

# Poland Country Report



## About ENISA

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

## Contact details

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

### Mr. Giorgos Dimitriou

ENISA External Relations Expert

[Giorgos.Dimitriou@enisa.europa.eu](mailto: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

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004 as amended by Regulation (EC) No 1007/2008. This publication does not necessarily represent state-of-the-art and it might be updated from time to time.

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

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

© European Network and Information Security Agency (ENISA) 2011

## Table of Contents

<b>POLAND .....</b>	<b>4</b>
THE STRUCTURE OF THE INDIVIDUAL COUNTRY REPORTS .....	4
<b>NIS NATIONAL STRATEGY, REGULATORY FRAMEWORK AND KEY POLICY MEASURES .....</b>	<b>5</b>
OVERVIEW OF THE NIS NATIONAL STRATEGY .....	5
THE REGULATORY FRAMEWORK .....	7
OVERVIEW OF THE KEY STAKEHOLDERS .....	12
INTERACTION BETWEEN KEY STAKEHOLDERS, INFORMATION EXCHANGE MECHANISMS IN PLACE, CO-OPERATION & DIALOGUE PLATFORMS AROUND NIS .....	13
FOSTERING A PROACTIVE NIS COMMUNITY .....	16
<b>COUNTRY-SPECIFIC NIS FACTS, TRENDS, GOOD PRACTICES AND INSPIRING CASES .....</b>	<b>17</b>
SECURITY INCIDENT MANAGEMENT .....	17
EMERGING NIS RISKS .....	18
RESILIENCE ASPECTS .....	18
PRIVACY AND TRUST .....	19
NIS AWARENESS AT THE COUNTRY LEVEL .....	20
COUNTRY-SPECIFIC ACTIVITIES FOR IDENTIFYING AND PROMOTING ECONOMICALLY EFFICIENT APPROACHES TO INFORMATION SECURITY .....	22
INTERDEPENDENCIES, INTERCONNECTION AND IMPROVING CRITICAL INFORMATION INFRASTRUCTURE PROTECTION .....	22
<b>RELEVANT STATISTICS FOR THE COUNTRY .....</b>	<b>23</b>
<b>INTERNET ACCESS OF POPULATION AND ENTERPRISES .....</b>	<b>23</b>
<b>STATISTICS ON USE OF INTERNET BY INDIVIDUALS AND RELATED SECURITY ASPECTS .....</b>	<b>24</b>
<b>STATISTICS ON USE OF INTERNET BY ENTERPRISES AND RELATED SECURITY ASPECTS .....</b>	<b>25</b>
<b>OTHER STATISTICS .....</b>	<b>26</b>
<b>APPENDIX .....</b>	<b>27</b>
NATIONAL AUTHORITIES IN NETWORK AND INFORMATION SECURITY: ROLE AND RESPONSIBILITIES .....	27
COMPUTER EMERGENCY RESPONSE TEAMS (CERTs) .....	31
INDUSTRY ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY .....	32
ACADEMIC ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY BODIES .....	34
OTHER BODIES AND ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY .....	35
REFERENCES .....	37

## Poland

### 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

#### NIS as part of the information society strategy

During the course of 2010 Poland started to develop RPOC - Governmental Action Plan for Cybersecurity 2011-2016<sup>1</sup> (*Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2011-2016*) which is planned to be adopted in first half of 2011.

RPOC defines roles and responsibilities of relevant NIS stakeholders in Poland as well as goals to be achieved in NIS for the years 2011-2016.

In Poland the CERT community plays a key role in developing NIS strategy and is well developed. CERT GOV.PL team operating within the structure of Internal Security Agency (ABW) plays an active role of the governmental CERT. In cooperation with the CERT Polska (the oldest CERT of national scope) they operate state-of-the-art early warning system ARAKIS-GOV, in order to monitor NIS in all governmental networks and detect malware and other novel security threats. Major telecom operators in Poland cooperate in NIS using a platform of ABUSE forum – forum for exchange information, common initiatives, and operational cooperation in incident handling.

#### Strategy for the Development of the Information Society in Poland until 2013

The Poland government is continuing the national action plan Strategy for the Development of the Information Society in Poland started in 2007 which stretch out until 2013. This strategy document envisages a society where citizens and enterprises consciously use the potential of ICT for economic, social and cultural progress, with effective support from a modern and user-friendly public administration.

Poland's information society strategy should respond to the specific needs of society and be consistent with the European initiative "A Digital Agenda for Europe"<sup>2</sup>.

The following attributes for the information society in Poland have been set from the beginning:

- **Availability, security and confidence** – access to reliable information or a secure service that is indispensable to citizen and businesses;
- **Openness and diversity** – no preferences in access to information, especially public information;
- **Universality and acceptability** – efforts to ensure that participation in the information society is manifest and widespread to the maximum extent feasible, and information society products and services are as broad as possible;
- **Communicativeness and interoperability** – the search for and access to desired information is secure, quick and simple.

The information society strategy is multidimensional and covers different aspects of information society development. It defines the vision and mission for the development of the information

---

<sup>1</sup> Details about Governmental Action Plan for Cybersecurity 2011-2016 (*Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2011-2016*) available at <http://bip.mswia.gov.pl/portal/bip/6/19057>

<sup>2</sup> More details about The Digital Agenda for Europe available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF>

society in Poland. Within each of the three priority areas (Human, Economy and State), it maps out strategic directions and determines the objectives that should be accomplished in order to have achieved the desired outcome by 2013.

The strategic directions and main objectives of this action plan are:

- **People**, which has the main strategic direction to accelerate the growth of the intellectual and social capital of Polish citizens with the use of ICT solutions;
- **Business entities**, focused on area of ECONOMY, which has the main strategic direction to increase the productivity, innovation potential and competitiveness of Polish companies;
- **Public administration**, focused on area of STATE, which has the main strategic direction to increase the accessibility and effectiveness of public administration services with the use of ICT solutions in order to modernise internal processes in government and the provision of online services<sup>3</sup>.

### National Development Strategy 2007-2015

The National Development Strategy 2007-2015<sup>4</sup> (*Strategia Rozwoju Kraju 2007-2015, NDS*) is the key, long-term strategic document for the country's socioeconomic development, and serves as the point of reference for all future strategies and programmes prepared by the government in specific areas, including the information society.

NDS defines goals and identifies areas recognised as the most important from the point of view of achieving these aims, upon which the government's activities will be concentrated. At the same time, it takes into consideration the most important development trends in the world economy and the goals that the EU set in the Lisbon Strategy. NDS gives priority to activities that will be undertaken in the years 2007-2015 in order to fulfil the vision of Poland.

Based on the above goals, the following key priorities have been set:

- Improvement of the economy's competitiveness and innovativeness;
- Improvement of technical and social infrastructure;
- Employment growth and quality improvement;
- Growth and progress of rural areas;
- Regional development and improvement of territorial cohesion;
- NIS as part of the information society strategy.

### National Computerisation Plan for the Period 2007-2010

The aim of the National Computerisation Plan for the Period 2007-2010<sup>5</sup> (*Plan Informatyzacji Państwa na lata 2007-2010, NCP*) is to introduce 24 eServices between 2007 and 2013.

NCP lays down activities to reduce digital exclusion, mainly via the Strategy for the Development of the Information Society in Poland until 2013 (*Strategia rozwoju społeczeństwa informacyjnego w Polsce do roku 2013*). Inclusive eGovernment actions are focused on facilitating Internet access and ICT training in schools, local government bodies and Public Internet Access Points (PIAPs). Furthermore, it envisions that the initiatives set will significantly improve the level of ICT literacy, especially among students, teachers, rural populations and remote areas.

<sup>3</sup> For more details in regards to this area please consult the following document:

<http://epractice.eu/en/document/5270449>

<sup>4</sup> The National Development Strategy available at

<http://www.mrr.gov.pl/english/Strategies/srk/Documents/SRKwanqielska0607.zip>

<sup>5</sup> The National Computerisation Plan for the Period 2007-2010 available at

<http://www.mswia.gov.pl/download.php?s=1&id=2674>

## The regulatory framework

### eGovernment Legislation

Same as last year, the eGovernment legislation is based on the Act on the Computerisation of the Operations of the Entities Performing Public Tasks<sup>6</sup>. This act sets up horizontal/infrastructure programmes for all sectors of Public Administration and establishes a common interoperability framework for IT systems in the Polish public sector.

This law is essential for:

- The standardisation & interoperability of Public Administration systems (minimal standards/interoperability frameworks);
- The front & back office integration of Public Administration systems;
- The supervision & supporting of IT projects in Public Administration, at both central and local levels;
- The multi-annual Strategic Plan of IT implementation (horizontal & sectoral projects) in Poland in the context of the 2007-2013 National Development Plan.

### Freedom of Information Legislation

*The Act on Access to Public Information*

The Act on Access to Public Information<sup>7</sup> allows anyone to demand access to public information held by public and private bodies exercising public tasks, as well as trade unions and political parties. Public bodies are required to publish information on their policies, legal organisation and principles of operation, contents of administrative acts and decisions, as well as public assets. The law requires that each of these bodies create a Public Information Bulletin to allow access to information via computer networks.

