Slovakia 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, 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 **Slovakia Country Report** on behalf of ENISA: Dan Cimpean, Johan Meire and Jan D'Herdt.

Legal notice

Table of Contents

Slovakia

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*
        - *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

NIS national strategy, regulatory framework and key policy measures

Overview of the NIS national strategy

Strategy and Action Plan for the Development of the Information Society[1]

Slovakia's overall eGovernment strategic objectives were set in the Strategy and Action Plan for the Development of the Information Society adopted in January 2004. According to that document, strategic objectives of Public Administration computerisation were:

- to ease and widen citizens' participation in public affairs through the computerisation of public services;
- to ease communication between businesses and Public Administration;
- to increase the effectiveness of Public Administration through digitisation;
- effective eGovernment and modern on-line services;
- to prepare Slovak Public Administration for smooth integration into EU structures.

NIS elements in the overall National Security Strategy of the Slovak Republic

The National Security Strategy of the Slovak Republic highlights the need to adopt measures to reduce vulnerability of critical infrastructure elements, with emphasis on information and communication systems, and to minimise negative consequences of attacks against them.

According to the National Security Strategy, the Slovak Republic authorities will continue to work towards ensuring security and integrity of information and communication systems, in particular the systems that are essential for securing basic functions of the state. Also they will continue to cooperate with foreign partners in order to maximise the security of the systems of mutual communication and information exchange, in particular in the area of the transmission and protection of classified data.

Strategy for Protection of Cyberspace and of Critical Infrastructure

The Strategy for Protection of Cyberspace and of Critical Infrastructure is a government strategic initiative and is currently under preparation. At this stage the involved stakeholders are working on the conceptual aspects of the strategy.

In February 2008, the Slovak Government approved Slovak Republic which defines the vision by the year 2013 - to achieve continuous growth of citizens´ satisfaction with the public administration through the provision of services in an attractive and simple manner while simultaneously increasing its effectiveness and competence and reducing the costs of public administration. Four strategic objectives defined in the document are increasing satisfaction of citizens, businessmen and other public bodies with the public administration, enablement of public administration processes, re-engineering and increasing the effectiveness and competence of public administration.

During last and current year the main focus of Slovakia's NIS national strategy is on establishing and deploying a national CERT. The national CERT – CERT.SK is currently

[1] *http://www.epractice.eu/en/document/288351*

established and is in process of deployment. CERT.SK should be operational in January 2010.

Slovak Republic National Policy on Electronic Communications[2]

The National Policy on Electronic Communications (NPEC)defines the strategy of the development of electronic communications networks and services in the Slovak Republic, particularly in the field of improvement of the legal framework, strengthening of the independent regulatory body, development of a competitive environment, securing and protection of end users rights, support of the development of information society services and international co-operation. The National Policy on Electronic Communications was formulated by the Ministry of Transport, Posts and Telecommunications of the Slovak Republic that is the central body of the state administration for this area.

The primary strategic objective of the State policy in the area of electronic communications is the satisfaction of needs of the Slovak economy, requirements of natural and legal personalities and interests of the State in provision of quality, reliable and widely accessible services of electronic communications within a scope corresponding to the developed EU states and the integration of the Slovak Republic into information society of the 21st century. An important part of this primary strategic objective is support of the equalisation of the level of electronic communications in the Slovak Republic with the European context.

The main objective in the area of communications safety and personal data processing is to support protection of public communications data and to protect private and legal interests of subscribers and users of public communications services:

- Providers of public electronic communications services should take appropriate technical and organisational measures to protect safety of their services, with regard to the network safety, together with the network provider where necessary, that will secure the level of safety adequate to given risk; in the interest of damage prevention they also ought to inform subscribers and users about possible safety risks of the relevant communications,
- Service providers offering publicly available electronic communications services via Internet are obliged to inform the users and the subscribers about measures they have adopted to protect the communications safety (special software, coding, encrypting etc.);
- Where electronic communications network, in addition to transmitted data, are able to process also the data indicating the position of users or subscribers of the services, such data can be processed only if they remain anonymous, or with consent of the users or the subscribers and up to the extent and for the time period indispensable for provision of the value-added service;
- Service providers are obliged to provide the subscribers with an adequate protection against disturbance endangering their privacy by unsolicited calls and fax messages, electronic mail or other forms of communications for the purposes of direct marketing;
- Protection of personal data and privacy of the users of publicly available electronic communications services should be independent of configuration of the

