Hungary Country Report

enisa
European Network and Information Security Agency

www.enisa.europa.eu

About ENISA

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

Contact details

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

Mr. Giorgos Dimitriou

ENISA External Relations Expert

Giorgos.Dimitriou@enisa.europa.eu

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

Acknowledgments:

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

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

Legal notice

Table of Contents

Hungary

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 on the following Network and Information Security (NIS) related topics:

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

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

NIS national strategy, regulatory framework and key policy measures

Overview of the NIS national strategy

The New Hungary Development Plan (2007-2013)

The New Hungary Development Plan (text in English) was elaborated under the National Strategic Reference Framework of Hungary (NSRF) for 2007 - 2013 and was approved by a decision of the European Commission in May 2007. The NSRF is co-financed by the European Regional Development Fund, the European Social Fund and the Cohesion Fund. Planning, management and implementation is done by the National Development Agency (*Nemzeti Fejlesztési Ügynökség, NFU*), in co-operation with the ministries concerned and the development regions. Unlike the previous plan covering 2004 - 2006, the new plan has placed more emphasis on the information society and inclusion. Priority 6 supports the promotion of an information society for all.

Social Renewal is one of the priorities of the new plan, which stipulates the need for social integration of those with a disadvantaged background, amongst others the Roma, the old, the poor and the disabled. These groups are by the plan considered as being also digitally excluded, along with other groups such as women, the least educated, the unskilled, the unemployed and those living in poorly developed regions and municipalities.

To this end, particular attention has been paid to the promotion of active social participation and to equal access to a barrier-free environment facilitating communication. The significance of ensuring access to information and the information society has been laid down as a horizontal priority action.

Specific reference is made in page 106 to enhance participation by eliminating physical and info-communication obstacles. eInclusion is seen as the support of access to and the use of info-communication equipment and online services.

Realisation of the plan is via operational programmes. Of those, programmes relevant to eInclusion are:

- The Social Renewal Operational Programme[1](*Társadalmi Megújulás Operatív Program*) stipulates that particular attention should be paid to the promotion of active social participation, to equal access to a barrier-free environment and to the facilitation of communication. The significance of ensuring access to information is also addressed by the document;
- The Social Infrastructure Operational Programme[2] (T*ársadalmi Infrastruktúra Operatív Program*) seeks to create the physical infrastructural background required for the successful implementation of the interventions of the previous programme on social renewal so as to ensure equal access to quality services. Among others, it stipulates the development of IT infrastructure for schools, education and content-creation.

[1] *More details about The Social Renewal Operational Programme available at http://www.nfu.hu/doc/924*
[2] *More details about Social Infrastructure Operational Programme available at http://www.nfu.hu/doc/925*

NIS strategy, part of the National Security Strategy of the Republic of Hungary

Since the beginning of 2010 the protection of important information systems and critical information infrastructures is still an integral part of the National Security Strategy of Hungary. The challenges of the information society and the vulnerabilities of the new communication technologies are explicitly mentioned as risk factors for the country [3].

The National Security Strategy also clearly points out the need for collaboration with international and private partners in the field of protection of information systems which is the successful protection of information systems requires close co-ordination with allies, as well as information and telecommunication providers and research centers.

Additionally, it was stated that an overall risk management process regarding resilience of public e-communication networks would not be possible and could not work. In Hungary, a risk management plan is obligatory for all assigned companies active in the IT sector. Also, a risk management process has been established for all eGovernment areas. However, Hungary does not have a national risk management process.

Additionally, in order to keep the preparedness and recovery measures to mitigate risks up to date, regular big national exercises are held with all players in the telecom sector. Such a big exercise takes place at least every third year. Smaller dedicated exercises are carried out regularly in-between. These exercises might cover, for example, the interdependencies between telecommunication and energy, oil, gas etc. In every sector, specific scenarios for recovery measures have been developed.

The public telecommunication sector in Hungary does not have formal priority services. Only some informal prioritisation guidelines exist. All assigned telecom providers are obliged to have emergency recovery and business continuity plans. These are controlled by National Communications Authority Hungary[4] visiting providers on site. As a recent flood in Hungary has shown, all big providers ensure basic services in their domain in real incidents without posing any problems.

The Hungarian Information Society Strategy

The Hungarian Information Society Strategy consists of two pillars: the introduction of information technologies into (economic) processes, and the implementation of public electronic services.

Information security and the protection of privacy are seen as essential parts of the development towards an information society, since the extent to with ICT is used is determined by the extent to which people trust new technology. The strategy therefore identifies IT security[5] as a field of governmental intervention and highlights the necessity of regulatory, organizational, and technological measures.

"E-Public Administration 2010" Strategy[6]

The objective of the Strategy is to define a general vision of future eAdministration for all stakeholders and provide a uniform framework for the detailed objectives of developments for the years to come. In addition, the document defines the most important strategic factors influencing

---

[3] *Source: http://www.crn.ethz.ch/publications/crn_team/ciip_by_chapter/partI/hungary.pdf*
[4] *Note: Please note that the National Communications Authority Hungary had been replaced with National Media and Infocommunications Authority once with the Hungary government change from summer of 2010.*
[5] *Source: http://www.crn.ethz.ch/publications/crn_team/ciip_by_chapter/partI/hungary.pdf*
[6] *Source: http://www.epractice.eu/en/document/288260*

the realisation of the objectives and encompasses all those substantive areas that institutions must take into consideration when developing their own services. This strategy also defines horizontally and vertically integrated as well as overall programmes that form a foundation and/or foster the systemic operation of the most important elements of eAdministration as regards the Government as a whole.

There are **4 key fields** of the strategy:

- Modernisation of the public services for the citizens, enterprises and the Public Administration;
- Introduction of integrated services for the governmental institutions, back offices in order to promote a transparent and effective Public Administration;
- Contribution to the spread of the professional eGovernment knowledge at leadership level and implementation;
- Development of the eGovernment adaptability especially of those enterprises and citizens in the area of IT.

Broadband policy

The aim of the government, as expressed in the most recent **Digital Renewal Action Plan**[7] (*Digitális Megújulás Cselekvési Terv*) for 2010 - 2014, is the achievement of full broadband coverage.

The main broadband policy document is the National Broadband Strategy[8] (*Nemzeti Szélessávú Stratégia*), which covers the period 2005 - 2013 and which set the aim of increasing broadband access with a target of 90 % residential broadband coverage by the end of 2008 and full coverage by the end of 2010. Offering more relevant content and providing the preconditions for equal opportunities (eInclusion) for the disadvantaged groups were stated as other priorities, realised via specific objectives, such as:

- Digital illiteracy targets, set to a drop below 50 % by 2008 and below 33 % by 2013;
- IT equipment for the visually impaired;
- Support for procurement of IT equipment to be used for education, including minorities;
- Promotion of the use of Internet among children;
- Creation of e-work jobs.