### Data Protection/Privacy Legislation

*Act on the Protection of Personal Data*<sup>8</sup>

Protection of Personal Data mostly follows the rules established by the European Union Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

### eCommerce Legislation

The eCommerce legislation has not been changed since last year and is based on the following three acts:

- **The Act on Providing Services by Electronic Means** implements into Polish Law the provisions of the Directive 2000/31/EC on certain legal aspects of Information Society services, in particular electronic commerce, in the Internal Market ('eCommerce Directive');

---

<sup>6</sup> The Act on the Computerisation of the Operations of the Entities Performing Public Tasks available at [http://www.mswia.gov.pl/portal/pl/589/3886/Ustawa\\_o\\_informatyzacji\\_dzialalnosci\\_podmiotow\\_realizujacych\\_zadania\\_publiczne.html](http://www.mswia.gov.pl/portal/pl/589/3886/Ustawa_o_informatyzacji_dzialalnosci_podmiotow_realizujacych_zadania_publiczne.html)

<sup>7</sup> The Act on Access to Public Information available at [http://ec.europa.eu/information\\_society/policy/psi/docs/pdfs/implementation/po\\_tra\\_%20dz-u-01-112-1198\\_21-03-05.doc](http://ec.europa.eu/information_society/policy/psi/docs/pdfs/implementation/po_tra_%20dz-u-01-112-1198_21-03-05.doc)

<sup>8</sup> The Act on the Protection of Personal Data available at [http://www.giodo.gov.pl/data/filemanager\\_en/61.pdf](http://www.giodo.gov.pl/data/filemanager_en/61.pdf)

- **The Act on the Protection of Certain Services Provided by Electronic Means** based on, or relying on conditional access implements the Directive 98/84/EC on the legal protection of services based on or consisting of conditional access;
- **The Act on Electronic Payment Instruments** implements the EU Directive 2000/46/EC on the taking up, pursuit of and prudential supervision of the business of electronic money institutions. The Act defines an 'electronic payment instrument' as every payment instrument (including that with a remote access to money resources) enabling its holder to perform operations by means of an electronic device or making possible the electronic identification of the holder, necessary to perform an operation<sup>9</sup>.

### eCommunications Legislation

#### *Telecommunications Law*<sup>10</sup>

The eCommunications Legislation is based on the Telecommunications Law, transposing the EU regulatory framework for electronic communications, was adopted in order to upgrade the regulative process in telecommunications, better adjust national provisions to EU regulations, and introduce new pro-consumer regulations, especially within the scope of solutions to settle arguments between telecommunications operators and consumers.

### Cybercrime legislation

Most of the typical computer misuse acts and computer security breaches have been labeled as offences in the Criminal Code of 6 June 1997. Procedural issues including search and seizures are regulated by provisions of the Criminal Procedure Code of 6 June 1997. Several amendments concerning computer crimes have since entered into force. The latest amendment of 18 March 2004 aimed to harmonize the Polish Criminal Code and the Criminal Procedure Code with the Council of Europe's Convention on Cybercrime.

Polish anti-spam regulation has been implemented by Parliament into the legal system through the Act of 18 July 2002 on electronically provided services. As a result, the distribution of unsolicited commercial information became a misdemeanor.

The organisational structure of the police has been regulated in the Police Act of April 6<sup>th</sup>, 1990. The police is centrally organised and is governed by the Main Commander of Police, who is under supervision of the Minister of Interior.

The police force consists of six basic divisions: criminal police, traffic police, prevention and anti-terrorists squads, special police (e.g. for protection of railway and rivers), and local police. The Minister of Internal Affairs and Administration can establish other divisions if necessary. So far there is no separate computer crime division.

The Polish cybercrime law is built on the three main articles of the Polish Penal Code<sup>11</sup>:

#### *Article 267:*

§ 1 Whoever, without being authorised to do so, acquires information not destined for him, by opening a sealed letter, or connecting to a wire that transmits information or by breaching

<sup>9</sup> For more details in regards to this area please consult the following document:

<http://epractice.eu/en/document/288334>

<sup>10</sup> The Telecommunication Law available at

[http://www.en.uk.gov.pl/gallery/10/75/1075/Telecommunications\\_Law.pdf](http://www.en.uk.gov.pl/gallery/10/75/1075/Telecommunications_Law.pdf)

<sup>11</sup> For more details in regards to this area please consult the following document:

<http://www.cybercrimelaw.net/Poland.html>

electronic, magnetic or other special protection for that information shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to 2 years.

§ 2. The same punishment shall be imposed on anyone, who, in order to acquire information to which he is not authorised to access, installs or uses tapping, visual detection or other special equipment.

§ 3. The same punishment shall be imposed on anyone, who imparts to another person the information obtained in the manner specified in § 1 or 2 discloses to another person.

§ 4. The prosecution of the offence specified in §1 - 3 shall occur on a motion of the injured person.

#### Article 268:

§ 1: Whoever, not being himself authorised to do so, destroys, damages, deletes or alters a record of essential information or otherwise prevents or makes it significantly difficult for an authorised person to obtain knowledge of that information, shall be subject to a fine, the penalty of liberty or the penalty of deprivation of liberty for up to 2 years.

§ 2. If the act specified in § 1 concerns the record on an electronic information carrier, the perpetrator shall be subject to the penalty of deprivation of liberty for up to 3 years.

§ 3. Whoever, by committing an act specified in § 1 or 2, causes a significant loss of property shall be subject to the penalty of deprivation of liberty for a term of between 3 months and 5 years.

§ 4. The prosecution of the offence specified in § 1-3 shall occur on a motion of the injured person.

#### Article 269:

§1. Whoever destroys, deletes or changes a record on an electronic information carrier, having a particular significance for national defense, transport safety, operation of the government or other state authority or local government, or interferes with or prevents automatic collection and transmission of such information, shall be subject to the penalty of deprivation of liberty for a term of between 6 months and 8 years.

§ 2. The same punishment shall be imposed on anyone, who commits the act specified in §1 by damaging a device used for the automatic processing, collection or transmission of information.

### **eSignatures Legislation**

The Polish Act on Electronic Signature, dated 18.09.2001 (*Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym*), aimed to achieve similar standards as in the Electronic Signature Directive.

The act on electronic signatures differentiates three kinds of signatures:

- Electronic signature (Art. 3 item 1 of the Act);
- Safe electronic signature (Art. 3 item 2 of the Act);
- Safe electronic signature verified by qualified certificate (Art. 5 section 1 of the Act).

The last type of signature (safe electronic signature verified by qualified certificate) is equivalent to the hand written signature in terms of its legal effects. The qualified certificate may be issued only by qualified entity subject to stringent requirements defined in the Act (Articles 14-20 and Article 23). The entities providing qualified certificate services are subject to enrolment to the registry of

the qualified suppliers of certificate services. The registry is supervised by the Ministry of Economy.

The Act on Electronic Signatures was amended in 2004, 2005 and 2010 respectively. This Act is compliant with the EU Directive 1999/93/EC on a Community framework for electronic signatures<sup>12</sup>.

### **eIdentification/eAuthentication**

#### *Commercial CAs Certificates*

Qualified and unqualified certification authorities (CAs) issue electronic identifiers to individual persons. Usually these identifiers are Integrated Circuit Cards (ICC) with crypto-controller, private cryptographic keys and public key certificates installed inside (obligatory solution for qualified CAs) or software-based tokens (cryptographic keys and certificates stored outside ICC's cryptographic modules).

In case of eGovernment systems and applications, most frequently used identifiers are the ones with qualified public key certificates. On the other hand, electronic signatures with unqualified certificates are used rather rarely, and the scope of their usage is mainly limited to message authentication, authentication of servers, workstations and other IT equipment.

#### *National register numbers*

Each Polish citizen is obligatorily provided with two distinctive identifiers: General Electronic System for Citizens Evidence (PESEL no.) and Tax Identification Number (NIP).

PESEL numbers are stored in PESEL registers. Incidents occurred in the past regarding the attribution of PESEL numbers: different persons had been assigned with the same PESEL number. This is one of the reasons why the Minister of Interior and Administration started the PESEL2 project for a new public registers implementation.

With regard to the use of electronic signatures in eGovernment applications, both types of numbers appear particularly relevant as they have been envisaged to be used as the unique identifier in the certificate of the future eID card (but not in commercial CA certificates).

Furthermore, the national registry number PESEL and NIP can be envisaged to become the identifiers to be used in the future for all back-office information exchanges in eGovernment applications for those who hold such numbers.

### **Self-regulations**

#### *Self-regulatory Code of Conduct for safe use of mobile phones<sup>13</sup>*

As in the previous years the Polish 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 Polish mobile electronic telecommunications market and complies with applicable European and Polish national legislation.

---

<sup>12</sup> For more details in regards to this area please consult the following document:  
<http://epractice.eu/en/document/288334>

<sup>13</sup> For more details in regards to this area please consult the following document:  
[http://www.qsmeurope.org/documents/eu\\_codes/poland\\_coc.pdf](http://www.qsmeurope.org/documents/eu_codes/poland_coc.pdf)

---

### *ABUSE forum*

Many major telecom operators and ISPs in Poland has joined the initiative of CERT Polska ([www.cert.pl](http://www.cert.pl)) creating a forum of cooperation of operator's security teams in terms of common practices in Internet security in Poland. Ten to twenty representatives from CERTs, Abuse teams, other security teams from polish large and medium size operators and providers meet four times a year, starting from 2005 to respond to current trends in NIS, establish working informal channels of cooperation and data exchange in case of security incident response and build common initiatives like common statistics approach, BGP black holing (successfully deployed in many of operators on the self regulatory basis).