[2] *http://www.telecom.gov.sk/index/open_file.php?file=telekom/Strategia/Politika/npec.pdf&lang=en*

components necessary for the service provision and of the distribution of necessary functions among such components.

eGovernment Strategy [3]

In May 2008, the Slovak Government approved the **National Concept of eGovernment** presented as the "second key document for the development of eGovernment in Slovakia", this concept is a follow-up to the country's 'Strategy for Public Administration Informatisation'. The document defines an integrated architecture for the Information Systems operated by the Public Administration (referred to as 'ISPA'). The new concept specifies common bases, principles and priorities for the building of information systems operated by the State Administration and local authorities in compliance with their defined competencies. The aim is to ensure the interconnection and mutual cooperation of all Slovak Public Administrations' systems.

Among other basic architecture components, the National Concept of eGovernment notably specifies identifiers, registers, code-books, access components, common CPAP (Central Public Administration Portal) modules, etc. It aims to ensure that any particular data is modified only once, at one point, and are automatically forwarded to all registers, that, thus, will not be asked to provide the same data several times.

National Strategy for Information Safety [4]

The National Strategy for Information Safety of Slovakia was approved by the Slovak Government in August 2008 and deployed from April 2009. This document consists of three levels. First level describes long term strategic goals for information safety in Slovakia. Second level focuses on strategic priorities and third defines most important problems and tasks. This document includes separation of competences, priorities and steps to reach the objectives. The document also describes tasks for ensuring protection of non-secret information in digital space of Slovakia. These tasks include regulation of information leak, illegitimate use of information and of data integrity violation.

Concept of software products usage for public administration [5]

The concept of software products usage for public administration was approved by the Government of Slovakia in July 2009. This document defines a general strategy for procurement, implementation and operation of software products in public administration environment, taking into account eGovernment goals according requirements and recommendations of EU in the field of open source software.

[3] *http://www.epractice.eu/en/document/288351*

[4] *http://www.epractice.eu/files/eGovernment%20in%20SK%20-%20June%202009%20-%2012.0.pdf*

[5] *http://www.epractice.eu/en/document/288351*

The regulatory framework

In the past year there has been significant activity on programs regarding information security regulation. The following regulations of the Slovak Republic have relevance and applicability in the domain of network and information security:

Cyber Security Law

A Cyber Security Law for Slovakia is currently a work in process. The Law is made by the Ministry of Finance and will regulate principles to apply in public administration information systems.

eGovernment Legislation [6]

There is currently no overall eGovernment legislation in Slovakia. However, the Act No. 275/2006 on Public Administration Information Systems (20 April 2006) provides a framework for the development of information systems of public authorities. On 1 October 2008 the Edict about Standards for Information Systems of Public Administration, No. MF/013261/2008-132, came into force.

Data Protection/Privacy Legislation [7]

Act No. 428/2002 on Personal Data Protection

The Office for Personal Data Protection of the Slovak Republic has developed a regulation regarding the protection of personal Data, Act No. 428/2002 of 3 July 2002 on Protection of Personal Data. This act implements the principles set in the EU's Data Protection Directive (95/46/EC).

Next to this regulation other regulations regarding the privacy protection of natural person are also in place, Act No. 460/1992 Coll. Constitution of the Slovak Republic of September 1st, 1992, and Act No. 40/1964 Coll. Civil Code. of February 26th, 1964.

eCommerce Legislation [8]

Act No. 22/2004 on Electronic Commerce

The Act on Electronic Commerce, which came into force on 1 February 2004, regulates relationships between providers of Information Society services and their recipients arising during their long-distance communication, during connection of electronic equipment via an electronic communication network and consisting of electronic processing, transmission, storage, search or collection of data including text, sound and picture, supervision over compliance with this Act, and also international co-operation in electronic commerce.

