Authority</td>
<td></td>
<td></td>
<td></td>
<td>Data Security Management Magazine</td>
</tr>
<tr>
<td>BIS</td>
<td></td>
<td></td>
<td></td>
<td>Security World Magazine</td>
</tr>
<tr>
<td>Czech Telecommunication Office</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For contact details of the above-indicated stakeholders we refer to the ENISA “Who is Who” – 2010 Directory on Network and Information Security and for the CERTs we refer to the ENISA CERT Inventory⁵

**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.

---

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

Co-operation via the Government Council for the Information Society, Ministry of the Interior and other government bodies

A key driver for the information exchange between the Czech NIS stakeholders is the Government Council for Information Society, which is performed by the Ministry of the Interior. It is a government advisory body for the development and the implementation of national information society strategy.

The Government Council for Information Society serves as coordinator in place of the abolished Ministry of Informatics, and ensures the government has an adequate knowledge base to help address concerns and make decisions regarding information society development.

The council consists of 28 members from the ministries of the interior, finance, industry and trade, as well as additional experts in from other public administrative bodies. The academic and business communities are also represented on the council. The chair of the council is a prime minister of the government.

Ministry of the Interior is responsible for eGovernment and for the information security coordination in public administration. Furthermore it is the main body which is responsible for an overall coordination in the area of critical infrastructure protection and critical information infrastructure protection both at the national and the international level. This role results from the Czech legislation covering particularly areas of civil protection, public order provision and internal security, civil emergency preparedness, crisis management and integrated rescue system.

Ministry of Industry and Trade is a central public administration authority for Electronic Communications and Postal services.

Czech Telecommunication Office - exercises state administration in the area of electronic communications and postal services, including market regulation and the determination of business conditions to substitute for the missing effects of economic competition and to provide conditions for appropriate functioning of economic competition and for the protection of users and other market actors until a fully competitive environment is achieved. The Office also provides protection of certain services in the area of audio and television broadcasting and information society services.

National Security Council - standing working body of the government, Bodies for managing and organizing the security of our State, oriented towards the comprehensive safeguarding of the security of the State i.e. in dealing with all serious crises and not only those connected with securing the defense of the Czech Republic against attack from the outside.

Civil Emergency Planning Committee - standing working body of the National Security Council. It is responsible for the area of civil emergency planning and for the coordination and planning of measures to safeguard the protection of the country's internal security.

The Committee was established under Resolution of the Government of the Czech Republic No. 391 of 10 June 1998 on the National Security Council and on the planning of measures to safeguard the security of the Czech Republic.
Co-operation via the National Security Authority

The Czech National Security Authority is responsible for the coordination in the area of classified information. It is an independent body which co-operates with all national government bodies.

The Czech National Security Authority is responsible for carrying out certification of information systems and for approving security projects of communication systems handling classified information and further, playing a role of national security accreditation authority, for accreditation of NATO and EU information systems in the territory of the Czech Republic.

The Authority performed development of security standards for conducting certification of cryptographic devices, it processed and issued updated security standards for the field of compromising electromagnetic emanations and prepared a new standard to be issued for so-called controlled cryptographic items.

Methodical materials have been processed on an ongoing basis addressing partial problems of safeguarding of information systems, setting of security parameters of the most used operational systems, general policy of information systems safeguarding and the method of documentation of information systems security.

These methodical materials are published or provided to applicants for certification, security standards are provided in accordance with their security classification level and at the same time the principle of "need-to-know" shall be applied.

Information exchange managed via CERTCZ

The Czech Republic has the model security team (CSIRT.CZ) which coordinates security incident solving in the computer networks of the Czech Republic. There is the objective it will become a national CSIRT. The cooperation CSIRT.CZ with other organizations as CERTS-CESNET and CZNIC-CSIRT helps to reach their goal.

CERTS-CESNET is an academic organization and it's main objectives is to provide a single, trusted point of contact for the CESNET2 network, to coordinate the handling of security incidents, which originated in the CESNET2 network, as well as preventing such incidents. Their activities include also helping the CESNET2 members and customers to improve their computer and network security.

Co-operation and information exchange via the Czech intelligence services and other government bodies and authorities

Within its legal jurisdiction, the Security Information Service maintains close and intensive cooperation with other relevant state authorities, in particular Czech intelligence services and Police of the Czech Republic.