## 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.

<b>National Authorities</b>	<ul style="list-style-type: none"> <li>• Ministry of Interior and Administration</li> <li>• Ministry of National Defense (Information Society Department, Department for Information , Technology Development, Department for State Registers and ICT)</li> <li>• Ministry of Infrastructure</li> <li>• Bureau of the Inspector General for the Protection of Personal Data (GIODO)</li> <li>• ABW(National Internal Security Agency)</li> <li>• Polish Committee for Standardisation</li> <li>• RCB (National Security Centre)</li> <li>• BBN (Bureau of National Security)</li> <li>• Office for Competition and Consumer Protection</li> <li>• Office of electronic communications</li> <li>• Polish Chamber of Commerce</li> </ul>
<b>CERTs</b>	<ul style="list-style-type: none"> <li>• CERT POLSKA</li> <li>• CERT GOV PL</li> <li>• PIONIER-CERT</li> <li>• TP CERT (Telekomunikacja Polska)</li> </ul>
<b>Industry Organisations</b>	<ul style="list-style-type: none"> <li>• KIGEiT (Krajowa Izba Gospodarcza Elektroniki I Telekomunikacji)</li> <li>• PIIT (Polska Izba Informatyki i Telekomunikacji)</li> <li>• The Polish Chamber for Electronic Communication (Polska Izba Komunikacji Elektronicznej)</li> </ul>
<b>Academic Organisations</b>	<ul style="list-style-type: none"> <li>• Academic Computer Centre in Gdansk - TASK (Centrum Informatyczne Trójmiejskiej Akademickiej Sieci Komputerowej)</li> <li>• NASK</li> <li>• The Academic Computer Centre CYFRONET AGH</li> <li>• ICM – Interdisciplinary Centre for Mathematical and Computational Modelling</li> <li>• Wrocław Centre for Networking and Supercomputing</li> </ul>
<b>Others</b>	<ul style="list-style-type: none"> <li>• ISSA PL</li> <li>• OWASP PL</li> <li>• ISACA PL</li> <li>• Nobody’s Children Foundation(Polish Awarenode)</li> <li>• Dyżurnet.pl(Polish hotline for reporting illegal content in the Internet)</li> <li>• SIC (Safer Internet Centre)</li> <li>• Kidprotect.pl Foundation</li> <li>• TP Group Foundation (Fundacja Grupy TP)</li> <li>• FK(Polish Consumer Federation National Council)</li> </ul>

For contact details of the above-indicated stakeholders we refer to the ENISA “Who is Who”<sup>14</sup> – 2010 Directory on Network and Information Security and for the CERTs we refer to the ENISA CERT Inventory<sup>15</sup>.

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.

<sup>14</sup> 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

<sup>15</sup> <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**

A key component of the eGovernment Strategy in Poland was the National Computerisation Plan for the period 2007-2010. This plan covers the realisation of public eServices, and recommends the use of open, publicly available IT standards while calling for technological neutrality in all Government-led IT projects. It also introduces the Electronic Platform of Public Administration Services (ePUAP) project, which is a key driver for interoperability efforts.

The Interoperability Framework as well as the existing interoperability guidelines are all law enforced in Poland: the core standards around electronic communications (protocols) and mandatory fields in electronic messages are explicitly laid down in law.

The key goal of the Interoperability Framework is to allow interaction of information systems through technological neutrality (using open standards) and alignment of different government entities in terms of organisational and semantic interoperability.

The Interoperability Frameworks assigns responsibility to the Polish Department of Information Technology of the Ministry of Internal Affairs and Administration to evaluate recommendations and update the Framework at least once a year. Recommendations are gathered using a formal public consultation process. An advisory body is to be installed.

### **Co-operation between public authority bodies**

Since the beginning of 2010, there is still no single body recognized among NIS stakeholders in Poland as the national security agency. The Ministry of Interior and Administration and Office of Electronic Communications both hold responsibility for the development and implementation of information security policy.

Departments under the ministry's control include the Department of Information Technology Development, Information Society Department, and Center of Information Projects.

The Ministry of Interior and the Ministry of Transportation are closely working with the Office of Electronic Communications for policy development and policy implementation. The Ministry of the Interior and Administration is charged with oversight of information technology, national tele-information systems, and national information administrative registers.

The Council of Ministers' Committee for Computerisation and Communications (Komitet Rady Ministrów do Spraw Informatyzacji i Łączności) under the Ministry of the Interior and Administration deals with the coordination and monitoring of the implementation of public institutions' activities in the area of informatisation, information society development and electronic communications.

According to the Program of Cyberspace for the Republic of Poland, it is necessary to define responsibilities of those entities in the private sector whose protection against cyber threats is important for the proper functioning of the state. This group of entities should include amongst others the owners of telecommunication infrastructure. However, it should be emphasised that the matter of protection of cyberspace is not limited to telecommunication area, but also other areas of services, such as the banking sector. Achieving real cooperation between state administration and the private sector is a challenge. Such cooperation is possible only when in the established solution the benefits of cooperation outweigh the risks resulting from even a partial loss of control over information.

### **Co-operation via Office of Electronic Communications**

Cooperation via Office of Electronic Communications (UKE) is the national regulatory authority for the telecommunications sector. It intervenes in all matters related to the functioning of the telecommunications market, and ensures that all citizens have access to universal service.

UKE supports the development of telecommunications services in Poland and cooperates with domestic and international telecommunications organisations, other competent national authorities, the EC and related bodies.

UKE is also cooperating with other regulatory authorities in the Member States and with the EC, aimed at the consistent implementation and application of legal provisions.

### **Co-operation and initiatives on internet security**

Since 2005, two projects have been underway in Poland as part of the European Commission's Safer Internet Action Plan. Both projects are under the auspices of the Ministry of Education and Science, the Interior and Administration Ministry, the Children's Ombudsman, the Police Headquarters, the Office for Competition and Consumer Protection, and UNESCO. Starting with 2008 the above mentioned projects were combined in one project called SIC (Safer Internet Centre: [www.saferinternet.pl](http://www.saferinternet.pl)) as the model initiative in Europe.

The first project is NIFC Hotline Polska<sup>16</sup>. This project is managed by the Dyżurnet team of NASK (the Research and Academic Computer Network). The project objectives are organizing and maintaining a Hotline that receives reports on illegal content published on the Internet.

The Hotline cooperates with the police in tracking down offenders who post illegal content on the Net and eliminates such content in cooperation with the respective ISPs. The Polish NIFC Hotline—Dyżurnet.pl team became a member of the INHOPE Association on the 28th January 2005, and received full membership within a year. The other project is maintained by the Awareness consortium formed by NASK and the Nobody's Children Foundation.

The proposal to establish the "Awareness" Node was submitted in response to the European Commission's Call for Proposals 2003/2004 and is also based on the European Union guidelines presented in the Safer Internet Action Plan, Work Programme 2003-2004.

Also a Platform for Homeland Security has been developed. The activities of the Polish Platform for Homeland Security (PPBW) are aimed at creating integrated computer tools to support the broadly defined efforts to improve public security. The participating authorities to the PPBW platform are: National Police Headquarters, Supreme Court National Prosecution Office, Poznan Supercomputing and Networking Center, and different universities.

The main focus of these efforts is to support police and other security services with modern technologies, and some of the proposals worked out within the Platform may strengthen the efforts to improve both security and prevention of crimes committed with the use of modern technologies and the ubiquitous Internet. The integrated computer tools that are developed within the Platform improve the competitiveness and innovativeness of Polish science in the European arena, and increase the effectiveness of government services and institutions responsible for the security of citizens and the state. The joint performance of projects contributes also to strengthening cooperation between the research institutions participating in the projects and the industry represented by commercial companies. Due to the sensitive nature of data and project

---

<sup>16</sup> <http://hotline.org.pl>

topics, a part of the research work within the Polish Platform for Homeland Security has the classified status.

### **Co-operation initiatives involving CERT's**

During the course of 2010 Poland had security response teams in place to handle security breaches and other incidents. NASK/Computer Emergency Response Team Polska, Polish CERT, CERT GOV PL, and National Internal Security Agency (ABW) are the main national points of contact for IT security. ABW is also responsible for key elements of CIP/CIIP at the national level in Poland. What regards the CIP/CIIP and Cert the CERT GOV PL collaborates with PIONIER CERT.

CERTs and other security teams organized by telecom operators and providers are also cooperating in the formula of ABUSE forum.

ARAKIS is a CERT Polska (NASK) project that aims to create an early warning and information system for novel network threats. The system focuses on detection and characterization of new automated threats. Currently the system detects threats that propagate actively through scanning. ARAKIS aggregates and correlates data from various sources, including honeypots, darknets, firewalls and antivirus systems. Each of these sources gives a different perspective on what is happening in the network.

The HoneySpider Network Project is a joint venture between NASK/CERT Polska, GOVCERT.NL and SURFnet. The goal is to develop a complete client honeypot (or honeyclient) system, based on existing state-of-the-art client honeypot solutions and a novel crawler application tailored for the bulk processing of URLs. The system focuses on attacks against, or involving the use of, Web browsers.

The CLOSER (CLuster Of SEcurity Resources) Program awarded by NATO to NASK (and others) helps establishing and coaching new CSIRT teams in CEE region. Additional goals of the program are to: provide training and mentoring services; instruct in usage of IR systems; increase cooperation among CERTs worldwide; help in establishing CERT standards and procedures in countries where this may be necessary; and introduce new CERT stakeholders to worldwide forms and assist in their collaboration.

## Fostering a proactive NIS community

### Cyber Europe 2010

During 2010 Poland took part in the first pan-European exercise on critical information infrastructure protection, Cyber Europe 2010, organised 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.