Act No. 610/2003 on Electronic Communications

---

[6] *http://www.epractice.eu/en/document/288352*

[7] *http://www.dataprotection.gov.sk/buxus/docs/act_428.pdf*

[8] *http://www.epractice.eu/en/document/288352*

The Act on Electronic Communications, which entered into force on 1 January 2004, transposes to Slovak Law the EU's New Regulatory Framework for electronic communications: Directive No. 2002/58/EC on Privacy and Electronic Communication, Authorisation Directive No. 2002/20/EC, Access Directive No. 2002/19/EC, Universal Service Directive No. 2002/22/EC and Framework Directive No. 2002/21/EC.

Enforcement of the Act on Electronic Communications is done by the Telecommunications Office of the Slovak Republic, that is focused mainly on: inspecting compliance with conditions for the provision of electronic communication networks and services, on inspecting compliance with conditions for the placing on the market of telecommunications terminal equipment and radio equipment and their introduction into operation, disturbance protection, and settling disputes out of court.

Act No. 215/2002 on Electronic Signatures

The Act on Electronic Signatures (15 March 2002), which came into effect on 1 July 2002, transposes Directive 1999/93/EC on a Community framework for electronic signatures. It requires the use of advanced electronic signatures for communication with Government bodies.

Cybercrime

Criminal Code [9]

The Criminal Code article 257a covers the damaging and misuse of the records on the information bearers, which in principle comprises all the alternatives defined in articles 2-7 of the Council of Europe Convention on Cybercrime.

Self-regulations

Self-regulatory Code of Conduct for Public Mobile Electronic Communications Operators concerning Safer Mobile Use by Younger Teenagers and Children [10]

The Slovakian 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 Slovakian mobile electronic telecommunications market and complies with applicable European and national legislation.

[9] *http://www.fidis.net/interactive/wiki-on-id-related-law/wiki/Slovakia%20B4c.%20Computer%20Fraud/*

[10] *http://www.gsmeurope.org/documents/eu_codes/Slovenian_code_of_conduct.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.

National Authorities	• Ministry of the Economy, Directorate for Electronic Communications • Ministry of Finance • Ministry of the Interior • Ministry of Transport, Posts, and Telecommunications • Government Plenipotentiary for Information Society • The Office for Personal Data Protection • National Security Authority • Telecommunications Office • Institute of Security and Defence Studies of MoD • Commission for Information Security
CERTs	-
Industry Organisations	• ITAS (IT Asociacia Slovenska) • Slovak Association for Information Security (SASIB)
Academic Organisations	• Department of Computer Science, Faculty of Mathematics, Physics and Informatics, Comenius University • Faculty of Informatics and Information Technologies, Slovak University of Technology in Bratislava • Faculty of Electrical Engineering and Informatics, Technical University of Kosice • Faculty of Special Engineering (University of Zilina)
Others	• Magazine DSM - Data Security Management and TATE International Slovakia • ISACA • ZSS (Association of Slovak Consumers)

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 Inventory[11]

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.

[11] 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

Co-operation via the Commission for Information Security

The Commission for Information Security under the Ministry of Finance, together with Slovak government, acts as national decision-making authorities in developing the information security policy in the Slovak Republic. The Commission is a working group consisting of employees of Ministry of Finance, national network and information security stakeholders (such as other ministries) and external experts in the field of information security The Commission cooperates with the Slovak Telecom office, Personal Data Protection Office, Ministry of Interior, National Security Authority. The Ministry of Finance oversees all execution concerning methodical and legislative activities connected to information society and information security issues at the national level as well as is responsible for implementation of all above mentioned.

Slovakia is currently in the process of deploying a national CERT. The responsible national authority for the national CERT.SK is a department in the Ministry of Finance.

Co-operation via the National Security Authority

The National Security Authority, an independent government body, is recognized among NIS stakeholders in the Slovak Republic as the national security agency responsible for the area of classified information. For unclassified information the Ministry of Finance is the main responsible. There exists also specific areas (like Digital Rights or Personal Data Protection), that are supervised by other state bodies (shown examples belongs to Ministry of Culture of the Slovak Republic and Personal Data Protection Office in this order), which should interfere but not over compete with the competences within the basic division. An advisory and coordination board has been established by Ministry of finance of the Slovak republic to facilitate mutual communication - Committee for Information Security.