The cooperation focuses particularly on international terrorism, terrorist threats, activities conducive to disclosure of confidential information, protect people and entities who work with classified information, extremism, illegal migration and organized crime, proliferation of weapons of mass destruction and their carriers, trade in weapons and arms, and operations of foreign intelligence services.
Co-operation and information exchange via the Office for Foreign Relations and Information

The Office for Foreign Relations and Information is an intelligence service of the Czech Republic. Its principal goal, effort and mission is to provide foreign intelligence vital for the security and protection of foreign policy interests and economic policy interests of the Czech Republic.

In addition to routine day-to-day exchange of information, particularly on international terrorism, extremism, illegal migration and operations of foreign intelligence services, mutual discussions and professional consultations were held as necessary.

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

The competent national data protection authority (Office for Personal Data Protection) cooperates with the Czech internet service providers: it informs them which of their clients infringe applicable legislation for the information society and requests suspension of email accounts or hosting services based on the general terms and conditions of the service provider. Internet service providers are however not entitled to provide information about their clients to the Office for Personal Data Protection.

Upon request of the national Office for Personal Data Protection, the national DNS provider must suspend access to problematic domains.
Country-specific NIS facts, trends, good practices and inspiring cases

Security incident management
The Czech National Security Authority is reporting, in general on security incidents, in particular in the domain of security incidents related or with an impact on the classified information. This reporting is public, via the annual report of the National Security Authority – the last published one (i.e. 2007) disclose that during the year 2007 a number of 107 events of the breach of the law were notified:

- 76 thereof in the field of classified information and
- 31 in the field of security eligibility.

A number of 17 cases were dealt with by another body, 41 were not proceeded with, in one case information was presented to the police on the commission of crime, in 4 cases sufficiency of evidence has not been accumulated yet, which would permit commencement of administrative proceedings.

In 44 cases administrative proceedings were commenced with natural and legal persons for breach of duties in the field of protection of classified information, in 39 cases thereof with natural persons and in five cases with a legal person. In one case the administrative proceedings were not proceeded with; in 5 cases the admonition and in 31 cases a fine was imposed.

The total amount of fines reached 77.500,- CZK, 28.000,- CZK thereof is the sum of money paid by natural persons and 42.000,- paid by legal persons.

The Authority issues the Bulletin of the Authority, in accordance with the Act, as periodic publication published twice a year or more frequently, as necessary. The Bulletin contains in particular a list of certified technical means according to the Act, further a list of organizations, which have been issued with the confirmation according to the Act N. 412/2005 Coll., a list of organizations, the validity of confirmation of which has expired or has been terminated, as well as a list of facilities, which have been issued with a facility security clearance.

In addition, in the Bulletin of the Authority information is published from areas of personnel security, security eligibility, industrial security, administrative security, physical security, security of information or communication systems or from the area of the cryptographic protection. Further, guidance notes issued by the Authority are published, various directions, guides, manuals and instructions, requests and other information for the professional public.

In general, providers in Czech Republic do not voluntarily report security incidents. Such cases are usually reported by media, by NGOs and by consumer protection organisations.

CSIRT.CZ (Computer Security Incident Response Team) is a name of the model security team which coordinates security incident solving in the computer networks of the Czech Republic. There is the objective it will become a national CSIRT.

The CSIRT.CZ goal is to help Internet Service Providers in the Czech Republic founding their own Security Incident Response teams as well as their security infrastructure,

solving security incidents and thus improving the security of their own networks as well as of the global Internet.

CSIRT.CZ also helps delivering security incident reports to the administrators of networks or domains where the incidents originated but whose administrators do not respond. In a sense, one can say that CSIRT.CZ acts as a "Last resort institution" when all regular forms of contacting appropriate administrators fail.