[7] *The Digital Renewal Action Plan available (only in Hungarian) at* http://www.nfm.gov.hu/data/cms2089529/Digitalis_Megujulas_Cselekvesi_Terv.pdf
[8] *The National Broadband Strategy available at* http://www.vus.sk/broadband/nbbs/hu_nbbs.pdf

The regulatory framework

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

eGovernment Legislation[9]

Similar to 2009, there is currently no specific overall eGovernment law in Hungary. However, a number of eGovernment regulations are laid down in Government decrees and resolutions passed between 2004 and 2009.

Government decree 223/2009 on the security requirements of the e Government (amongst others, on the creation of the Hungarian National Cyber Security Centre)

The Hungarian National Cyber Security Centre ("the Centre") is an accredited member of the international organisation specialised in cyber security and the protection of critical information infrastructures, which protects the services of the central government system against attacks coming from the internet. In this scope, the Centre pursues activities relating to technical protection, prevention and awareness rising. Moreover, it represents Hungary in international co-operations and organisations specialised in cyber security and the protection of critical information infrastructures.

The Centre also participates in the preparation of strategies and regulations relating to information and network security and the protection of critical information infrastructures. The Minister heading the Prime Minister's Office exercises control of the Centre, its operation is supervised by the Information Security Supervisor of the Government.

The Centre is operated by the Theodore Puskás Government Foundation on the basis of a public service agreement, concurrently with the cooperation of the National Alert Service for Informatics and Communications.

Other NIS related regulations are: Government decree 84/2007. (IV. 25.) on the security requirements of the Central Electronic Service System and the related systems; Government decree 195/2005. (IX. 22.) on security criteria of information systems used for electronic administration; Government Decree 194/2005 (IX. 22.) on the requirements of electronic signatures and certificates used in (actions of) public administration and Certification Service Providers issuing those certificates.

Data Protection/ Privacy Legislation [10]

Act No. LXIII of 1992 on the Protection of Personal Data and Disclosure of Data of Public Interest is a combined Data Protection and Freedom of Information Act. The Act sets rules and safeguards regarding the processing of personal data by public and private bodies. Its application is overseen by the Parliamentary Commissioner for Data Protection and Freedom of Information.

Government resolution 2041/2007. (III. 13.) on the necessary IT developments for the online verification of identity.

---

[9] *Source: http://www.epractice.eu/en/document/288261*

[10] *Source: http://www.epractice.eu/files/eGovernment%20in%20HU%20-%20Sept%202009%2012.0.pdf . The same source was used for multiple laws and regulations indicated in this section.*

eCommerce Legislation

Since the beginning of 2010 the legislation applicable in Hungary relevant for eComerce is:

- Decree of the Ministry of Justice 25/2006. (V. 18.) on the electronic paying of fees as for public notices in the administration of business processes;
- Decree of the Ministry of Finance 46/2007. (XII. 29.) on the electronic invoice;
- Act No. XCVII. of 2003 on the modification of the Act No. CVIII. of 2001. on certain legal aspects of Information Society services, in particular electronic commerce;
- Decree of the Ministry of Justice 24/2006. (V. 18.) on certain aspects of the electronic business registration procedure and the electronic business register;
- Decree of the Ministry of Finance 24/1995. (XI. 22.) on the identification of invoices, simplified invoices and receipts for tax administration, as well as on the application of cash registers and taxameters ensuring the issuance of receipts;
- Act No. CVIII. of 2001 on Electronic Commerce and Information Society Services. Adopted on 18 December 2001, the Act implements EU Directive 2000/31/EC on certain legal aspects of Information Society services, in particular electronic commerce. The Act governs the eCommerce legal relationships of individuals, legal entities and organisations without legal personhood, where the service is provided for or from the territory of the Hungarian Republic.

eCommunications legislation

The Act on Electronic Communications

Also applicable for 2010 the Act 2003.C on Electronic Communications (*2003. évi C. törvény az elektronikus hírközlésről*) implemented the European Universal Service and Directive 1999/5/EC on Radio and Telecommunications Terminal Equipment.

The Act aims to take into consideration the needs of the disabled and the low-income users. To this end, it postulates that:

- Subject to other regulations, some types of radio devices and electronic communications terminal equipment might be required to be accessible to disabled persons;
- At least 3 % of the mandatorily installed public payphones shall be such as to be accessible to those with impaired hearing or movement.

eSignatures Legislation

Since the beginning of 2010 no changes were noted related to the Hungarian eSignature legislation and eIdentification/ eAuthentication.

Act No. XXXV. of 2001 on Electronic Signature. The Act on Electronic Signature was adopted on 29 May 2001 and entered into force on 1 September 2001. It creates a legal framework for the provision of certified electronic communication and data transmission in business, public administration and other areas of life affected by the information society.

The regulatory mandate of the Hungarian National Communications Authority Hungary also extends to information technology[11]. Responsibilities here include official activities in regard to electronic signatures and unsolicited electronic advertising; the regulatory tasks related to informatics and information society and also the public administration service of root certification.

[11] *See the document "The National Communications Authority of Hungary and the Hungarian Electronic Communications Market" available at: http://www.nhh.hu/dokumentum.php?cid=14073*

Additional aspects on the regulatory framework[12]

An interesting specific aspect of Hungary is that the Ministry of Informatics and Communications launched the Hungarian Information Security Evaluation and Certification Scheme (MIBETS). MIBETS is aimed to assist in evaluating and testing the security of software.

In addition, the ministry introduced the Information Security Management Framework (*Magyar Informatikai Biztonság Irányítási Keretrendszer - MIBIK*), which aims to evaluate security measures at the organizational level. The current government scheme includes an updated version of the MIBETS and MIBIK, now jointly abbreviated as MIBA.

Government IT systems must be in compliance with the recommendations of the scheme, and a supervisory body began operating within the Prime Minister's Office Electronic Government Centre[13] already as from the first half of 2008.

Self-regulations

Hungarian Mobile Telephone Service Providers Self-Regulation Code for Safer Mobile Telephone Use by Young Teenagers and Children [14]

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

[12] *Source: http://www.crn.ethz.ch/publications/crn_team/ciip_by_chapter/partI/hungary.pdf*
[13] *Note: Please note that the Electronic Government Centre was active until mid 2010 and doesn't exist anymore since summer 2010. The institution has been dissolved once with the Hungary government changes.*
[14] *Source: http://www.gsmeurope.org/documents/eu_codes/hungary1.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	• MEH EKK (Prime Minister's Office, Electronic Government Centre) • Ministry of Transport, Telecommunications, Energy • National Media and Infocommunications Authority (former National Communications Authority Hungary) • National Bureau of Investigation • Data Protection Commissioner of Hungary • Parliamentary Informatics Commission • Ministry of Defence • Ministry of Justice and Law Enforcement • National Cyber Security Centre • NACPH-OFE (National Association for Consumer Protection in Hungary)
CERTs	• CERT-Hungary • HUN-CERT SZTAKI • NIIF-CSIRT
Industry Organisations	• IVSZ (Hungarian Association of IT Companies) • eSec.hu (Hungarian Cyber Security Package) • Melasz (Hungarian Association for Electronic Signature) • Inforum • Association of Hungarian Content Providers • Hungarian IT Security Centre • MATISZ – Hungarian Association of Content Industry
Academic Organisations	• BME CIT (Budapest University of Technology and Economics/ Laboratory of Informatics/ Centre of Information Technology) • NIIF-CSIRT
Others	• Internethotline • Biztonsagos Internet (Safe Internet) • BIF (Friendly Internet Forum) • NHIT (National Telecommunications and Information Council) • MSZT (Hungarian Standards Institution) • ISACA Local Chapter • Critical Information Infrastructure Protection Workgroup (KIIV) • OWASP local chapter

For contact details of the above-indicated stakeholders we refer to the ENISA "Who is Who"[15] – 2010 Directory on Network and Information Security and for the CERTs we refer to the ENISA CERT Inventory[16].