Co-operation via the Cooperative Cyber Defence Centre of Excellence

The Slovak Republic is participating in the Cooperative Cyber Defence Centre of Excellence (CCD COE[12]) together with other sponsoring nations: Estonia, Germany, Italy, Latvia, Lithuania and Spain. CCD COE is located in Estonia and is open to all NATO nations and may cooperate with other nations as contributing participants.

The CCD COE first priorities are to provide insight, subject matter expertise, and assistance to NATO on various aspects of cyber defence: input to concept development, training and exercises, publishing lessons learned, and the development of a legal framework for cyber defence.

Others

ITAS, the IT Association Slovakia is a professional association that cooperates with the Slovakian Government on solving IT problems regarding electronic communications (e-government), IS and NIS.

[12] *http://www.ccdcoe.org/*

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

Security incident management

Although, there is not a national CERT in place, incidents regarding the security of personal data and privacy sensitive data have been noted by the Office for personal Data Protection. With the development and deployment of CERT.SK, Slovakia hopes to increase and centralize incident reporting.

It is interesting to mention that during the first half of 2009, Slovakia was reported in the global Top 20 Phishing TLDs[13] in the 2009 report[14] published by the Anti-Phishing Working Group (APWG)[15]:

- 132 unique phishing attacks were reported
- 46 unique Slovak domain names used for phishing were reported
- A score of 2,5 phish per 10.000 domains registered in Slovakia
- A score of 7,1 attacks per 10.000 domains registered in Slovakia

No specific network or information security incident information is published on the web site of Slovak Telekom – the main telecommunication provider.

Emerging NIS risks

Vulnerability of information and communication systems, their overloading, unauthorised access to information, spread of computer viruses, and misinformation are specifically identified as growing threats for the Slovak Republic – this is highlighted in the overall National Security Strategy[16] of the Slovak Republic.

There is no indication of the involvement of NIS-responsible bodies in the pan-European initiatives focused on emerging risks, like for example in the FORWARD[17] initiative of the European Commission to promote the collaboration and partnership between academia and industry in their common goal of protecting Information and Communication Technology (ICT) infrastructures. The FORWARD initiative aims at identifying, networking, and coordinating the multiple research efforts that are underway in the area of cyber-threats defenses, and leveraging these efforts with other activities to build secure and trusted ICT systems and infrastructures.

Resilience aspects

Concerning resilience of the eCommunications network – the National Policy on Electronic Communications (National Telecommunications Policy) highlights that an objective is to in the case of any unpredictable crisis (such as a natural disaster) causing the mass malfunction of traditional communications links, is to install as fast as possible

---

[13] *Top Level Domain*
[14] *http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_1H2009.pdf*
[15] *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.*
[16] *See: http://www.mosr.sk/data/files/795.pdf*
[17] *See: http://www.ict-forward.eu/home*

the alternative communications links based on the rules defined in advance. The rules of installation of alternative communications should be determined before the crisis occurs, whereupon the essence of crisis management consists in preparation to crisis situations. When a crisis occurs, the procedure is performed according to the decisions of the crisis management, utilising the procedures, plans and means which have been prepared in advance.

Privacy and trust

Status of implementation of the Data Protection Directive [18]

The Data Protection Directive has been implemented by Act No. 428/2002 Coll. on the Protection of Personal Data dated 3 July 2002, as amended by Act No. 90/2005 Coll. (the "Act" or the "DPA").

The competent national regulatory authority on this matter is the Office for the Protection of Personal Data (Úrad na ochranu osobných údajov) (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. In particular, it only applies to individuals as opposed to legal entities.

In practice, the Office often interprets the definition of personal data more narrowly and only considers that information (a set of information) can be personal data if the individual is either identified or identifiable based on such particular (set of) information (and not other information that might be held by the data controller now or in the future).

This interpretation is demonstrated, inter alia, from the most recent Report on Data Protection in the Slovak Republic. However, this approach has not been tested by the Slovak courts yet. As the interpretation of the Office does not correspond to the Opinion on Personal Data and departs from the statutory definition under the DPA, it remains highly controversial.