The **CSIRT.CZ** provides an online channel to report network and security incidents, and provides information mainly on:

- scanning
- spam
- viruses
- alleged misuse of copyrighted work
- phishing
- pharming

CZNIC-CSIRT team is responsible for incident handling within AS25192 and incident relating to nameservers for .cz and 0.2.4.e164.arpa:

- b.ns.nic.cz. 217.31.205.188, 2001:1488:dada:184:0:0:0:188
- c.ns.nic.cz. 195.66.241.202, 2a01:40:1000:0:0:0:2
- d.ns.nic.cz. 193.29.206.1, 2001:678:1:0:0:0:1
- e.ns.nic.cz. 194.146.105.38

CESNET-CERTS team is fully responsible for handling and responding to security incidents in domains cesnet.cz, cesnet2.cz, ces.net, liberouter.org, liberouter.net, ipv6.cz, eduroam.cz, and in the CESNET2 internal infrastructure marked as INFRA-AW in the RIPE database. The goals are following: providing a single, trusted point of contact for the CESNET2 network; coordinating the handling of security incidents which originated in the CESNET2 network, as well as preventing such incidents and helping the CESNET2 members and customers to improve their computer and network security.

It is interesting to mention that during the first half of 2009, Czech Republic was mentioned in the global report published by the Anti-Phishing Working Group (APWG) with the following relevant statistics:

- 195 unique phishing attacks reported for this country
- 99 unique domain names used for phishing reported for this country
- A score of 1.8 phish per 10,000 domains registered in this country
- A score of 3.5 attacks per 10,000 domains registered in this country

---


8 The Anti-Phishing Working Group (APWG) is the global pan-industrial and law enforcement association focused on eliminating the fraud and identity theft that result from phishing, pharming and email spoofing of all types.
Emerging NIS risks

There is a consolidated list of emerging NIS risks that are officially considered by the Czech Security Information Service (BIS) in its latest annual report. According to this public document, the Security Information Service also pays attention to related negative phenomena, such as cyber-terrorism, information warfare, information espionage etc.

In the view of BIS, there is considered a visible trend in the area of electronic attacks, namely an increasing number of thefts and subsequent abuse of electronic identities and economically motivated fraud related thereto. Non-financial services are targeted more and more often. One concern is related to the fact hackers subsequently use the compromised identities for other, often more sophisticated, electronic attacks, which make use, inter alia, of social engineering methods, or for other malevolent activities, e.g. distribution of spam, malware etc.

Another risk noted related to cross-border transfers of funds between individuals and entities without any control. Such funds can either come from illegal activities, or be subsequently used for such activities. There is a risk observed that some Islamic extremist groups may also carry out their financial operations in a similar way.

The attacks noted, whether real or potential, target users of mobile communication equipment, owners of various electronic cards or documents provided with electronic chips. In this respect, a factor identified by the BIS, which facilitates the attacks, is a low level of awareness of both users and manufacturers of potential risks associated with the use of modern advanced technologies.

Concerning the development and proliferation of harmful software, there is a risk linked to marked trend showing that malware is better protected against detection and subsequent analyses. The number of newly identified specimens of malware is decreasing. In addition to making a continuous use of weaknesses of computer programs, the perpetrators attempt to employ increasingly sophisticated methods of social engineering.

Resilience aspects

Although it seems that the primary authority responsible for network resilience is the Czech Telecommunications Office (the national regulatory authority), the competence of handling crisis situations is with the Ministry of Interior and/or Ministry of Defence.

The Electronic Communications Act of the Czech Republic states, for instance, that the national regulatory authority for telecommunications shall issue network plans for public communications networks in which it will define the basic characteristics of those networks and their interfaces, including the technical conditions for securing traffic through such networks in compliance with the national preference scheme for crisis situations. Other provisions of the same act lay down more specific rules on measures that operators shall/may take to handle crisis situations or network disruptions. In the Czech Republic, special requirements are addressed in the regulation with respect to the operators of which networks are to be used in crisis situations.

A special section of the Electronic Communications Act of the Czech Republic is dedicated “to the security and integrity of the electronic communications networks and services” and the provision of service in crisis situations. The section defines, inter alia, at a general level, the obligations of operators of public communications networks that
should be made available in crisis situations, especially in terms of the duty of these providers to communicate certain information to the national regulatory authority or to prioritize traffic. Furthermore, the regulation defines how the terms —national preference scheme and —international preference scheme should be understood. Also, the Czech Telecommunications Office can specify, through special regulation, the technical and organizational rules that should guide operators in the adoption of measures to ensure network service in crisis situations.