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).

### NATO Cyber Defence Workshop

During 2010, Poland participated at the 13<sup>th</sup> NATO Cyber Defence Workshop which took place on May 26-28, 2010 in Tallinn, Estonia.

Cyber defence has become an important building block and confidence building measure within NATO transformation. The scope and complexity of these issues will likely require the release of many concept development and experimentation trials in the future. However, NATO has already achieved three important milestones in the field of cyber defence:

Firstly, a real-time management capability is ensured with the creation of the Cyber Defence Management Authority (CDMA). Secondly, 24/7 NATO's network defence and incident handling support is the responsibility of NATO Computer Incident Response Capability. Last but not least, an intellectual platform for long-term doctrinal and strategic thinking about the cyber domain is in place through the accreditation of the International Military Organisation - Cooperative Cyber Defence Centre of Excellence (CCDCOE).

Evolving threats in cyber space and society's growing dependency on critical information infrastructure enforces the Euro-Atlantic community to keep a constant momentum when building cyber defence capabilities in cooperative and holistic manner. This workshop aims at supporting NATO and NATO nations in participating and influencing the process of building a multinational and multidisciplinary framework among allies. NCIRC and CCDCOE invite representatives from NATO member states to the workshop to contribute to the process.

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

### Security incident management

Similar to 2009, there is no legal obligation to exchange information and inform the authorities responsible for the network security. However, in situations when the computer incidents have elements of criminal offences (crimes) or represent a serious threat to the operation of the networks that are relevant to the state's security, the incident must be reported. Such obligation is due to the general provisions of criminal law. Regardless, the state authorities responsible for public safety are equipped with the powers that allow them to request certain information or to demand an infrastructure owner or network operator to supply them with documentation, testimonies, expertises and so forth.

Since 1996 the role of national CSIRT is served by the CERT Polska team. Earlier (from 1996 till 2001) it was known as CERT NASK. Apart from the CERT teams, some specific tasks and powers are assigned to the Polish National Internal Security Agency (ABW).

According to the last annual report of ABW from 2009<sup>17</sup>, there have not been any serious incidents of violating information security of the Internet computer networks of state administration or other computer systems included in the critical information infrastructure of the country. However, in ABW's assessment, cyber terrorism threats in Poland remain to be relatively high.

The responsibility to fighting threats to cyberspace rests with the Governmental Computer Security Incident Response Team – CERT.GOV.PL. This team constitutes a platform for coordinating a response to incidents threatening the security of information systems or network used by state organs whose destruction or disturbance might lead to a severe disruption of the country.

One of the Team's tasks is to implement and oversee an early warning system to report threats from the Internet – ARAKIS-GOV. The system has been developed by ABW in cooperation with a CERT Polska Team operation the NASK organization. The ARAKIS-GOV was established in order to support the protection of tele-information resources of the public administration, following the supplementing of the ARAKIS system, created by CERT Polska, with additional functionality. At the present time, system sensors are installed in over 60 offices of the central and local administration.

A unique feature of the ARAKIS-GOV system is that it does not monitor in any way contents of information exchanged between the protected institution and the Internet, because system sensors are installed outside the protected internal network of a given institution, on the side of the Internet network. Since the ARAKIS-GOV system became fully operational (mid-2009), 3367 security incidents have been reported via this system.

ABW, and within its structures the Information Security Department (DBTI) deals with telecommunication security issues in a comprehensive way. Fast development of IT technologies implies using these technologies also against the law, which undoubtedly influences security of electronically processed information. It is the role of DBTI to minimise this unwanted phenomenon. For this reason the Department is equipped with professional background, such as Certification Unit, specialised laboratories researching cryptographic and electromagnetic security, highly qualified and experienced staff and system solutions.

---

<sup>17</sup> ABW Annual Report 2009 available at <http://www.abw.gov.pl/download.php?s=2&id=620>

The effect of comprehensive actions of DBTI allows us to shape the IT security policy at high level and propagate it amongst the users of the systems and networks in the form of recommendations as well as during specialised trainings, and above all execute its implementation with processes of accreditation and implementation related to IT security.

Comparing with 2009, during the first half of 2010, Poland was mentioned in the global report published by the Anti-Phishing Working Group (APWG) in TOP10 with the following relevant statistics:

- 1582 unique phishing attacks reported for this country;
- 744 unique domain names used for phishing reported for this country;
- A score of 4.1 phish per 10.000 domains registered in this country;
- A score of 8.8 attacks per 10.000 domains registered in this country.

### Emerging NIS risks

Since the beginning of 2010 there were no major changes to the emerging NIS risk area.

A study of the Ministry of National Defense published during 2008 the Vision of the Polish Armed Forces 2030<sup>18</sup>. According to the above mentioned document a constantly growing level of society's dependence upon telecommunication systems shall make cyber terrorism a real threat to the state security. It will essentially consist in attacking and destroying information resources of the state defence system and major elements of the IT system (info sphere) responsible for the administration of the energy sector, economy and state finances. Level of threats to Poland's security in the energy sector will also increase.

### Resilience aspects

Similar with previous years, in 2010, a key role regarding network resilience aspects are played by the NASK and CERT Polska.

The primary goal from an action plan undertaken to improve resilience is to keep network "miscreant free":

- Identify compromised nodes;
- Identify and analyze new exploit/vulnerability (root cause);
- Identify and analyze malware;
- Identify groups/individuals behind attacks;
- Organize takedowns (cooperation with LEA);
- Mitigation: BGP blackholing, DNS blackholing, URL blacklisting.

According to NASK and CERT Polska, information used in above mentioned activities could come from various sources as external parties like other CERTs, security teams, ISPs, banks, etc. , or network sensors based on server-side honeypots, client-side honeypots, darknets, existing logging infrastructure, netflow data, etc.

---

<sup>18</sup> The Vision of Polish Armed forces 2030 available at [http://www.wp.mil.pl/pliki/File/vision\\_of\\_paf\\_2030.pdf](http://www.wp.mil.pl/pliki/File/vision_of_paf_2030.pdf)

## Privacy and trust

### Status of implementation of the Data Protection Directive

The rules established by the Data Protection Directive were implemented in Poland by the Act on the Protection of Personal Data of 29 August 1997 (Journal of Laws of 2002, No. 101, item 926, as amended) (the "DPA").

The competent national regulatory authority on this matter is the Polish Inspector General for the Protection of Personal Data (the "IGPPD").

### Personal Data and Sensitive Personal Data

The definition in the Polish DPA is based on the standard definition of personal data. In particular, information is not personal data if identifying the relevant individual would require an unreasonable amount of time, cost and manpower.

Under the DPA, sensitive personal data include both: (i) the standard types of sensitive personal data; and (ii) data concerning genetic code, addictions and data relating to convictions, decisions on penalties or fines and other decisions issued in court or administrative proceedings.

Sensitive personal data may be processed if the standard conditions for processing sensitive personal data are met. In this respect, it is important to note that consent to the processing of sensitive personal data must be given in writing. Additionally conditions apply allowing the processing of sensitive personal data if a specific legal act permits their processing or the processing is for scientific research.

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

Data controllers must comply with the general data security obligations. Regulations were issued in 2004 setting out basic, medium and high levels of security including details of the specific measures that must be employed by the data controller.

### Data protection breaches and enforcement

The Polish DPA does not contain any obligation to inform the IGPPD or the data subject of a security breach.

### Enforcement

The IGPPD may issue an administrative decision that: (i) the negligence be remedied; (ii) the personal data be completed, updated, corrected, disclosed or not disclosed; (iii) additional measures be applied in protecting the personal data; (iv) the flow of personal data to a third country is suspended; (v) the data is safeguarded or transferred to other data subjects; or (vi) the personal data is erased.

The IGPPD has no ability to fine organisations, but it can inform proper prosecuting bodies about infringement of the DPA in order for them to instigate criminal proceedings.

## NIS awareness at the country level

### eChallenges e-2010 Conference

The eChallenges e-2010 Conference<sup>19</sup> took place in Warsaw on 27-29 October. This was the twentieth in a series of Annual Conferences supported by the European Commission, which regularly attracts over 650 delegates from leading commercial, government and research organisations around the world to share knowledge and experience, lessons learnt and good practice in the areas of eInfrastructures, ICT for Networked Enterprise & RFID, eGovernment & eDemocracy, eHealth, Collaborative Working Environments, Living Labs, Digital Libraries and Cultural Heritage, Technology Enhanced Learning, Intelligent Content & Semantics, High Performance Computing Applications, Security and Identity Management and Mobility.

The goal of e-2010 was to stimulate rapid take-up of Research and Technology Development (RTD) results by industry and in particular SMEs, and help open up the European Research Area (ERA) to the rest of the world.

The two EU-funded projects, WINS-ICT and ICT-WEB-PROMS, jointly organised a stand throughout the three day eChallenges e-2010 Conference to inform interested EU and WBC stakeholders of the projects' activities and cooperation opportunities with the WB region. The project teams collected expressions of interest for cooperation and act as intermediaries. It was furthermore possible to register in the contact database of WB and EU stakeholders, managed by the two projects, during the conference.

### International Conference "Keeping Children and Young People Safe Online"

During 2010, Poland hosted the 4<sup>th</sup> International Conference "Keeping Children and Young People Safe Online"<sup>20</sup>.

The conference brought together approx. 500 representatives from the education sector, NGOs, law enforcement, government and industry. It will address a wide variety of issues relating to children and young people's safety online, such as the use of social networking sites and mobile phones, privacy, online gaming, educational strategies, etc. This conference aims to raise awareness of the new challenges and opportunities in fighting online threats and to help share best practices across different sectors.