Under the DPA, sensitive personal data includes: (i) the standard types of sensitive personal data; (ii) national identification number; (iii) information on psychological identity or psychological ability to perform work; (iv) biometric information; and (v) information about breaches of criminal or civil law and the enforcement of the respective judgments.

Biometric data can be processed if data subjects have agreed to such processing in a written form, or under a special law and processing by the data controller stems from such law. This restriction does not apply where a special registration requirement in respect of the biometric data processing applies (in such case, the biometric data processing is approved by the Office).

Sensitive personal data may be processed if conditions which substantially follow the standard conditions for processing sensitive personal data are met. However, these are interpreted very restrictively in practice. In addition, it should be noted that consent to the processing of sensitive personal data must be in writing.

---

[18] *https://clientsites.linklaters.com/Clients/dataprotected/Pages/Slovakia.aspx*

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

Both the data controller and the data processor are responsible for compliance with the general data security obligations. When taking the appropriate measures, the following must be taken into consideration: (i) the technical means that may be used; (ii) the extent of risks that may negatively impact the safety or functionality of the information system; and (iii) the confidentiality and importance of data that are processed. In certain cases, the technical and organisational measures are to be implemented by the data controller and the data processor in the form of a security project.

Data protection breaches

The data protection officer must inform the data controller of each breach of the DPA. If the data controller does not, without undue delay, remedy the breach, the data protection officer must notify the Office of such breach.

Enforcement

The Office has broad powers to take various enforcement actions, including the power to issue remedy measures imposing obligations upon the data controller or data processor and the power to impose penalties.

Prosecutions for criminal offences are brought by the prosecutor's offices before the Slovak courts, which can impose criminal sanctions.

Civil law remedies can be sought by the affected individuals before the Slovak courts.

NIS awareness at the country level

Awareness actions targeting the consumers/citizens and the industry

In Slovakia different portal websites have been launched concerning computer security and networking. These webportals are gateways to all news and highlights in Slovakia and surrounding/other countries. An example of such a community website is NewOrder[19].

The EU Safer Internet Programme is also active in Slovak under the name www.zodpovedne.sk. The zodpovedne.sk project has animated story tales as prevention against Internet, mobile and new technology risks with a focus on young children, www.ovce.sk.

The Kry Sa! project aims at rising awareness of Internet users about the security risks connected with internet usage, Internet banking and PC usage in general. Project lasted three months in the form of publishing technical/scientific articles, interviewing security professionals and discussions. The project continues through maintaining website providing online advice.

Currently there are no ongoing initiatives with regards to raising awareness for the ISP target group. To date there has not been any official programme with regards to raising awareness in users of the local government.

[19] *http://neworder.box.sk/*

National Security Authority - the magazine DSM - Information Security Survey in Slovak Republik 2008[20]

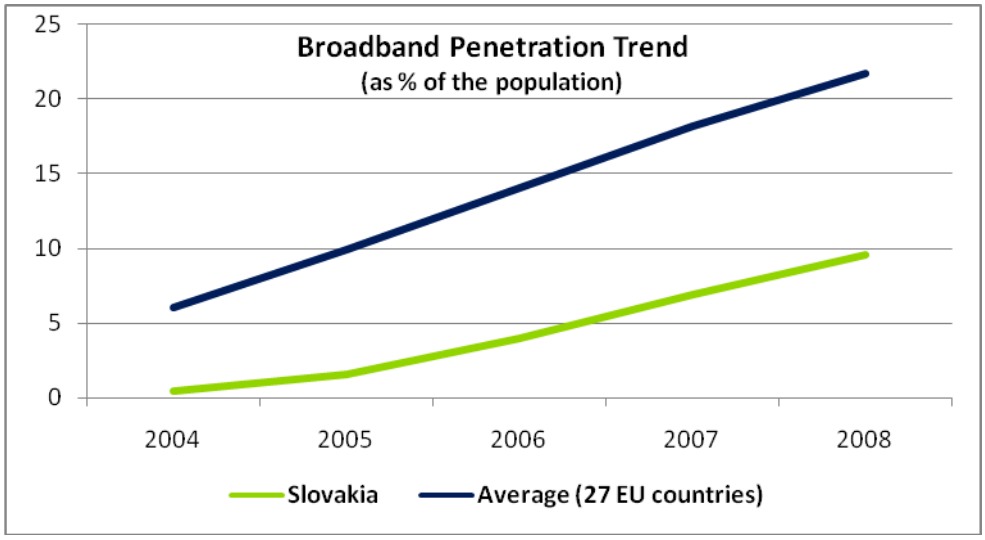
This publication compares and evaluates which paths information security has trodden since the last survey performed in the Slovak Republik in 2006. The survey provides a basic idea of preparedness and information security development across the whole territory of the EU, with all the risks, threats and possibilities which this integration brings with it.