The State Authorities especially the Czech Telecommunication Office cooperate and collaborate with many non – governmental agencies and providers. The main co-operators are:

**Association of Mobile Network Operators (“AMNO“)**

The subject of activity of the AMNO includes creation of optimum conditions for development of public mobile telecommunication networks and provision of public mobile telecommunication services in the Czech Republic. The AMNO protects common interest of its members as well as individual interests of its members, unless this is contrary to the common interest. With regard to the fact that the optimum conditions of development of entrepreneurial activities of the AMNO members are based on open competition, the main aim of the Association is to support and protect fair open market of electronic communications in the Czech Republic based on rules that respect protection of economic competition.

**Association of Public Telecommunication Network Operators (“APTNO“)**

The APTNO assists and encourage market liberalization and competition, protects members interests, represents telecommunications industry to key government and regulatory bodies, forms a platform for discussion among incumbent and alternative operators, projects contribute to the customers protection.

The most important task of the APTNO is the analysis of the telecommunication legislation and regulatory issues, assessment of the most important topics and proposal for their solution in defined projects. Such expertise has been going on in committees and expert teams, operating on the APTNO ground. Expert teams are being formed from experts nominated by member companies.

In addition, experts from specialized institutions such as the Czech telecommunication Office are invited to join the teams. A closed contact has been established with the Regulator (Czech telecommunication Office). The APTNO has been charged by the Office to carry on several projects: the operation of National Reference Database and NP service for fixed networks, Network Plans of Signalization and Transmission Parameters. The APTNO expert teams participate in the Office projects such as the development of Numbering Plan. The APTNO has become respective partner of the Ministry of Industry and Trade as well.
Privacy and trust

**Status of implementation of the Data Protection Directive**

The Data Protection Directive was implemented by Act No. 101/2000 Coll., on Personal Data Protection (the “DPA”).

The competent national regulatory authority on this matter is the Office for Personal Data Protection (Úřad pro ochranu osobních údajů) (the “Office”)

**Personal Data and Sensitive Personal Data**

The definition of personal data in the DPA is closely based on the standard definition of personal data and is interpreted broadly. It includes any information which can lead to the direct or indirect identification of an individual. According to the guidance issued by the Office in 2001, the definition of personal data cannot be considered in isolation, it should be interpreted in light of concrete circumstances of personal data processing.

The DPA does not apply to data relating to legal entities. However, data relating to legal entities are also protected by national legislation, in particular, by the provisions of the Commercial Code relating to business names and unfair competition.

Under the DPA, sensitive personal data includes: (i) the standard types of sensitive personal data; (ii) information about criminal offences and alleged criminal offences; and (iii) biometric and genetic data. Personal data may be processed if the standard conditions for processing sensitive personal data are met. If consent is relied upon, then the data controller must be able to prove the data subject’s consent during the entire period of data processing.

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

The data controller (as well as the data processor) must comply with the general security obligations.

The data controller (or the data processor) must develop and document technical and organisational measures it implements and perform a risk assessment in relation to: (i) fulfilment of data processing instructions by persons who have immediate access to the personal data; (ii) prevention of unauthorised persons’ access to personal data; (iii) prevention of unauthorised reading, creating, copying, transferring, modifying or deleting of records containing personal data; and (iv) measures enabling determination and verification of to whom the personal data was transferred.

**Data protection breaches**

The DPA does not contain any obligation to inform the Office or data subjects of a security breach. However, data controllers in certain sectors may be required to inform special sectoral regulators of any breach (for example, financial services firms may be required to report any security breach).

**Enforcement**

The fines for breaches of the DPA are imposed by the Office. If not paid, fines are enforced by the competent customs authority. Sanctions under the Criminal Code are imposed by the criminal courts.
NIS awareness at the country level

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

Awareness actions targeting the consumers/citizens

The Czech Safer Internet National Center (Saferinternet CZ\(^9\)) has been launched in January the 1st 2009 as the follow up of the CzeSICO\(N\) project. It is supported by the European Commission in the frame of the Safer Internet programme.

In compliance with the programme objectives, the project strives to enhance Internet users’ awareness of possible on-line threats; to establish and run the Hotline for notification of illegal and harmful content, especially sexual child abuse and bullying.

The project is operating also the Helpline to provide psycho-social assistance to children who got in troubles on the Internet.

The Czech National Safer Internet Centre supports self-regulation initiatives, commitment of children to create safer on-line environment and to learn new things about latest trends in the use of on-line technologies and their impacts on children’s lives.