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.

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

[16] 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

Hungarian National Interoperability Framework (HNIF)

The first version of the Hungarian e-Public Administration Framework - Hungarian National Interoperability Framework (HNIF) was published by the Public Administration IT Committee in March 2009. The HNIF was published as a recommendation and the government passed a decree about its compulsory use for electronic public service providers.

The Hungarian e-Public Administration 2010 Strategy gives priority to interoperability.The aim of the strategy is twofold:

- Develop the skills of citizens and enterprises in applying e-administration building on the available technological foundation;
- Increase e-administration service efficiency.

The main objective of the HNIF is to define standards, requirements and regulations which guarantee the solid technical-semantic, monitoring, project management, IT security and application development methodology platform for the expansion and operation of electronic public administration.

Ensuring the fulfilment and consistent enforcement of these aims give adequate guarantee to having an interoperable, secure and up-to-date electronic public administration system, as a result of the development of independently launched departmental and local governmental subsystems.

At present, the coordination and maintenance processes of the HNIF have been defined, but not yet implemented. Proposed processes include best practice capturing and sharing, lifecycle and change management on the framework, as well as the creation of an expert group. There is no supporting infrastructure yet.

Proposed is a repository, which will be used for the publication of standards, requirements, specifications, recommendations and other informative materials necessary for the development and operation of services that fall under the HNIF.

Co-operation via the Electronic Government Centre (MEH EEK)

Part of the Prime Minister's Office; cooperates with Data Protection Commissioner of Hungary; National Communications Authority Hungary; Ministry of Transport, Telecommunications and Energy; NHIT; National Telecommunications and Information Council; National Association for Consumer Protection in Hungary (NACPH-OFE); and Hungarian Association of IT Companies (IVSZ).

Co-operation via the National Bureau of Investigation

Cooperates with the Prime Minister's Office; Electronic Government Centre (MEH EKK); and with the dedicated division within the Hungarian National Police.

Co-operation via the Ministry of Transport, Telecommunications, and Energy

Cooperates with the Data Protection Commissioner of Hungary, National Communications Authority Hungary; NHIT, National Telecommunications And Information Council, National Association for Consumer Protection in Hungary (NACPH-OFE), CERT-Hungary, Ministry of Transport, Telecommunications, and Energy; and Barátságos Internet.

Co-operation via the Parliamentary Informatics Commission

Cooperates with the Prime Minister's Office and Electronic Government Centre (MEH EKK).

Co-operation via the MSZT – Hungarian Standards Institutions

Cooperates with Prime Minister's Office; Electronic Government Centre (MEH EKK); Ministry of Transport, Telecommunications and Energy and National Communications Authority Hungary.

Co-operation via the National Association for Consumer Protection in Hungary (NACPH-OFE)

Cooperates with the Prime Minister's Office, Electronic Government Centre (MEH EKK), Ministry of Transport, Telecommunications, Energy and National Communications Authority Hungary.

Co-operation via the Hungarian Association of IT Companies (IVSZ)

Cooperates with the National Communications Authority Hungary; Prime Minister's Office; Electronic Government Centre (MEH EKK), Internet hotline, NHIT, and National Telecommunications and Information Council. Concerning the exchange of information between stakeholders, the National Communications Authority Hungary keeps contact with providers on information security policies. However not clear exchange mechanism are in place in the area of information on geographical and topological network structures.

The network databases of the different stakeholders differ and are not compatible. Therefore, a large amount of data and information is collected and available but it cannot be assessed in a structured way.

Other co-operation aspects

The telecom and competition authorities entered into an overall agreement for the protection of the electronic communications market and compliance with its applicable legislation. The national CERT signed cooperation agreements with the national telecom and financial regulator and with most major Hungarian players.

The Hungarian Police has separate cooperation agreements with the largest service providers – the details are not public. The Police experts in this field have personal and informal contacts with the representatives of the network and service providers.

Fostering a proactive NIS community

International co-operation via the European Government CERTs (EGC) group

CERT Hungary is amongst the active members[17] of the European Government CERTs (EGC) group. ECG is an informal group of governmental CSIRTs that is developing effective co-operation on incident response matters between its members, building upon the similarity in constituencies and problem sets between governmental CSIRTs in Europe. To achieve this goal, the EGC group members:

- Jointly develop measures to deal with large-scale or regional network security incidents
- Facilitate information sharing and technology exchange relating to IT security incidents and malicious code threats and vulnerabilities
- Identify areas of specialist knowledge and expertise that could be shared within the group
- Identify areas of collaborative research and development on subjects of mutual interest
- Encourage formation of government CSIRTs in European countries
- Communicate common views with other initiatives and organizations.

Bilateral cooperation between CERT Hungary and the Slovak GovCERT (CSIRT.SK)

In 2010 CERT Hungary performed a formal bilateral meeting together with the Slovak GovCERT - CSIRT.SK in Budapest. The bilateral meeting was held at Theodore Puskas Foundation, host of the National Cybersecurity Center.

The aim of the consultation was to introduce the two national governmental CERT structures, find common points of interest for cooperation, and to support CSIRT.SK in gaining international memberships to the main CSIRT forums.

International co-operation via the Cooperative Cyber Defence Centre of Excellence (CCD COE)

Hungary is participating in the Cooperative Cyber Defence Centre of Excellence (CCD COE) together with other sponsoring nations: Estonia, Germany, Italy, Latvia, Lithuania, the Slovak Republic 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.

Cyber Europe 2010

During 2010 Hungary took part in the first pan-European exercise on critical information infrastructure protection, Cyber Europe 2010, organized by EU Member States and jointly supported by the European Network Security Agency (ENISA) and the EU's Joint Research Centre (JRC). This exercise is part of the measures stipulated by the Digital Agenda for Europe (strategy launched by the European Commission) in order to increase confidence in the Internet and improve network security.