The surveys contains topics such as importance of Information security, organisational security, security policy and standards, internet, disaster and recovery plans, security solutions, electronic signatures, personal data and confidential material security, ...

Relevant statistics for the country

In order to provide an overview of recent IT developments in the Slovak Republic, we present a few indicators in this section. The indicators show the current IT market development stage as they clearly have an impact on network and information security (NIS) aspects.

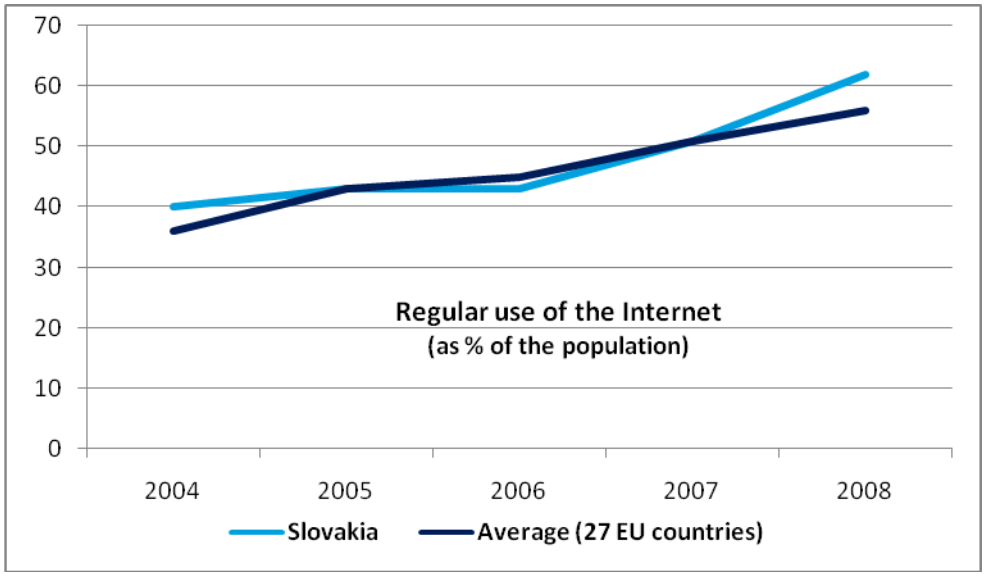
Based on the Eurostat[21] information, it appears that the broadband penetration trend for Slovakia is below the EU average but it continues on an increasing path:



Based on the same source of information, the regular use of Internet by the population (use as % of the population) is in line with the EU average. Rates of Internet usage have been gradually improving over the last few years:

[20] *http://www.dsm.tate.cz/en/psib-sr-2008/*

[21] *Source: Eurostat*


70
60
50
40
30
20
10
0
Regular use of the Internet
(as % of the population)
2004
2005
2006
2007
2008
Slovakia
Average (27 EU countries)

APPENDIX

National authorities in network and information security: role and responsibilities