The Centre is initiating, coordinating and contributing to a broad range of activities and campaigns with the aim to raise the safer Internet awareness. Among others:

**National campaign:**

The Czech National Safer Internet Centre coordinates the celebration of Safer Internet Day in the Czech Republic and organizes annually the story telling competition Mobilstory\(^10\) run under auspices of the Minister of Education, and the WebQuest\(^11\) contest for teachers to prepare online learning tools incorporating the safer Internet issues. The centre continuously cooperates with stakeholders on variety of other campaigns such as Juniorinternet\(^12\), Bambiriada\(^13\), Night with H.Ch.Andersen\(^14\), etc.

**Reaching the target groups:**

In order to reach and learn from the specific target groups the Czech National Safer Internet Centre is organising workshops in schools and public libraries around the country. The Centre is holding presentations and debates for librarians, teachers and parents about the Internet and possible threats for children, discussing safe use of the internet and methods of how to avoid possible problems.

The Centre is organising annual Safer Internet conference for professionals – teachers, representatives of public administration, lawyers, children welfare organisations, etc.

\(^12\) [http://www.juniorinternet.net/](http://www.juniorinternet.net/)
Youth Panel:

The Youth Panel of the Czech National Safer Internet Centre includes young people aged 15-18 years. The representatives of the Czech Safer Internet youth Panel took part at the meeting organized by the EC in Brussels last year by occasion of the Safer Internet Day 2008. They contribute also to the Youth Panel meeting 2009 in Luxembourg.

Educational and promotion materials:

The Czech Safer Internet National Centre is contributing to localised version of the Teachtoday.eu portal as a very important tool to deliver educational content to schools. The Centre took advantage of the e-safety family kit of the Insafe to localise it into the Czech and deliver the interesting safer internet related content in an attractive form to households.

The Czech National Safer Internet Centre launched this year the anti-cyberbullying website in the frame of the campaign started during the Safer Internet Day 2009. Children and their parents can find here basic information about issues connected with such a misuse of the Internet.

New knowledge:

Gathering information and initiating new knowledge is important for the Centre. That is the reason why two surveys of the online behaviour of children were launched in the past. The last Safer Internet survey of 2009 allows the Centre to compare the results with outcomes of the similar research made in 2006. Based on such comparison the Centre is able to tune up the planned activities and campaigns according the real habits and needs of children and their parents on the Internet.

Czech Safer Internet National Centre:

The Safer Internet project is operating since 2006 with the support of the European Commission. It includes the Online Safety Institute to coordinate awareness campaigns and provide the relevant content. It operates the Internet hotline to struggle against online crime and the Internet helpline to provide assistance to children in troubles on the Internet.

Awareness measures to combat spam and/or malware

The website of the Czech national Office for Personal Data Protection contains general information about spam and phishing. There is no official resource for information about spyware and malicious software.

Awareness actions towards cybercrime

CYTER 2009 is the third conference on Cyber terrorism and Cybercrime held in Prague, Czech Republic. As in the past, the conference covered broad spectrum of topic from technology and networking to sociological and psychological effects of internet misuse. The politics and global view of the cyber terrorism and crime created integral part of conference.

CYTER 2009 was a part of the Czech Republic EU presidency program and was organized under patronage of top political and scientific personalities in Czech Republic as well as
in European Union. Major organizer was Czech Technical University Prague in cooperation with the Ministry of the Interior of the Czech Republic.  

**IT Security Workshop: Data and Network Security**

The objective of the event is to acquaint the professionals involved in building and managing information security with the risks in the field of data protection and with the possibilities of mitigating these risks. Main topics are: security management, data and software protection, network security, antivirus protection, antispam and antispyware. The event is an annual event and was last held on 23 March, 2009 in Prague.

**Relevant statistics for the country**

The information society in the Czech Republic is at a relatively early stage of development. Although progress has taken place since last year in the areas of broadband and internet usage, there is still room for improvement.

Based on the Eurostat information, it appears that the broadband penetration trend for the Czech Republic is currently below the EU average:

![Broadband Penetration Trend](diagram)

**Broadband**

Progress in DSL coverage has been strong and is in line with the EU27 average. There has been a significant improvement in households' connectivity over the last years and the share of broadband subscriptions relative to total internet subscriptions has increased from 23% in 2004 to over 79% in 2008.