---

[17] *The members of the European Government CERTs group include: Austria - GovCERT.AT, Finland - CERT-FI, France – CERTA, Germany - CERT-Bund, Hungary - CERT-Hungary, Netherlands - GOVCERT.NL, Norway – NorCERT, Spain - CCN-CERT, Sweden - CERT-SE, Swiss - GovCERT.ch, United Kingdom – CSIRTUK, United Kingdom – GovCertUK; See more details at: http://www.egc-group.org/*

The exercise scenario called Cyber Europe 2010 foresaw the gradual loss or considerable reduction of Internet connections between European countries and in the worst case, the effective cancellation of the main cross-border connections in Europe. The objectives of the exercise were:

- To establish trust in between actors within the Member State, and between the Member States (MS);
- To increase understanding of how management of incidents is done in different MS across Europe;
- To test the communication channels, communication points and procedures in the MS/between MS;
- To highlight interdependencies between MS across Europe;
- To increase mutual support procedures during incidents or massive cyber attacks.

Participants in Cyber Europe 2010 were only public authorities of EU Member States. The players involved include ministries, national regulatory agencies, CIIP and information security related organisations, and national computer security incident response teams (CSIRTs). Hungary has been represented by CERT Hungary.

This experience has shown that even at the national level, Hungary is need to do plenty of information security incident management, critical information infrastructures security coordination at government level to develop rules of procedure, and some development of national information security functions, and those based on the preparations for the conservation practices based on ability maintenance.

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

Security incident management

During the course of 2010, the CERT Hungary is still the national coordination point and coordinates all actions against attacks - CERT-Hungary is ready to handle incidents 24 hours a day, 365 days a year. At the international level, CERT Hungary cooperates with various networks, associations and with centres in other countries.

CERT-Hungary assist system administrators in handling the technical and organizational aspects of incidents. In particular, it provides assistance or advice with respect to the following aspects:

- **Incident Triage**: investigating whether indeed an incident occurred, determining the extent of the incident;
- **Incident Coordination**: determining the initial cause of the incident (vulnerability exploited); facilitating contact with other sites which may be involved; facilitating contact with law enforcement, if necessary; making reports; composing announcements to users, if applicable;
- **Incident Resolution**: analysing and if possible removing the vulnerability; securing the system from the effects of the incident; collecting evidence where criminal prosecution, or community disciplinary action, is contemplated;
- **Intrusion Detection Services**
- **Security Audits:** CERT-Hungary offers security audits on information technology systems. CERT-Hungary helps its clients get ready for the worst by providing business continuity and disaster recover planning solutions, so when a problem disrupts normal business operations, they will be among the first ones to get back to normal operations;
- **Development of Security Applications**: CERT-Hungary can also be commissioned to install, configure, maintain or even develop security applications, to evaluate the security of software applications, hardware, or IT services to help supported organisations choose the best products available;
- **Malware Analysis**
- **Technology Watch**: CERT-Hungary can determine the need for a new security tool, and develop effective deployment methods for its clients.
- **Security Consultancy**: CERT-Hungary, with the support of its external experts, can give advice on any security issue to its clients. The 70-30 rule is still effective, which means that most Security threats are coming from inside the organization, CERT-Hungary can provide educational materials and hold training sessions for their constituents, so employees and managers become part of the security, instead of being a security risk.

In addition, CERT-Hungary collects statistics concerning incidents which occur within or involve its constituency, and will notify the community as necessary to assist it in protecting against known attacks. As regards to incident reporting, a decree states that network incidents must be reported and gives the structure for incident reporting, and specifications about critical incidents.

Accordingly, the report must address the following topics:

- Nature of the incident;
- Persons injured if any;
- Financial damage;
- Measures taken to rectify the situation;
- Expected time for recovery;
- The number of subscribers affected, etc.

The CERT Hungary uses the Traffic Light Protocol. Incident information that is sensitive (but unclassified) is labelled using the TLP. Here, the originator signals how widely one wants this information to be circulated beyond the immediate recipient, if at all. CERT Hungary shares this kind of information with other government offices. National Communications Authority Hungary Relationships releases information to the press too.

In general, reporting of security incidents to the public at large is obligatory for the assigned telecom providers in Hungary. The number of users of a service affected is the most important criteria whether a public announcement is made or not. The size and number of affected networks is the criteria whether the information is published by the authority or by the telecom provider.

Incidents dealt with in the working groups are still treated confidential. No communications are made to the outside. For example, there were massive incidents (phishing attacks) in 2006 against the seven biggest banks in Hungary; the problem was communicated by the individual banks to their customers separately but not published in the media or by CERT Hungary.

No public information available on open sources on the Hungarian judicial decisions related to network and security incidents.

Emerging NIS risks

Compared to 2009 no significant changes occurred regarding the emerging NIS risk domain during 2010. No information is available on the participation of authorities, academic bodies or industry organisations from Hungary on pan-European initiatives to promote the collaboration and partnership initiatives focused on emerging NIS risks, like for instance the FORWARD[18] initiative.

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.

No relevant information was identified on the participation of Hungarian CERT, ISPs, etc in other European-wide projects aiming at identifying emerging NIS risks, like for example in the Worldwide Observatory of Malicious Behaviors and Attack Threats (WOMBAT)[19].

Resilience aspects

Similar to 2009 the good practices in network resilience have been worked out in the form of recommendations by the **Hungary National Communications Authority** and the service providers regarding business continuity and recovery measures. The eGovernment guidelines on information security and resilience are considered good practice. T

he National Communications Authority of Hungary was established in January 2004 as a public administration body with a communications market regulation mandate much wider than that of its legal predecessor the Communications Inspectorate.

[18] *See: http://www.ict-forward.eu/home*
[19] *See: http://www.wombat-project.eu/*

Privacy and trust

Status of implementation of the Data Protection Directive

The Data Protection Directive has been implemented by the Hungarian Personal Data Protection Act No LXIII of 1992 on the protection of personal data and disclosure of public information (the "DPA"). The Hungarian competent national regulatory authority on this matter is the Parliamentary Commissioner for Data Protection and Freedom of Information (the "Commissioner").

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 this respect, it only applies to information about natural persons and the information remains personal data as long as its relationship with a private individual can be maintained.

Under the DPA, sensitive personal data includes: (i) the standard types of sensitive personal data, (ii) information about criminal records; and (iii) information about addictions.

Personal data may be processed if: (i) the processing is carried out with the data subject's explicit consent; or (ii) the processing is permitted by an act of Parliament or regulation of a local municipality based on act of Parliament.

Sensitive personal data may only be processed: (i) if the data subject has given consent in writing; or (ii) in connection with sensitive data related to racial, national or ethnic origin, political opinions and any affiliation with political parties, religious or philosophical beliefs or trade union membership, if prescribed by an international treaty, or if ordered by law in connection with the enforcement of some constitutional right or for national security or criminal law enforcement purposes; or (iii) if ordered by an act of Parliament in other cases.

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

Data controllers, and within their sphere of competence, data processors, must comply with the general data security obligations. For the technical protection of personal data, the data controller, data processor or operator of the telecommunications or information technology equipment shall implement security measures, in particular, if the processing involves the transmission of data over a network or any other means of information technology.