National authorities	Role and responsibilities	Website
1. Ministry of the Economy, Directorate for Electronic Communications	The Electronic Communications Directorate draws up proposals for sectoral laws and the implementation of regulations in the area of post, electronic communications, digital signatures and related areas working together with the Post and Electronic Communications Agency.	http://www.mg.gov.si/index.php?id=6250&L=1#c9296
2. Ministry of Finance	The Ministry of Finance is linked to Information society and NIS in the area of non-classified information. The main effort of the Ministry management is to ensure harmony of public administration receipts and expenditures with macroeconomic and strategic objectives of Government policies, monitoring their efficient use, the fiscal consolidation and long-term sustainability of public finance within the eurozone, compliance with the rules of public funds spending, efficient implementation of EU financial instruments and other forms of foreign assistance while complying with the principles of good financial governance, developing informatisation of society, reducing the tax burden for low- and medium-income groups, reducing tax and customs evasion, and suppressing grey economy.	http://www.finance.gov.sk http://www.mfsr.sk
3. Ministry of the Interior	Ministry of the Interior is responsible for: protecting the constitutional system, public order, security of persons and property, governance of private security services, identity cards (eID), travel documents and driving licences, police force, fire fighting and rescue units.	http://www.minv.sk
4. Ministry of Transport, Posts, and Telecommunications	The Ministry of Transport, Posts, and Telecommunications is primarily responsible for coordination and fulfilment of national policy for electronic communications, National table of Frequency Allocations of the Slovak Republic, Digital Broadcasting, Broadband Access and Research Projects concerning Telecommunications.	http://www.telecom.gov.sk/index/index.php?lang=en
5. Government Plenipotentiary for Information Society	The Government Plenipotentiary for Information Society is responsible for the Information Society coordination.	http://www.government.gov.sk
6. The Office for Personal Data Protection	The Personal Data Protection Office as a state body participates in protection of fundamental rights and freedoms of persons in the course of processing their personal data. The Office performs its tasks and duties indecently and in course of the law. Its tasks include: continuous inspection of the state of personal data protection, recommendations for the measures of personal data protection in the filing systems, issuing a binding decision in the case of doubts, provides inspection of the processing of personal data in the filing systems, imposes sanctions in the case of a breach, executes registration of filing systems and provide access to the registration, issues generally binding legal regulations within the scope of its power, and gives opinions on draft laws and other generally binding legal regulations, which regulate processing of personal data.	http://www.dataprotection.gov.sk
7. National Security Authority	The National Security Authority is responsible for the protection of classified information. It provides support in domain of information security and information systems	http://www.nbusr.sk

National authorities	Role and responsibilities	Website
	certification, crypto – security and crypto - certification, personal security, R&D, and administrative security for the Slovak Republic. The National Security Authority is also the electronic signature scheme root certification authority for Slovakia.	
8. Telecommunications Office	The Telecommunications Office is the Electronic communications regulatory body. The main activities of the office comprise carrying out state regulation of electronic communication, managing the frequency spectrum, maintaining international relations with regulatory authorities in the area of electronic communications, cooperating with the Council for Broadcasting and Retransmission, exercising state supervision, and imposing sanctions in the electronic communications field.	http://www.teleoff.gov.sk
9. Institute of Security and Defence Studies of MoD SR	The Institute of Security and Defence Studies of MoD SR is responsible for the professional preparation of documentation for decisions to be taken in the area of security, defence and crisis management.	http://www.mosr.sk
10. Commission for Information Security	The Commission for Information Security is a working group consisting of employees of Ministry of Finance and external experts in the field of information security. The Commission for Information Security is responsible for the evaluation of proposed security standards for protection and security of public administration information systems in the scope of non-classified information, proposals of security standards, change or modification of existing security standards for security of public administration information systems, presentation of expert opinion concerning norms and legislation related to NIS, and appointing working groups so that the NIS-related tasks could be carried out .	http://www.finance.gov.sk/Default.aspx?CatID=5797&ContentID=2285%22%20target=_self http://www.informatizacia.sk/vdok_simple-zoznam-clenov-komisie-pre-ib/616s3247c

Computer Emergency Response Teams (CERTs): roles and responsibilities

Slovakia is currently in the process of deploying a national CERT. The CERT.SK was established in July 2009 and is currently in a preparation phase to be operational. The estimated operating date is in January 2010. The budget for the national CERT.SK is allocated from the Government. The responsible national authority for the national CERT.SK is a department in the Ministry of Finance.

No other CERTs have been identified for Slovakia.