The aim of the conference is to raise awareness of the new challenges and opportunities in fighting online threats and to help share best practices across different sectors. The objective was to present the latest achievements in education on safety online and combating illegal web content.

### Awareness actions targeting the safe use of the internet

In December 2004, NASK together with the Nobody's Children Foundation signed an agreement and became partners of the INSAFE consortium managed by European Schoolnet, which coordinates the work of national "Awareness" Nodes at the European level, on behalf of the European Commission. The Awareness project aims at creating a centre that would raise awareness of threats that the youngest users in Poland face on the Internet.

Awareness Node has also run the idea of the National Coalition for Safer Internet in executing an initiative where everybody can participate starting from [www.saferInternet.pl](http://www.saferInternet.pl) web site.

<sup>19</sup> For more information see the eChallenges e-2010 website at <http://www.echallenges.org/e2010/>

<sup>20</sup> More details available at [http://www.saferinternet.pl/konferencja\\_en/articles-2010/4rd\\_international\\_conference\\_keeping\\_children\\_and\\_young\\_people\\_safe\\_online.html](http://www.saferinternet.pl/konferencja_en/articles-2010/4rd_international_conference_keeping_children_and_young_people_safe_online.html)

Participation in the "Awareness" project also involves Information Security Awareness programmes in the EU: Insight and Guidance for Member States cooperation with institutions that work to ensure safe Internet use. The consortium has recently been invited to preparatory negotiations for input/work with another Safer Internet programme that will be implemented in the years 2007/2008.

The project is co-sponsored by NASK and the Nobody's Children Foundation, with 50% co-sponsored by the European Union. Previously in 2004 the Foundation started the program "Dziecko w Sieci" (Kid on the Web) which is focused on raising awareness in children of the threats coming from Internet. From 2008 EU Safer Internet Programme in Poland is realized by SIC (Safer Internet Centre): [www.saferinternet.pl](http://www.saferinternet.pl).

Another initiative that NASK has carried out for many years under the auspices of the Minister of Science, Information Society Technologies (now the Minister of Education and Science) and Minister of Interior and Public Administration with the cooperation of ENISA is a series of "SECURE" annual conferences that promote the awareness of network and computer system security.

The conference structure and program is specifically aimed at: senior managers directly charged with protecting their corporate infrastructure; technical experts who determine security requirements and implement solutions; policy and decision makers with overall security responsibility; legal/compliance/regulatory professionals who work with policy and decision makers in establishing security policies; and government executives and practitioners who are responsible for protecting systems and critical infrastructures. Every year current issues concerning security matters of IT systems and networks are discussed at the conference, which for 10 years has been organized by CERT Polska team acting within NASK<sup>21</sup>.

### **Awareness actions targeting national authority bodies**

The National Computerization Plan (the NCP) details the level of development of eGovernment and is a starting point for discussion on the priorities for the computerization plan for the years 2007-2010. The NCP is an instrument used to plan and coordinate computerization activities of public bodies with regard to tasks being fulfilled by these bodies. The following target related to NIS awareness has been set:

- Creating conditions for the increase of awareness and education of users with regards to protection of their systems against malicious software and spam – this includes notifying the appropriate body of the threats encountered.

In the area of awareness programs derived by local government entities, the following initiatives can be highlighted:

- Initiative on awareness raising set up by the Association of Polish Districts and three leaders on IT technology in the Polish market (Symantec, Microsoft and Polkomtel). The Association of Polish Districts, founded in February 1999, has members in 313 districts. The district cities have organized a series of seminars and training sessions in 2005 and 2006 based on awareness raising;
- Initiative on awareness raising set up by the e-administration club, which associates self-government and government organisations. Established in October 2003, the mission is to gather and exchange knowledge on implementation of IT technology in administration. E-administration club has organized and co-organized with other organisations several training courses on IT technology. Twice a year, the administration club organizes a

---

<sup>21</sup>More details available at: <http://www.enisa.europa.eu/events/ee/secure09>

conference called "Forum of IT in e-administration". This year the VI<sup>th</sup> Forum of IT in e-administration was held in Toruń (Poland) on 25<sup>th</sup> and 26<sup>th</sup> April. Awareness raising on ICT was an important point at the conferences.

### **Awareness actions targeting industry and citizens**

NASK and CERT Polska also maintain a very important website in awareness raising for IT Specialists and Home Users; information on the website include details on new threats, vulnerabilities, incidents and preventive information as well as warning on possible attacks.<sup>22</sup>

FISHA is a framework for Information Sharing & Alerting and is collaboration between CERT Polska, CERT-Hungary and the University of Gelsenkirchen to build a common European information and alerting system based on the findings of the EISAS study of ENISA. The goals of FISHA are:

- Improve security awareness amongst home users and SMEs through the creation of a European information sharing and alerting system;
- Create a channel that can be used to reach these groups and supply them with timely best practice information, alerts and warnings phrased in an easy to understand, non-technical way;
- Design and implement the framework: Set up pilot (N)ISAS systems Design and implement protocols for exchange of alerting information;
- Prepare a awareness campaign;
- Improve cooperation between relevant stakeholders.

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

During 2010 Poland participate to the event Critical Information Infrastructure Protection(CIIP): "Where We Stand and Where We Are Heading To" .

The event was meant to be a forum at the EU level to facilitate exchanges of views on issues related to Critical Information Infrastructure Protection (CIIP). Information Infrastructures have become a key building block of virtually all Critical Infrastructures (CIs) which are being built today, as well as of a plethora of critical applications. As such, the design and operation of Critical Information Infrastructures (CIIs) is increasingly being characterized by challenging security and dependability requirements.

The Member States have varying approaches to CIIP, but the success of CIIP programmes depends heavily on the cooperation and level of involvement that different stakeholders can achieve. This special session aimed at sharing ideas towards the creation of a common approach for the establishment of requirements and needs to improve the protection of Critical Information Infrastructures.

### **Interdependencies, Interconnection and Improving Critical Information Infrastructure Protection**

Polish National Security Center (RCB) ([www.rcb.gov.pl](http://www.rcb.gov.pl)) is responsible for creating National Programme for Critical Infrastructure Protection). This work is ongoing.

---

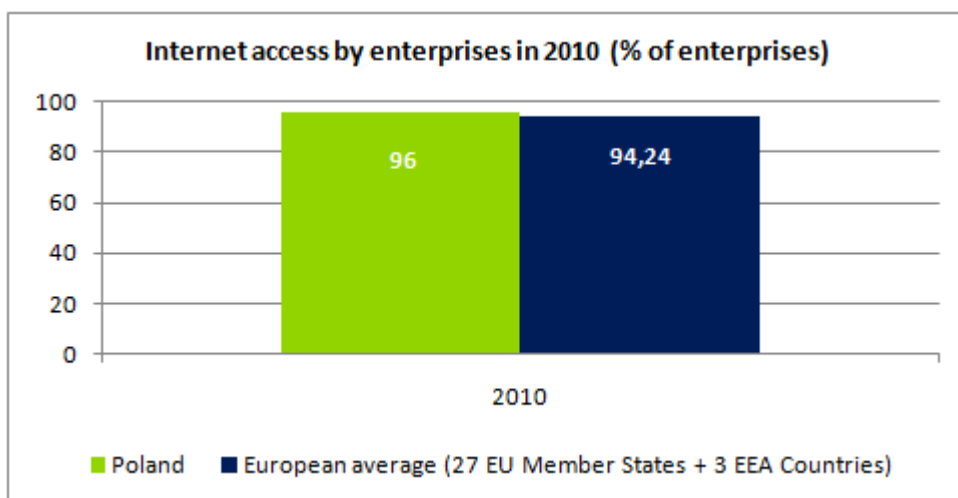
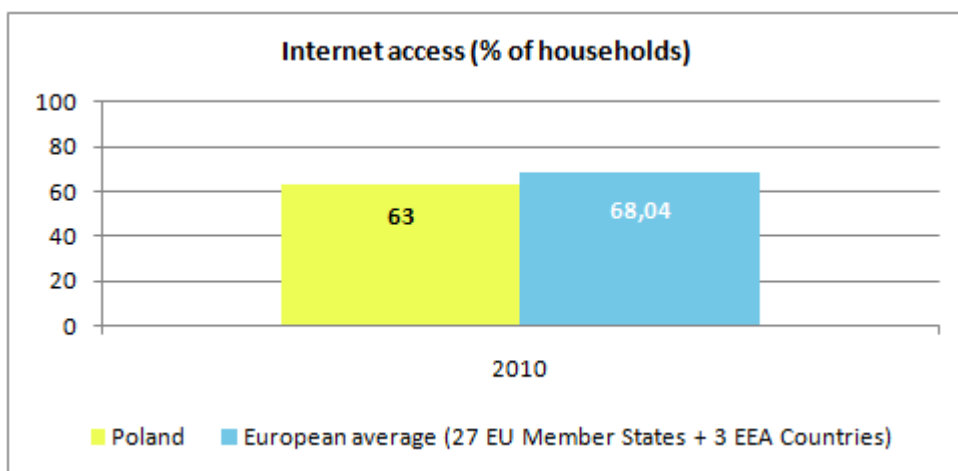
<sup>22</sup>More details available at: <http://www.cert.pl/>

## Relevant statistics for the country

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

### Internet access of population and enterprises

The following graphs provide an overview of the situation<sup>23</sup> of Internet access in Poland for enterprises and respectively households, relative to the European average.