The data controller and the data processor must enter into a written contract for the processing of personal data. Any company interested in the business activity for which the personal data is to be processed may not be contracted for the processing of such data. The DPA does not contain any obligation to inform the Commissioner or data subjects of a security breach. The data controller is responsible for compliance with the DPA.

Enforcement

Based on the report prepared by the Data Protection Commissioner for the Hungarian Parliament, there were altogether 3,953 matters (including, in connection with data protection issues, 1,079 complaints and 596 consultations) which were handled by the Commissioner's Office in 2009. In relation to penalties, the Commissioner is not entitled to order penalties as a sanction for the violation of the Hungarian DPA.

The Commissioner and the Commissioner's Office acts as the enforcement authority - the status of the Commissioner's Office and the official procedure is not subject to clear regulation. The decision

of the Commissioner can be challenged at the ordinary courts. Criminal and civil courts are competent in criminal offences and civil law sanctions in connection with data protection.

NIS awareness at the country level

Similar to 2009, Hungary can still be considered as a Member State where substantial information can be found on the NIS awareness actions and measures that can be taken by public authorities and industry actors.

Awareness actions targeting the industry

In general, there is exchange of information within the early warning system. Many working groups are in place, the ones in the banking sector and on energy and telecoms operate in the form of Public Private Partnership (PPP). In general, it can be said that the cooperation among providers is not very intensive, unless the state and public authorities initiate and promote the cooperation.

Among the initiative, we should point out the one for the promotion of network security coming in the form of CERT - Hungary's consultancy role with its constituency. Being a government CERT, the main clients include some parts of the critical information infrastructure of Hungary, such as Civil Aviation Authority of Hungary, Ministry of Informatics and Communication and National Communications Authority.

Awareness actions targeting the Internet Service Providers

Measures for increasing awareness are undertaken by the service provider industry – a summary of tasks against malicious actions, including spam, can be found in the Acceptable Use Policy (AUP) of the Council of Hungarian Internet Providers, which is compulsory for all its members.

Most ISPs take technical measures against malicious actions via filtering of spam, blocking of malware and limiting traffic, and disclose such information on their web sites. Several ISPs also have an explicit spam policy in their terms and conditions, and use it as an awareness vehicle. Additionally, several websites exist which provide spam related information. One of them is the website of the Hungarian telecom regulator.

Awareness actions targeting the consumers/citizens

Since the beginning of 2010, the ongoing www.biztonsagosinternet.hu project ("biztonsagos" means "safe") is still providing the website for the general public with information on IT security in an easy understandable manner. The project is a Hungarian adaptation of the German awareness-raising-program *BSI für Bürger* where the structure of the German model was adopted, and the texts were fitted to the Hungarian circumstances.

The website gives advice for Internet usage in general, and for e-shopping and e-banking in particular; it provides information on spam, viruses, and other threats to information security, and demonstrates how users can protect their privacy (with a special focus on child protection).

Other ongoing awareness-raising programs include www.internethotline.hu and www.baratsagosinternet.hu. Both initiatives came into being as part of the Safer Internet Program – the first operating as an internet hotline for reporting harmful and illegal content, the other being the awareness node of Hungary.

Other awareness-raising events

Several awareness-raising events are held in Hungary:

- The day of Information Security – September 28h, 2010 : Annual event for IT security under the patronage of Budapest University of Technology, focusing on current security trends, threats, and solutions [20]
- NETWORKSHOP 2010 – April 7-9, 2010: Annual event organized at the *College of Dunaújváros*, focusing on computing solutions, networking, and IT security. [21]
- *Kriminál expo 2010* – November 23-25, 2010: Annual conference organized by the Hungarian Ministry of Police about current and upcoming security threats and solutions.[22]

Country-specific activities for identifying and promoting economically efficient approaches to information security

There was identified no relevant recent information regarding country-specific activities for identifying and promoting economically efficient approaches to information security in Hungary.

Interdependencies, Interconnection and Improving Critical Information Infrastructure Protection

Regarding the Critical Information Infrastructure Protection (CIIP) and the development of the information society, the most important change was the integration of the Ministry of Informatics and Communication – which was the central body for questions related to information and communication technology – into the Ministry of Economy and Transport and the Prime Minister's Office. The major tasks of CIIP are now mainly allocated in different ministries:

- Ministry of Economy and Transport: As the ministry responsible for the maintenance and development of economic infrastructure – including the information infrastructure – the Ministry of Economy and Transport coordinates the various efforts in the field of CIP and CIIP;
- Prime Minister's Office: Through the Electronic Government Center, the Prime Minister's Office coordinates the efforts with regard to e-Government, as well as other CIIP-related issues;
- Ministry of Defense: is responsible for national security, including the security of information. In particular, it is responsible for protecting state secrets and public data;
- Ministry of Justice and Law Enforcement: The duties and responsibilities of this ministry include crime prevention and data protection. It controls the Public Administration and Central Electronic Public Services Office, which is the central body for all tasks relating to the provision of e-government services and the management of electronic records and documents.

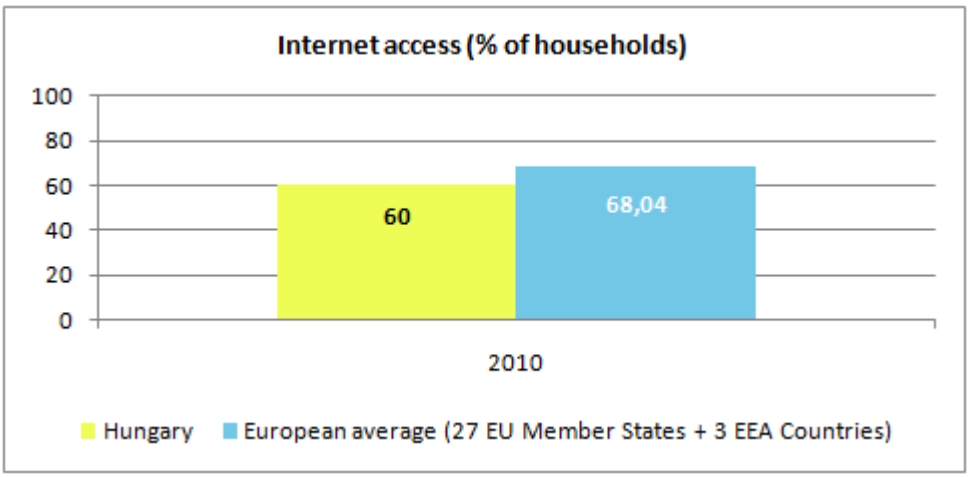
[20] *Source: http://www.itbn.hu/*
[21] *Source: https://nws.niif.hu/ncd2010/*
[22] *See: http://www.kriminalexpo.hu*