Industry organisations active in network and information security: role and responsibilities

Industry organisations	Role and responsibilities	Website
11. ITAS (IT Asociacia Slovenska)	IT Association Slovakia (ITAS) is an association representing local and international companies operating in ICT in Slovakia. ITAS was founded in 1999 and presently has 65 members. It is a member of EICTA.	http://www.itas.sk

Industry organisations	Role and responsibilities	Website
12. Slovak Association for Information Security (SASIB)	The goal of the organization is to increate knowledge and awareness of security legislation and expert knowledge of its members in the domain of progessionals and public in information security and software protection. SASIB supports the NIS research activities of government and public administration, and prepares recommendation in the field of NIS and cyber-crime.	http://ww.sasib.sk

Academic organisations active in network and information security bodies: role and responsibilities

Academic organisations	Role and responsibilities	Website
13. Department of Computer Science, Faculty of Mathematics, Physics and Informatics, Comenius University	The department, established in 1974, continues to be responsible for organizing the major part of the undergraduate and graduate computer science education to this date. The distinguishing feature is a balanced coverage of the mathematical foundations, theoretical computer science, and practical computer science. The faculty covers courses on computer architecture, system software, networks, databases, software design, design and analysis of algorithms, formal languages, computational complexity, discrete mathematics, cryptology, data security and others. NIS related courses: Cryptography. A faculty professor is a member of the Commission for Information Security that acts as an expert group in developing national security policy and security standards for public information systems.	http://www.dcs.fmph.uniba.sk
14. Faculty of Informatics and Information Technologies, Slovak University of Technology in Bratislava	The faculty is one of the most successful, largest and the most experienced (opened in 1941) technical faculty aimed at electrical engineering, information and communication technologies in Slovakia. In the NIS area it cooperates closely with security professionals in the project based education form. NIS with related courses: Cryptography in communication networks, Information security, Classical cryptography.	http://www.fiit.stuba.sk/generate_page.php?page_id=749
15. Faculty of Electrical Engineering and Informatics, Technical University of Kosice	The Faculty of Electrical Engineering and Informatics of the Technical University of Kosice is focused on NIS research.	http://www.fei.tuke.sk
16. Faculty of Special Engineering (University of Zilina)	The Faculty of Special Engineering handles the topics of civil and social security . The Faculty has special courses in the area of Risk Management & Cyber Protection.	http://fsi.uniza.sk/_english/index-en.html

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

Others	Role and responsibilities	Website
17. Magazine DSM - Data Security Management and TATE International Slovakia	DSM (Data Security Management) magazine was established in the second half of 1997 as a result of the efforts of Tate International, s.r.o. to create a professional-level periodical magazine, which would bring high quality and up-to date information on the status and development in the area of information security.	http://www.dsm.tate.cz/en/

Others	Role and responsibilities	Website
18. ISACA	ISACA is a Worldwide association of IS professionals dedicated to the knowledge and good practices regarding audit, control, and security of information systems. The ISACA chapter in the Slovakia organizes local events such as education and training, workshops, roundtables and other specific events.	http://www.isaca.sk
19. ZSS (Association of Slovak Consumers)	A consumer organisation, its aim is to protect and educate consumers.	http://www.zss.sk

Country specific NIS glossary

Broadband Penetration Indicator	Number of total subscriptions to broadband connections (households, enterprises, public sector) by platform (DSL, all others) divided by the number of inhabitants. 3G subscriptions are not included in the total. Source: European Commission.
CCD COE	Cooperative Cyber Defence Centre of Excellence
CPAP	Central Public Administration Portal
DPA	Data Protection Act
NPEC	National Policy on Electronic Communications
Personal Data	The definition of personal data in the Slovak DPA is closely based on the standard definition of personal data. In particular, it only applies to individuals as opposed to legal entities. In practice, the Office often interprets the definition of personal data more narrowly and only considers that information (a set of information) can be personal data if the individual is either identified or identifiable based on such particular (set of) information (and not other information that might be held by the data controller now or in the future). This interpretation is demonstrated, inter alia, from the most recent Report on Data Protection in the Slovak Republic. However, this approach has not been tested by the Slovak courts yet. As the interpretation of the Office does not correspond to the Opinion on Personal Data and departs from the statutory definition under the DPA, it remains highly controversial.

References

- Slovak Republic National Policy on Electronic Communications, available at http://www.teleoff.gov.sk/data/files/355.pdf
- 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
- Global Phishing Survey: Trends and Domain Name Use 1H2009, available at http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_1H2009.pdf
- Iceland - ENISA CERT Directory: http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country/slovakia

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