Fixed broadband penetration and the percentage of households having access to broadband however remain low. Nevertheless, all broadband subscriptions now display 2MB/s speeds, suggesting that the Czech Republic is benefiting from the

---

16 See [http://www.itsw.cz/?lang=1](http://www.itsw.cz/?lang=1)
17 Source: Eurostat
The development of platform competition and accelerating its transition to broadband. The percentage of user accessing the internet through UMTS is also above average. \(^{18}\)

**Internet Usage**

The Czech Republic has a somewhat lower proportion of regular and frequent internet users in the population than the EU average, although the proportion of those who have never used the internet is the same as for the EU as a whole.

In addition, the number of users has risen substantially over the past few years: the number of regular users has doubled over the period since 2005 to reach 51% in 2008, and the number of frequent users has tripled, to reach 30%. \(^{19}\)


### National authorities in network and information security: role and responsibilities

<table>
<thead>
<tr>
<th>National authorities</th>
<th>Role and responsibilities</th>
<th>Website</th>
</tr>
</thead>
</table>
| 1. Ministry of the Interior | The Ministry of the Interior is supreme office for the realms of public administration, internal security, border protection, crisis management and eGovernment in the Czech Republic. The Ministry of the Interior is a central governmental authority for home affairs, in particular for:  
- Public order, internal order and security within its defined scope of competence, including supervision of road traffic safety  
- Fire protection;  
- The right of association and the right of assembly, and registering organisations with international links;  
- Public collections;  
- State, economic and service secrets;  
- Maintaining archives; and  
- The territorial structure of the state;  
- Travel documents, granting residence to foreign nationals and granting refugee status;  
- The national border, surveying of the national border, maintenance and documentation;  
- National symbols;  
- First names and surnames, Registers of Vital Records; nationality, identity documents, reporting residence, the register of inhabitants, and birth (personal) identification numbers;  
- Firearms and ammunition.  
The Ministry of the Interior is also  
- Responsible for public administration communication infrastructure  
- Maintains the telecommunication network of the Police of the Czech Republic and provides guidance relating to encoding services;  
<p>| 3. Czech Telecommunication Office | The Office exercises state administration in the area of electronic communications and postal services, including market regulation and the determination of business conditions to substitute for the missing effects of economic competition and to provide conditions for appropriate functioning of economic competition and for the protection of users and other market actors until a fully competitive environment is achieved. The Czech Telecommunication Office also provides protection of certain services in the area of audio and television broadcasting and information society services. | <a href="http://www.ctu.cz">www.ctu.cz</a> |</p>
<table>
<thead>
<tr>
<th>National authorities</th>
<th>Role and responsibilities</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>abolished Ministry of Informatics, and ensures the government has an adequate knowledge base to help address concerns and make decisions regarding information society development. The council consists of members from the ministries of the interior, finance, industry and trade, as well as additional experts in from other public administrative bodies. The academic and business communities are also represented on the council.</td>
<td></td>
<td>spolecnost.aspx</td>
</tr>
</tbody>
</table>
| 5. Office for Personal Data Protection | The Office for Personal Data Protection is an independent agency which supervises compliance with personal data legislation and deals with citizen complaints in this domain. Responsibilities include:  
  - supervises the observance of legally mandated responsibilities in the processing of personal data,  
  - maintains a register of instances of notified personal data processing,  
  - deals with incentives and complaints from citizens concerning infringements of the law,  
  - provides consultations in the area of personal data protection. | | www.uouu.cz |
| 6. National Security Authority | National Security Authority is responsible for the coordination in the area of classified information. It is an independent body which co-operates with all national government bodies. Responsibilities include:  
  - responsible for personnel and facility security clearance procedures;  
  - issues personnel security clearance certificates, facility security clearance certificates and security eligibility certificates;  
  - has overall competences in the area of the protection of classified information (including supervision and methodology);  
  - maintains the central registry of CI and approves establishment of registries in the state bodies and in facilities;  
  - approves a release of classified information internationally;  
  - carries out a certification of technical means, information systems, cryptographic devices, cryptographic sites and shielded chambers;  
  - develops and approves national cipher algorithms and creates a national cryptographic protection policy; issues security standards on the protection of classified information;  
  - is responsible for recognition of personnel and facility security clearances. | | www.nbu.cz |
| 7. BIS | The Security Information Service is an intelligence institution of the Czech State, active within the Czech Republic. It reports to and is audited by the Government of the Czech Republic  
  The mission and goal of BIS work is to anticipate, reduce and eliminate the most serious threats to our civilization, our state and in their ultimate effect the lives and wellbeing of all its citizens. In the extraordinary instances when the Service is compelled to infringe upon human rights and liberties, it invariable does so in compliance. | | www.bis.cz |
National authorities | Role and responsibilities | Website
--- | --- | ---
with the rules set by law. For example, no phone is ever tapped without the consent of the President of a High Court Senate. The Service has no authority to detain, arrest or interrogate any individual. Its creed is faithfulness to democratic values, the Constitution and the laws of the Czech Republic. It attaches extraordinary importance to communicating with the public, as it could hardly fulfil its mission without its support, and highly appreciates any help with which it is provided in protecting democracy, freedom and national security.