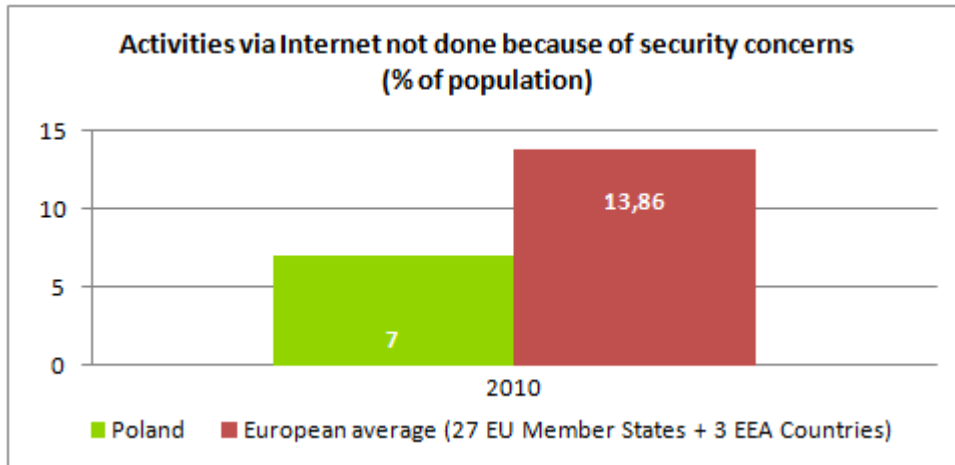


In 2010, the statistics indicate that the enterprises and the households in Poland have almost the same level of Internet access as the European average.

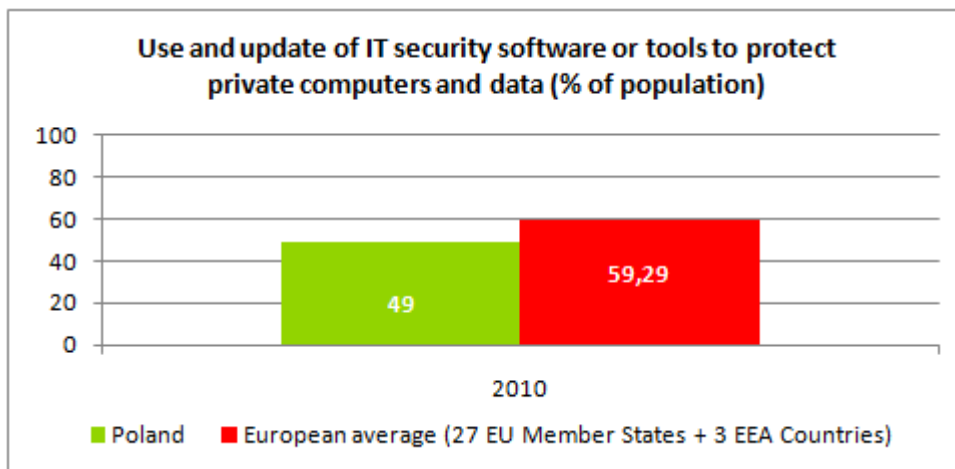
<sup>23</sup> Source: Eurostat

### Statistics on use of Internet by individuals and related security aspects

The percentage of population in Poland 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:



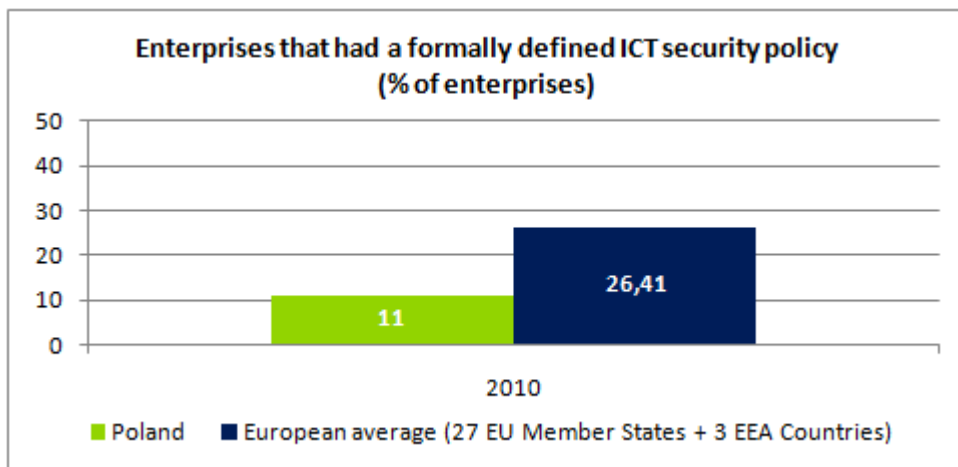
This can be an indication of either much confidence in web-based transactions or of a lack of awareness of the general public regarding IT threats.



Also, it appears that the use of security tools to protect private computers and data is below the European average.

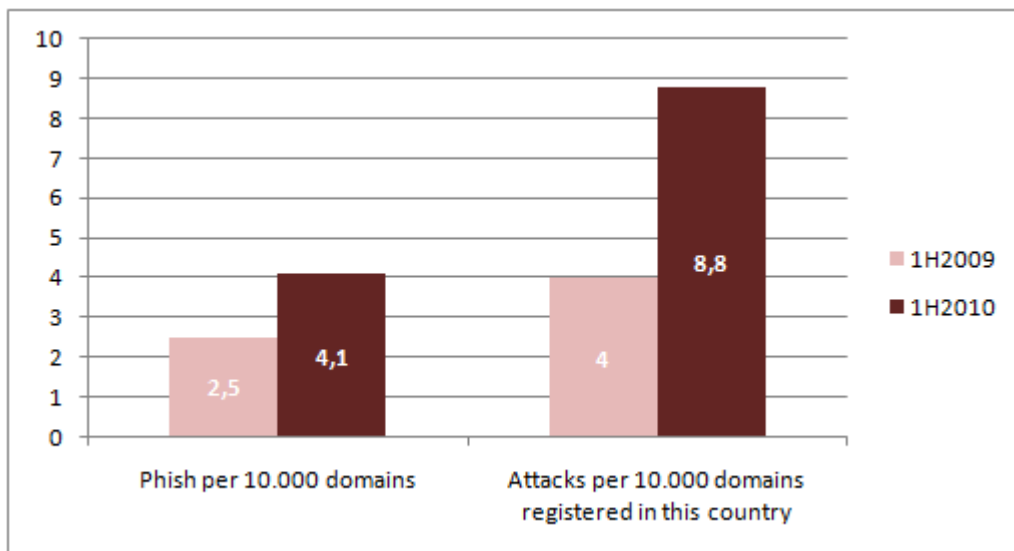
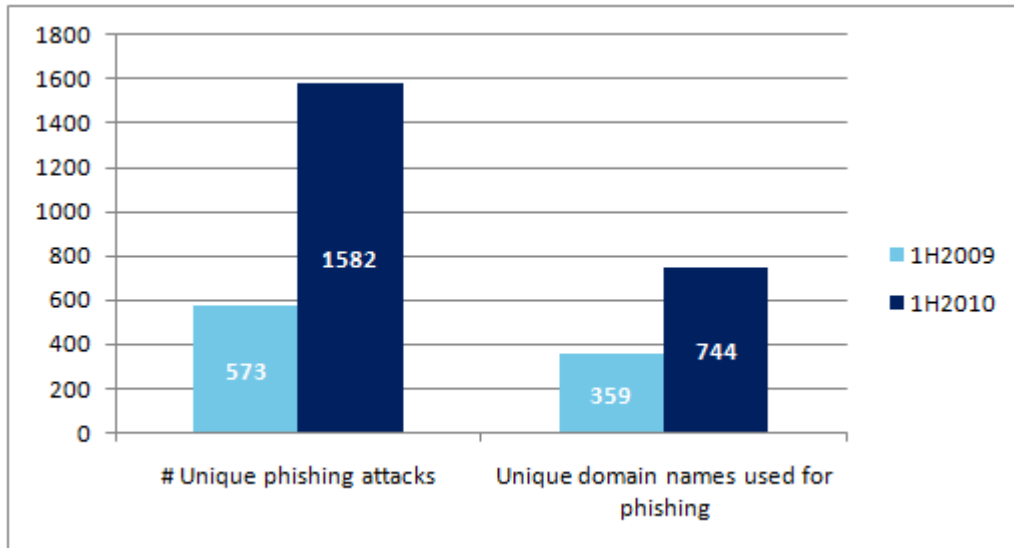
**Statistics on use of Internet by enterprises and related security aspects**

Fewer enterprises in Poland 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 1<sup>st</sup> half of 2010, and respectively for the 1<sup>st</sup> half of 2009, Poland was mentioned in the global report<sup>24</sup> published by the Anti-Phishing Working Group (APWG) with the following relevant statistics:



<sup>24</sup> See: *Global Phishing Survey: Trends and Domain Name Use 1H2010*, available at: [http://www.antiphishing.org/reports/APWG\\_GlobalPhishingSurvey\\_1H2010.pdf](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. Ministry of Interior and Administration	<p>The Ministry of Interior and Administration is responsible for information technology, national tele-information systems and national information administrative registers. The main tasks being realized by the Ministry of Interior included:</p> <ul style="list-style-type: none"> <li>• General state management;</li> <li>• Local government supervision;</li> <li>• Supervision over press and any associations;</li> <li>• Police issues.</li> </ul> <p>The ministry has the control over the Department of Information Technology Development, Information Society Department, and Center of Information Projects.</p> <p><i>Information Society Department</i></p> <p>The Information Society Department is under the responsibility of the Ministry of Interior and Administration. This department is composed by the following units:</p> <ul style="list-style-type: none"> <li>• Strategy and Coordination Unit for National Initiatives;</li> <li>• Coordination Unit for European Initiatives;</li> <li>• Structural Funds Unit;</li> <li>• Administrative Service Unit.</li> </ul> <p><i>Department for Information Technology Development</i></p> <p>The Department of Information Technology Development is under the responsibility of the Ministry of Interior and Administration. This department is composed by the following units:</p> <ul style="list-style-type: none"> <li>• Unit for Public Administration Information Systems;</li> <li>• Standardisation Unit;</li> <li>• Administrative Unit;</li> <li>• Support Unit for IT Projects Management.</li> </ul> <p><i>Department for State Registers and ICT</i></p> <p>The Department for State Registers and ICT is under the responsibility of the Ministry of Interior and Administration. This department is composed by the following units:</p> <ul style="list-style-type: none"> <li>• Planning and Coordination Unit for Radio and Telecommunications Systems;</li> <li>• Unit for ICT Infrastructure Systems Security;</li> <li>• Unit for Biometrics and Documents;</li> <li>• Certification Centre;</li> <li>• Unit for ICT Systems Maintenance;</li> <li>• Unit for Telecommunications and Teletransmission Systems Maintenance;</li> <li>• Unit for Registers Update and Data Verification;</li> </ul>	<a href="http://www.mswia.gov.pl/portal/en">www.mswia.gov.pl/portal/en</a>

National authorities	Role and responsibilities	Website
	<ul style="list-style-type: none"> <li>• Service Unit for Institutional Users;</li> <li>• General Unit;</li> <li>• Unit for State Registers Development;</li> <li>• Applications Maintenance Unit;</li> <li>• Individual positions.</li> </ul>	
<p>2. Ministry of National Defense</p>	<p>The Constitution gives the Minister of National Defence the right to realize the President's entitles to the supremacy over the Armed Forces during peace time.</p> <p>The Chief of the Staff and the commanders of different kinds of armed forces are submitted directly to the Minister of the National Defence. In the broad scope of the Minister of National Defence responsibility lie, among other things, such activities as:</p> <p>The management in peacetime all of the activities of the Armed Forces;</p> <p>The preparation of the assumptions of national defence, including proposals pertaining to the development and structure of the Armed Forces;</p> <p>The realization of the general assumptions, decisions and directives of the Council of Ministers in the area of national defence;</p> <p>The execution, within the scope of powers given by the Council of Ministers, of general supervision over the realization of defence-related tasks by the agencies and bodies of the State Administration, State institutions, local authorities, economic entities etc.;</p> <p>Overall leadership in matters connected with the execution of the common national defence duty;</p> <p>The fulfilling of international agreements, stemming from the decisions of the Council of Ministers, pertaining to the participation of Polish military contingents in international peacekeeping missions and humanitarian actions and military exercises conducted jointly with other countries or international organizations.</p>	<p><a href="http://www.wp.mil.pl/en/index">www.wp.mil.pl/en/index</a></p>
<p>3. Ministry of Infrastructure</p>	<p>The Ministry of Infrastructure is part of government administration that serves the minister responsible for issues related to construction, zoning and housing, maritime economy, communications, and transport.</p> <p>The Ministry is oriented to set directions, and also draft and improve solutions for national and international projects that fall within the scope of transport, maritime economy, communications, construction, spatial order and housing, and provide legislative foundation for their implementation</p>	<p><a href="http://www.en.mi.gov.pl">www.en.mi.gov.pl</a></p>
<p>4. Bureau of the Inspector General for the Protection of Personal Data (GIODO)</p>	<p>The main tasks of the Bureau of the Inspector General for the Protection of Personal Data Personal data protection are:</p> <ul style="list-style-type: none"> <li>• Supervision over ensuring the compliance of data processing with the provisions on the protection of personal data;</li> <li>• Issue administrative decisions and consider complaints with respect to the enforcement</li> </ul>	<p><a href="http://www.giodo.gov.pl/168/j/en">www.giodo.gov.pl/168/j/en</a></p>

National authorities	Role and responsibilities	Website
	<p>of the provisions on the protection of personal data;</p> <ul style="list-style-type: none"> <li>• Keep the register of data filing systems and provide information on the registered data files;</li> <li>• Issue opinions on bills and regulations with respect to the protection of personal data;</li> <li>• Participate in the work of international organisations and institutions involved in personal data protection.</li> </ul>	
<p>5. ABW (National Internal Security Agency)</p>	<p>The Internal Security Agency is a government institution which protects the internal security of the Republic of Poland and its citizens. Its primary objective is to know as much and as early as possible in order to effectively manage threats to the State's internal security.</p> <p>The ABW's status of a special service as well as its tasks and powers are regulated by a single law – the Internal Security Agency and Foreign Intelligence Agency Act of 24 May 2002. The ABW carries out its duties following both the spirit (rule) of legalism and the rule of law, which are characteristic of every single act undertaken by ABW officers. ABW is responsible for:</p> <ul style="list-style-type: none"> <li>• Investigation, prevention and combating threats against the State's internal security;</li> <li>• Investigation, prevention and detection of the crimes;</li> <li>• Carrying out, within the limits of its powers, the tasks of the state security authority and performing the function of the national security authority in relation to the protection of classified information in international relations;</li> <li>• Collection, analysis, processing and reporting to appropriate bodies information which may be significant to the protection of the State's internal security and its constitutional order.</li> </ul>	<p><a href="http://www.abw.gov.pl">www.abw.gov.pl</a></p>
<p>6. RCB (National Security Centre)</p>	<p>The Governmental Security Centre (RCB) is a state budget entity subject to the Prime Minister. It is a new solution in the Polish administrative system. It is the first such supraministerial structure, whose objective is the optimization and unification of the perception of threats by respective ministries, leading to a more efficient performance of their tasks related to crisis management.</p> <p>The mission and the main objective of the Centre is a comprehensive analysis of threats based on data obtained from all possible "crisis centres" existing within the framework of public administration, and on the information submitted by international partners. It shall enable the Centre to elaborate optimal strategies related to the arising crisis situations, and to play a pivotal role as the coordinator of the flow of information concerning the threats.</p> <p>The Centre is to give the Prime Minister, the Council of Ministers and the Governmental Crisis Management Unit the necessary support in decision-making related to security in the broad sense of the term by supplying them with the studies and analyses elaborated.</p>	<p>n/a</p>

National authorities	Role and responsibilities	Website
7. BBN (Bureau of National Security)	National Security Bureau is a body providing aid and support to the President of the Republic of Poland in executing security and defence tasks. National Security Bureau fulfils the tasks entrusted by the President related to security and defence matters. They result from the role of the President of the Republic of Poland as the supreme representative of the Republic of Poland and the guarantor of the continuity of State authority, responsible for ensuring observance of the Constitution, safeguarding the sovereignty and security of the State as well as the inviolability and integrity of its territory. Bureau's tasks result also from the constitutional function of the President who is the Supreme Commander of the Armed Forces	<a href="http://en.bbn.gov.pl">en.bbn.gov.pl</a>
8. Polish Committee for Standardisation	Polish Committee for Standardization (PKN) - a State Organizational Unit financed by the State budget recognized as a National Standards Body, the principal tasks of which are: Assessment of the state of the art and directions of standardization activity; Organization and supervision of publishing and dissemination of Polish Standards and other deliverables; Approval and withdrawal of Polish Standards and other standardization documents; Representation of the Republic of Poland in the international and regional standards organizations, participation in their work and representation of national interest abroad in matters concerning standardization; Initiating and organizing work of Technical Committees (KTs); Organization and conduct of training, publishing, promotional and informational activities with regard to standardization and related areas; Issuing opinions on draft executive acts related to standardization; Participation in the national notification system for standards and regulations.	<a href="http://www.pkn.pl/?lang=en">www.pkn.pl/?lang=en</a>
9. Office for Competition and Consumer Protection	The Mission of the Office of Competition and Consumer Protection is to improve the well-being of the consumers by creating adequate conditions for competition and its protection. They support the government of the Republic of Poland in the realization of the state's economic strategies and influence public authorities in order to raise their awareness regarding the hazards ensuing from anti-competitive and anti-consumer actions of entrepreneurs as well as of possible actions of the state.	<a href="http://www.uokik.gov.pl/en">www.uokik.gov.pl/en</a>
10. Office of electronic communications	The office regulates postal, telecommunications, and broadcast frequencies activities, and regulates electromagnetic compatibility. Among the tasks that the office is charged with are: ensuring that all citizens have access to universal service; ensuring a high level of protection for	<a href="http://www.en.uke.gov.pl">www.en.uke.gov.pl</a>

National authorities	Role and responsibilities	Website
	consumers in their dealings with telecommunications; encouraging a high level of personal data protection; and ensuring the integrity and security of the public telecommunications network.	
11. Polish chamber of commerce	<p>The Polish chamber of commerce is a polish business network, e.g., a local organization of businesses whose goal is to further the interests of polish business activities.</p> <p>The chamber of commerce gathers business owners in towns and cities form these local societies to advocate on behalf of the business community.</p>	<a href="http://www.chamberofcommerce.pl">www.chamberofcommerce.pl</a>