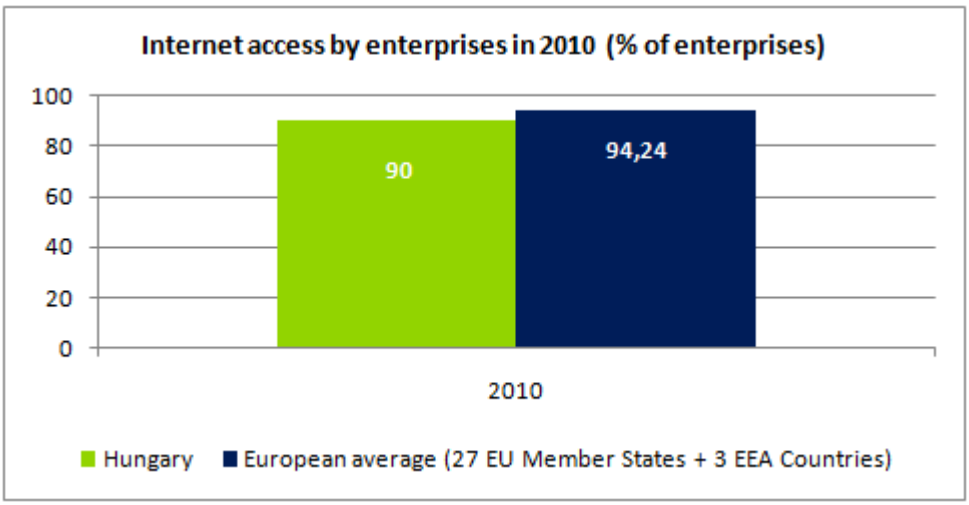
Relevant statistics for the country

In order to provide the reader with additional information about the relative stage of NIS development in Hungary, a series of relevant statistics are included in this section. These statistics show that Hungary is catching up on the European average in regards of Information Technology matters.

Internet access of population and enterprises

The following graphs, based on Eurostat information, provide an overview of the situation[23] of Internet access in Hungary for enterprises and respectively households, relative to the European average.



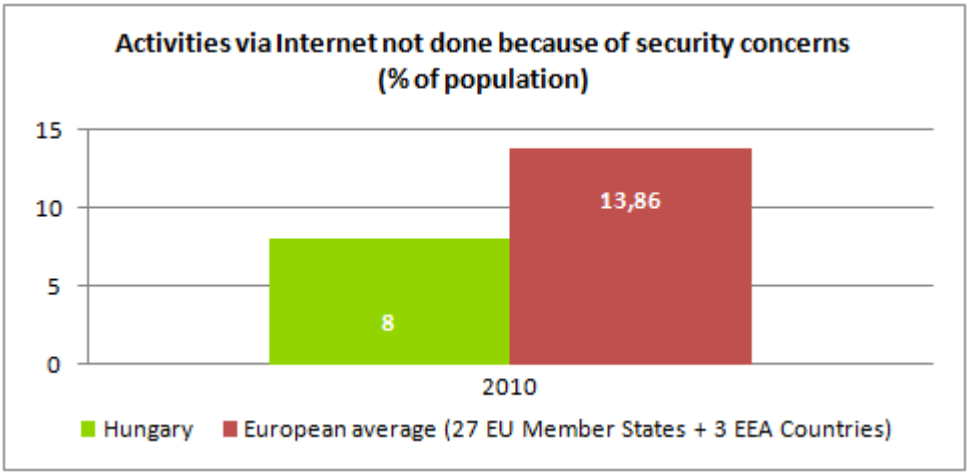


In 2010, the statistics indicate that the enterprises in Hungary have almost the same level of Internet access as the European average, while more effort is required to close the gap on the households.

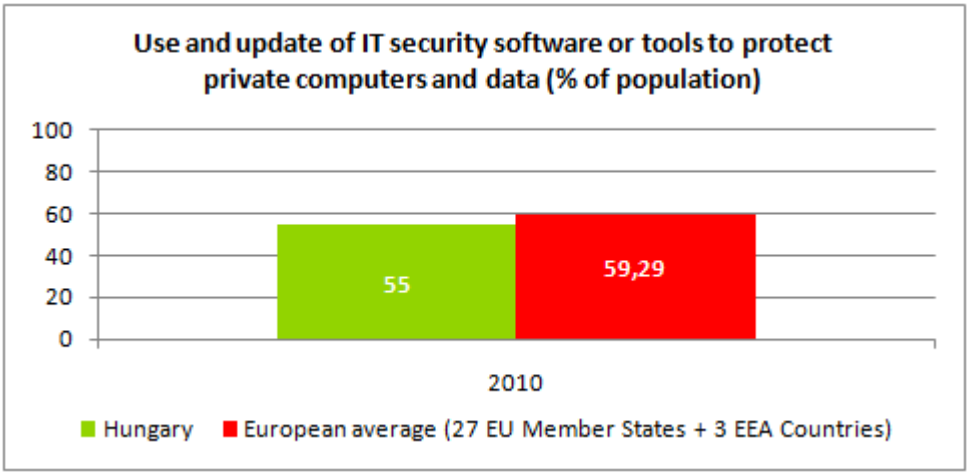
[23] *Source: Eurostat*

Statistics on use of Internet by individuals and related security aspects

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



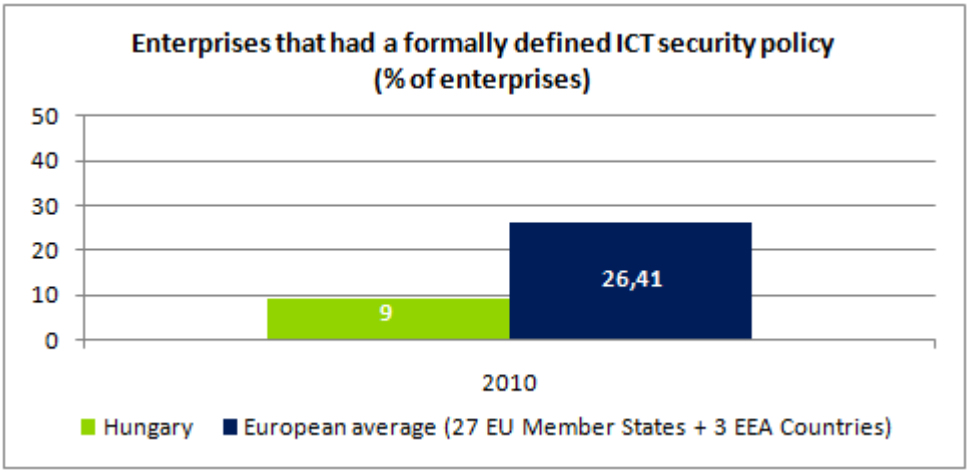
This can be an indication of either much confidence in web-based transactions or of a lack of awareness of the general public regarding IT threats.



Meanwhile, it appears that the use of security tools to protect private computers and data is on almost the same level as the European average.