Computer Emergency Response Teams (CERTs): roles and responsibilities

<table>
<thead>
<tr>
<th>CERT</th>
<th>FIRST member</th>
<th>TI Listed</th>
<th>Role and responsibilities</th>
<th>Website</th>
</tr>
</thead>
</table>
| 8. CESNET-CERTS | No | Yes | CESNET-CERTS is the Czech Republic National Research and Educational Network CERT. The roles of CESNET-CERTS are:  
- Providing a single, trusted point of contact for the CESNET2 network.  
- Coordinating the handling of security incidents which originated in the CESNET2 network, as well as preventing such incidents.  
- Helping the CESNET2 members and customers to improve their computer and network security. | www.cesnet.cz/csirt |
| 9. CSIRT-MU | No | Yes | CSIRT-MU is the Masaryk University CSIRT. | www.muni.cz/ics/ |
| 10. CZNIC-CSIRT | No | Yes | CZNIC-CSIRT is the CZNIC-CSIRT team. CZNIC-CSIRT team is responsible for incident handling within AS25192 and incident relating to nameservers for .cz and 0.2.4.e164.arpa. | www.nic.cz/csirt/ |
## Industry organisations active in network and information security: role and responsibilities

<table>
<thead>
<tr>
<th>Industry organisations</th>
<th>Role and responsibilities</th>
<th>Website</th>
</tr>
</thead>
</table>
| 11. The Association for Information Society (SPIS)          | The Association for Information Society (SPIS) is a professional organization of enterprises operating in the information and communication technology (ICT) sector. Its chief objective is to create an information society based on knowledge and innovation. The Association champions the importance of modern information technology as a fundamental tool for building an efficient public administration system, a prerequisite for the full integration of the Czech Republic into European structures and essential for increasing the competitive strength of the Czech economy.  

The principal objective of SPIS at present is the full implementation of eGovernment, as well as improving services for citizens and reducing the bureaucratic burden by employing modern methods and technologies. This involves monitoring and influencing the law-making process with regard to laws related to the use of ICT, particularly in areas that impact the lives of citizens, enterprises, the state, and especially public administration. Another important task is the provision of information to SPIS members in the preparation of projects that can potentially be, and are, financed from EU funds. SPIS is also involved in the implementation of international ICT standards in the Czech Republic. In relation to the Czech Republic’s EU presidency in 2009, SPIS has prepared a proposal to introduce knowledge society development as one of the themes of the Czech presidency. | www.spis.cz       |
| 12. Czech Association of IT Managers (CACIO)                | CACIO is an IT industry association and attempts to unite IT managers throughout the Czech Republic.  

The association aims to create a professional platform for CIOs so that they are able to contribute to IT management at an organizational level as well as to the overall Czech economy. Goals of the association include: information sharing, presentation of expert opinions, and support/develop professional/expert opinions concerning IT legislation. Members participate at NIS connected conferences, and organize workshops and seminars. | www.cacio.cz      |
| 13. Telefonica O2 – department of security                  | Dept. of security provide security for voice and data transmissions, certification authority and network services                                                                                                                                                                                                                                                                                                                                                                         | www.ctu.cz/        |
### Academic organisations active in network and information security: role and responsibilities

<table>
<thead>
<tr>
<th>Academic bodies</th>
<th>Role and responsibilities</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>14. CESNET</td>
<td>CESNET is an association of legal entities held by all universities of the Czech Republic and the Czech Academy of Sciences. Its main goals are operation and development of the Czech NREN, research and development of advanced network technologies and applications and broadening of the public knowledge about the advanced networking topics.</td>
<td><a href="http://www.ces.net/">http://www.ces.net/</a></td>
</tr>
</tbody>
</table>

### Other bodies and organisations active in network and information security: role and responsibilities

<table>
<thead>
<tr>
<th>Other organisations</th>
<th>Role and responsibilities</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>15. ISACA Czech Republic Chapter (ISACA CRC)</td>
<td>ISACA Czech Republic is a chapter of international Association ISACA. The chapter was established in 1997 and currently has about 170 members (IT and Security Professionals) both from public and private sector. Goals of the association include: information governance, control, security and audit professionals, organizing workshops and seminars.</td>
<td><a href="http://www.isaca.cz">www.isaca.cz</a></td>
</tr>
<tr>
<td>16. Czech Society for Quality</td>
<td>The Czech Society for Quality offers wide range of courses, publications and workshops focused on the quality management systems (ISO 9001, ISO TS 16949), environment (ISO 14001), safety and the protection of health at work (OHSAS 18001), information safety (ISO/IEC 27001), food safety (HACCP, ISO 22000), benchmarking, measurement of customer satisfaction (EPSI), project management, process management, CAF model, EFQM model, metrology, statistical method, sampling and operation of laboratories The Czech Society for Quality is an unincorporated association joining together the wide spectrum of people and organisations acting in various areas of management systems and at the same time it provides, not only its members, with top education in the area of management systems and quality management tools (information security - ISO/IEC 27001 ).</td>
<td><a href="http://www.csq.cz/cs/">www.csq.cz/cs/</a></td>
</tr>
<tr>
<td>17. OWASP Czech Republic Local Chapter</td>
<td>The Open Web Application Security Project (OWASP) is an open-source application security project. The OWASP community includes corporations, educational organizations, and individuals from around the world. This community works to create freely-available articles, methodologies, documentation, tools, and technologies. The OWASP Foundation is a 501(c)(3) charitable organization that supports and manages OWASP projects and infrastructure. OWASP is not affiliated with any technology company, although it supports the informed use of security technology. OWASP has avoided affiliation as it believes freedom from organizational pressures may make it</td>
<td><a href="http://www.owasp.org/index.php/Prague">www.owasp.org/index.php/Prague</a></td>
</tr>
</tbody>
</table>
### Consumer organisations active in network and information security: role and responsibilities

<table>
<thead>
<tr>
<th>Consumer organisations</th>
<th>Role and responsibilities</th>
<th>Website</th>
</tr>
</thead>
</table>
Country specific NIS glossary

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIS</td>
<td>Security Information Service</td>
</tr>
<tr>
<td>CACIO</td>
<td>Czech Association of IT Managers</td>
</tr>
<tr>
<td>CERTCZ</td>
<td>Computer Emergency Response Team under Ministry of Internal Affairs</td>
</tr>
<tr>
<td>CERTS-CESNET</td>
<td>Czech Republic National Research and Educational Network CERT</td>
</tr>
<tr>
<td>CESNET/CESNET2</td>
<td>Contemporary network built around the DWDM core in the Czech Republic.</td>
</tr>
<tr>
<td>CSIRT.CZ</td>
<td>Czech Computer Security Incident Response Team</td>
</tr>
<tr>
<td>CSIRT-MU</td>
<td>Masaryk University CSIRT</td>
</tr>
<tr>
<td>CYTER</td>
<td>Conference on Cyber terrorism and Cybercrime</td>
</tr>
<tr>
<td>CZESICON</td>
<td>CZEch Safer Internet Combined Node</td>
</tr>
<tr>
<td>CZESICON</td>
<td>Czech Safer Internet Combined Node</td>
</tr>
<tr>
<td>CZNIC-CSIRT</td>
<td></td>
</tr>
<tr>
<td>DPA</td>
<td>Data Protection Act</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>OWASP</td>
<td>Open Web Application Security Project</td>
</tr>
<tr>
<td>Saferinternet CZ</td>
<td>Czech Safer Internet National Center</td>
</tr>
<tr>
<td>SOS</td>
<td>Consumers Defence Association of the Czech Republic</td>
</tr>
<tr>
<td>SPIS</td>
<td>Association for Information Society</td>
</tr>
<tr>
<td>Úřad pro ochranu osobních údajů</td>
<td>Office for Personal Data Protection</td>
</tr>
</tbody>
</table>

References