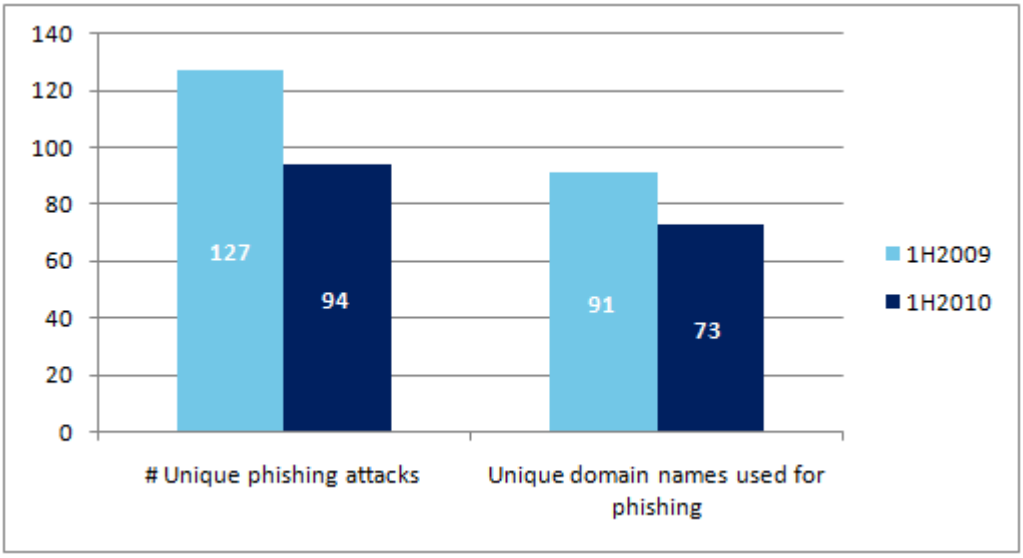
Statistics on use of Internet by enterprises and related security aspects

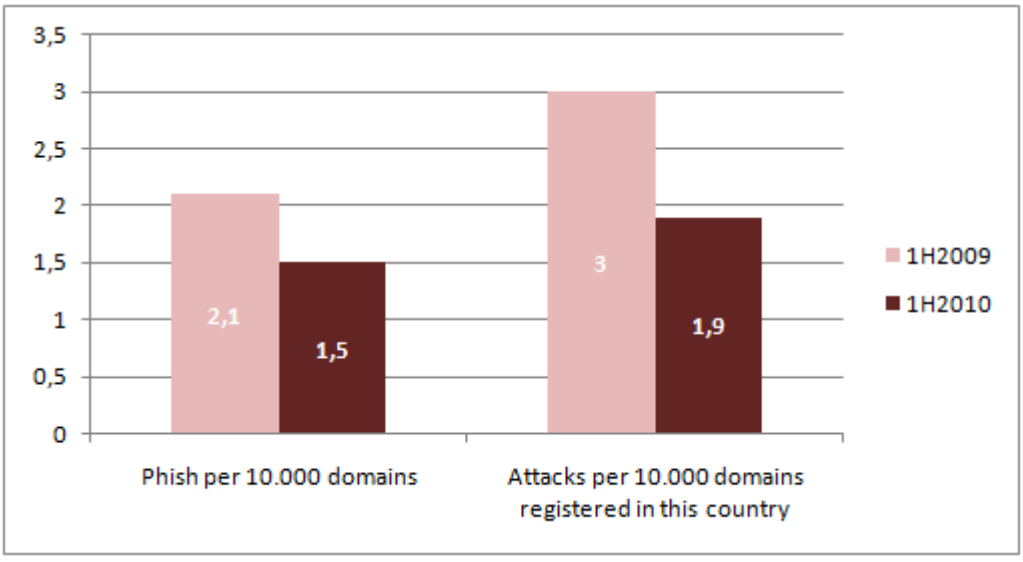
Fewer enterprises in Hungary have a formally defined ICT security policy, compared with their European peers. See below:



Other Statistics

It is interesting to also mention that during the 1st half of 2010, and respectively for the 1st half of 2009, Hungary was mentioned in the global report[24] published by the Anti-Phishing Working Group (APWG) with the following relevant statistics:





Comparing with the previous year the number of the phishing attacks, and of domain names used for phishing and the scores for phish and attacks were significantly reduced in the case of Hungary.

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

APPENDIX

National authorities in network and information security: role and responsibilities

National authorities	Role and responsibilities	Website
1. MEH EKK (Prime Minister's Office, Electronic Government Centre)*	The organization's main focus is the implementation of eGovernment and the supervision of IT development on the local and national government level to comply with regulations of the eGovernment framework. *Note: Please note that the Electronic Government Centre was active until mid 2010 and doesn't exist anymore since summer 2010. The institution has been dissolved once with the Hungary government changes.	www.ekk.gov.hu
2. Ministry of Transport, Telecommunications, Energy	The Ministry of Transport, Telecommunication and Energy takes special aim at assisting, with every available means, the further development of the information and communication technology (ICT) sector that contributes with its outstanding performance to the development of the Hungarian economy.	www.khem.gov.hu
3. National Media and Infocommunications Authority (former National Communications Authority Hungary)	The National Media and Infocommunications Authority's task is to ensure the undisturbed operation, in compliance with pertaining legislation in force, of the media and the markets for electronic communications, postal and information technology services. It places a strong emphasis on the protection of the interests of customers and users. Furthermore, it is also entrusted with establishing and maintaining the fair conditions of an effective competitive environment, as well as with supervising the compliant behaviour of service providers. The Authority has an active role in the work of international organisations in the fields of media regulation, electronic communications, postal and IT services, and establishes and maintains relationships	www.nmhh.hu
4. National Bureau of Investigation	Cyber-crime division of the Hungarian police	www.orfk.hu
5. Data Protection Commissioner of Hungary	National surveillance over the lawfulness of processing personal data, keeping databases and access to public information. The Data Protection Commissioner is independent from the government, other state organizations, and the private sector.	abiweb.obh.hu
6. Parliamentary Informatics Commission	Special commission of the parliament focused on information policy development	www.parlament.hu
7. Ministry of Defence	This ministry is responsible for national security, including the security of information. In particular, it is responsible for protecting state secrets and public data.	www.honvedelem.hu
8. Ministry of Justice and Law Enforcement	The duties and responsibilities of this ministry include crime prevention and data protection. It controls the Public Administration and Central Electronic Public Services Office, which is the central body for all tasks relating to the provision of e-government services and the management of electronic records and documents.	irm.gov.hu
9. National Cyber Security Centre	The Centre pursues activities relating to technical protection, prevention and awareness raising. It represents Hungary in international co-operations and organisations specialised in cyber security	www.cert-hungary.hu

National authorities	Role and responsibilities	Website
	and the protection of critical information infrastructures. The Centre also participates in the preparation of strategies and regulations relating to information and network security and the protection of critical information infrastructures. The Minister heading the Prime Minister's Office exercises control of the Centre, its operation is supervised by the Information Security Supervisor of the Government. The Centre is operated by the Theodore Puskás Government Foundation.	

Computer Emergency Response Teams (CERTs)

CERT	Role and responsibilities • FIRST[25] member • TI[26] listed	Website
10. CERT-Hungary	CERT-Hungary is the Hungarian governmental Computer Emergency Response Team and is operated by the Theodore Puskas Government Foundation. CERT-Hungary's task is to provide network and information security support to the entire Hungarian public, business and civil sectors. The center has a vital role in Hungary's critical information infrastructure protection. CERT-Hungary also acts as a knowledge base for IT professionals and the Hungarian public. CERT-Hungary is ready to handle incidents 24 hours a day, 365 days a year from its constituency CERT-Hungary is FIRST member and is TI listed.	www.cert-hungary.hu
11. HUN-CERT SZTAKI	The HUN-CRT SZTAKI is the Hungarian National Computer Emergency Response Team for Internet Service Providers. The Hun-CERT of the MTA SZTAKI working group responsibility is to assist in the analysis and treatment of incidents. It is also intended to increase safety awareness. This latter activity is not primarily aimed at dealing with computers professionally, but also a large number of users and to provide information to enable them using the Internet combined with the full understanding of risks and a successful defence. HUN-CRT SZTAKI is not FIRST member and is TI listed.	www.cert.hu
12. NIIF-CSIRT	NIIF-CSIRT is the Computer Security Incidents Response Team of NIIF/HUNGARNET. The National Information Infrastructure Development (NIIF) Program serves as a framework for the development and operation of the research network in Hungary. The Program covers the entire Hungarian academic, research and public collection community by providing them with an integrated computer networking infrastructure and, on the basis of that, a wide range of communication, information, and co-operation services, leading-edge environment for networking applications, as well as advanced framework for content generation and provision. NIIF-CSIRT is not FIRST member and is TI listed	csirt.iif.hu

[25] http://www.first.org/members/teams/
[26] http://www.trusted-introducer.nl/

Industry organisations active in network and information security

Industry Organisations	Role and responsibilities	Website
13. IVSZ (Hungarian Association of IT Companies)	Hungarian Association of IT Companies (IVSZ) represents the interests of Hungarian information technology companies and help develop a strong IT industry in Hungary. IVSZ has more than 350 members, a balanced distribution of SMEs (over 250), large Hungarian companies (45) and multinationals (over 40) and some other ICT-related organisations. IVSZ is a member of EICTA and sits on its board of directors.	english.ivsz.hu
14. eSec.hu (Hungarian Cyber Security Package)	Group of Hungarian IT firms providing expertise and lobbying in the field of information and network safety.	www.esec.hu
15. Melasz (Hungarian Association for Electronic Signature)	Stakeholder representation which, for example, undertook the verification of new equipment and methods for creating electronic signatures (e.g. software, chip card).	www.melasz.hu
16. Inforum	The association focuses on developing Hungarian Internet content and combating the negative aspects such as spam and viruses. It also acts as a lobby organization for increasing Internet penetration.	www.inforum.org.hu
17. Association of Hungarian Content Providers	Industry association created by content providers in order to establish safe content on the Internet and raise awareness about online security	www.mte.hu
18. Hungarian IT Security Centre	Industry association created to audit security solutions and develop new security processes.	www.itsecu.hu
19. MATISZ – Hungarian Association of Content Industry	Association of Hungarian content providers. The non-profit organisation has 160 members – 3/4th of them are small or medium enterprises. 50 members – mainly SMEs – are engaged directly or indirectly in multimedia production. MATISZ is member of the European Multimedia Forum (www.e-multimedia.org) and actively participate in EU 5th (ACTeN - www.acten.net) and 6th (PATENT - www.patentproject.org) R&D Framework Programmes and EU Safer Internet Programme (www.internethotline.hu). MATISZ is the Hungarian eContentPlus National Contact Point that help realizing the aims of the EU eContentPlus Programme.	www.matisz.hu

Academic organisations active in network and information security bodies

Academic Organisations	Role and responsibilities	Website
20. BME CIT (Budapest University of Technology and Economics/ Laboratory of Informatics/ Centre of Information Technology)	The most important specific aims of BME CIT are to: • help standardise computer engineer training at the university; • promote the development of syllabus and teaching skills; • help to train, with its own tools, the new generation of staff; • facilitate the university's efforts in retaining staff. CIT plays a very important role in establishing and supporting training grants for computer engineers, and manages a virus laboratory	www.ik.bme.hu
21. NIIF-CSIRT	Hungarian Academic Network's CSIRT	csirt.iif.hu

Other bodies and organisations active in network and information security

Others	Role and responsibilities	Website
22. Internethotline	Part of the European Internet safety programme, to protect against illegal and harmful content.	internethotline.hu
23. Biztonsagos Internet (Safe Internet)	Awareness-raising site for safe Internet use	biztonsagosinternet.hu
24. BIF (Friendly Internet Forum)	Awareness-raising portal against spam and harmful content	http://baratsagosinternet.hu/mss/alpha
25. NHIT (National Telecommunications and Information Council)	Advisory body for the government	www.nhit.hu
26. MSZT (Hungarian Standards Institution)	Certification body	www.mszt.hu
27. ISACA local chapter	ISACA focuses on the certification of various security professionals. The organization deals with information governance, control, security, and audits of professionals. The institution's IS auditing and IS control standards are followed worldwide. ISACA provides two certification programs: Certified Information Systems Auditor (CISA) and Certified Information Security Manager (CISM).	www.isaca.hu
28. Critical Information Infrastructure Protection Workgroup (KIIV)	Specialized in critical infrastructure protection for Hungary	www.kiiv.hu
29. OWASP local chapter	Open web Hungarian local chapter	www.owasp.org/index.php/Hungary
30. NACPH-OFE (National Association for Consumer Protection in Hungary)	A consumer organisation, its aim is to protect and educate consumers	www.ofe.hu

References

- An overview of the eGovernment and eInclusion situation in Europe, available at http://www.epractice.eu/en/factsheets
- ENISA, Information security awareness in financial organisation, November 2008, available at http://www.enisa.europa.eu/doc/pdf/deliverables/is_awareness_financial_organisations.pdf
- Hungary - ENISA CERT Directory: http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country/hungary
- "The National Communications Authority of Hungary and the Hungarian Electronic Communications Market" document available at: http://www.nhh.hu/dokumentum.php?cid=14073
- Global Phishing Survey: Trends and Domain Name Use 1H2010, available at: http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_1H2010.pdf
- More details about The Social Renewal Operational Programme available at http://www.nfu.hu/doc/924 .
- More details about Social Infrastructure Operational Programme available at http://www.nfu.hu/doc/925 .
- The Digital Renewal Action Plan 2010-2015 available in Hungarian at http://www.nfm.gov.hu/data/cms2089529/Digitalis_Megujulas_Cselekvesi_Terv.pdf
- The National Broadband Strategy available at http://www.vus.sk/broadband/nbbs/hu_nbbs.pdf
- Hungarian Mobile Telephone Service Providers Self-Regulation Code for Safer Mobile Telephone Use by Young Teenagers and Children available at http://www.gsmeurope.org/documents/eu_codes/hungary1.pdf

enisa
European Network and Information Security Agency

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