### Computer Emergency Response Teams (CERTs)

CERT	Role and responsibilities	Website
	<ul style="list-style-type: none"> <li>FIRST<sup>25</sup> member</li> <li>TI<sup>26</sup> listed</li> </ul>	
12. CERT POLSKA	<p>CERT POLSKA is the Computer Emergency Response Team Polska. The purpose of CERT Polska is to assist Polish internet users in implementing proactive measures to reduce the risks of computer security incidents and to assist them in responding to such incidents when they occur.</p> <p>CERT Polska also handles incidents that originate in Polish networks and are reported by any Polish or foreign persons or institutions</p> <p>CERT POLSKA is FIRST member and is TI Listed</p>	<a href="http://www.cert.pl">www.cert.pl</a>
13. CERT GOV PL	<p>CERT GOV PL is the Governmental Computer Security Incident Response Team. The Governmental Computer Security Incident Response Team is ensuring and developing the capability of public administration units to protect themselves against cyberthreats, in particular against attacks aimed at the infrastructure involving IT systems and networks the destruction or disturbing of which may considerably threaten the lives and health of people, existence of national heritage and the environment or lead to considerable financial loss or disturb the operation of public authorities.</p> <p>The CERT.GOV.PL team is a part of the IT Security Department at the Polish Internal Security Agency.</p> <p>CERT GOV PL is not FIRST member and is not TI Listed</p>	<a href="http://www.cert.gov.pl">www.cert.gov.pl</a>
14. PIONIER-CERT	<p>PIONIER-CERT is the Polish Scientific Broadband Network PIONIER CERT. The Polish Scientific</p>	<a href="http://cert.pionier.gov.pl">cert.pionier.gov.pl</a>

<sup>25</sup> More details available at: <http://www.first.org/members/teams/>

<sup>26</sup> More details available at: <http://www.trusted-introducer.nl/>

CERT	Role and responsibilities	Website
	<ul style="list-style-type: none"> <li>FIRST<sup>25</sup> member</li> <li>TI<sup>26</sup> listed</li> </ul>	
	<p>Broadband Network PIONIER CERT is a Computer Security Incident Response Team that has been established to provide effective incident response service to members and users of Polish Scientific Broadband Network PIONIER (and POL34/622). The main purpose of this initiative is to establish a single point of contact for all security incidents involving hosts classified as belonging to the constituency of PIONIER-CERT.</p> <p>The primary goal is to provide active incident handling with high quality technical support which can be guaranteed by five-year experience acquired by the Security Team of Poznan Supercomputing and Networking Center. As practical dealing with incidents is mainly related to the information analysis process, the team can also be considered as the coordination center managing actual responses and exchanging critical information among various interested parties.</p> <p>PIONIER-CERT is not FIRST member and is TI Listed</p>	
15. TP CERT (Telekomunikacja Polska)	<p>The TP CERT is the Telekomunikacja Polska CERT. Telekomunikacja Polska CERT is a Computer Emergency Response Team. TP CERT provides monitoring services for TP's constituency regarding network and computer security incident response and prevention.</p> <p>The main goal of TP CERT is to assist users of the TP network in implementing proactive measures to reduce the risks of computer security incidents, in particular by: providing consultancy and education services; providing information on network and computer security and warnings of possible attacks.</p> <p>TP CERT is not FIRST member and is TI Listed</p>	<a href="http://www.tp.pl/cert">www.tp.pl/cert</a>

### Industry organisations active in network and information security

Industry Organisations	Role and responsibilities	Website
16. KIGEiT (Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji)	<p>The Polish Chamber of Commerce for Electronics and Telecommunication (KIGEiT) is an independent organisation of economic entities involved in the manufacturing, export, import, trade, services and research and development work in electronics.</p> <p>Affiliating over 200 companies, KIGEiT is a member of EICTA (European Information, Communications and Consumer Electronics Technology Industry Associations).</p>	<a href="http://www.kigeit.org.pl">www.kigeit.org.pl</a>
17. PIIT (Polska Izba Informatyki i Telekomunikacji)	<p>Established in 1993, the Polish Chamber of Information Technology and Telecommunications (PIIT) brings together companies in the IT and telecommunications sector. At present PIIT has over 180 members. It is member of EICTA. Their</p>	<a href="http://www.piit.org.pl">www.piit.org.pl</a>

Industry Organisations	Role and responsibilities	Website
	<p>main tasks are :</p> <ul style="list-style-type: none"> <li>• Evaluation of Acts and decrees related to business in the sectors of information technology and telecommunication;</li> <li>• Formulation of opinions of the circles of interested professionals on the draft Acts and decrees of potential effect on the ICT;</li> <li>• Presentation to the government of the opinions of the IT and telecommunication circles on draft Acts and decrees, and lobbying for rational development of the ICT market;</li> <li>• Support and representation of the Chamber members at the administration agencies in matters of critical importance for relevant companies;</li> <li>• Furnishing media with information about events of importance for the IT and telecommunication companies;</li> <li>• Evaluation and furnishing of information to the Chamber members about potential effects of implementation of European Directives on the business running methods on the Polish and European ICT market;</li> <li>• Presentation of opinions and lobbying at European Commission and European Parliament;</li> <li>• Promotion of the Polish ICT market at the circles of the government, parliament, State administration and local-government administration;</li> <li>• Promotion of the Polish ICT and telecommunication companies on the EU markets;</li> <li>• Arbitration of business disputes and those concerning ownership of the Internet domains.</li> </ul>	
<p>18. The Polish Chamber for Electronic Communication (<i>Polska Izba Komunikacji Elektronicznej</i>)</p>	<p>The Polish Chamber of Electronic Communication (PIKE) represents 130 companies – broadband electronic communication operators and producers and distributors of equipment and services used by operators in their businesses. PIKE members serve over 4.5 million subscribers (75% of the market). PIKE supports members in their everyday business activity, representing their interests in relations with legislative bodies, the parliament, and the president, as well as many regulators and market participants. PIKE participates in the creation of legislation governing activities on the market, such as the Radio and Television Act, and telecommunications, copyright, and cinematography laws. PIKE represents the communications community with its most important business partners, such as broadcasters and copyright management organizations, as well as branch business partners such as self-government organizations from Poland and abroad. PIKE is also involved in educating its members on legal issues as well as supporting the implementation of ethical values in business. Twice a year, the chamber organises the PIKE Conference and Exhibition, which is the largest meeting for electronic media representatives in Poland.</p>	<p><a href="http://www.pike.org.pl">www.pike.org.pl</a></p>

## Academic organisations active in network and information security bodies

Academic Organisations	Role and responsibilities	Website
19. Academic Computer Centre in Gdansk - TASK ( <i>Centrum Informatyczne Trójmiejskiej Akademickiej Sieci Komputerowej</i> )	<p>Founded in 1994 by the State Committee for Scientific Research (KBN), the Academic Computer Centre in Gdansk (CI TASK) is an inter-university unit that manages one of the biggest and most modern metropolitan area networks (MAN) in Poland.</p> <p>The TASK network connects 70 LAN networks of various research institutes, in which over 6,000 computers, workstations, and servers are now installed. The network has about 16,000 users (not including students).</p>	<a href="http://www.task.qda.pl/english/">www.task.qda.pl/english/</a>
20. NASK	<p>NASK originally called as the Warsaw University Research and Academic Computer Network Coordinating Team is a research &amp; development organization and a leading Polish data networks operator.</p> <p>NASK offers state-of-the-art telecommunications and data solutions to business, administration and academic customers.</p> <p>NASK is the Polish national registry of Internet names in the .pl domain. The other main tasks of NASK are:</p> <p>Carry out scientific and research &amp; development activities in cooperation with the Faculty of Electronics and Information Technology of Warsaw University of Technology; Collects resources for the Polska.pl portal and its English language version; Provides service package comprising: broadband Internet access, corporate networks, data transmission, collocation and hosting, videoconference, as well as network security services.</p>	<a href="http://www.nask.pl/run/n/Who_we_are">www.nask.pl/run/n/Who_we_are</a>
21. The Academic Computer Centre CYFRONET AGH	<p>The Academic Computer Centre CYFRONET AGH, established over 30 years ago, is an autonomous organizational and financial entity of the AGH University of Science and Technology. The center currently employs around 60 people and incorporates the High-Performance Computing Department, Software Department, Computer Networks Department, Storage &amp; Security Data Department, Technical Department, Administration Department, Financial and Accounting Department, and the Operators Section. Furthermore, it includes the European Cooperation Group and the Research and Development Group.</p>	<a href="http://www.cyf-kr.edu.pl/en/">www.cyf-kr.edu.pl/en/</a>
22. ICM – Interdisciplinary Centre for Mathematical and Computational Modelling	<p>ICM is a center involved in scientific research, computational sciences, development and implementation research, education in computational science and modelling, and informational technology, as well as being a resource of knowledge and an organization strongly involved in the promotion of science.</p>	<a href="http://www.icm.edu.pl/web/guest/home">www.icm.edu.pl/web/guest/home</a>
23. Wrocław Centre for Networking and Supercomputing	<p>Wrocław Centre for Networking and Supercomputing is an organizational unit of Wrocław University of Technology. Founded in</p>	<a href="http://www.wcss.wroc.pl/english/">www.wcss.wroc.pl/english/</a>

Academic Organisations	Role and responsibilities	Website
	<p>1995, its main tasks include operation and development of the Wroclaw Academic Computer Network (WASK), operation and development of high performance computing services, and operation and development of network information services for all academic institutions in city of Wroclaw.</p> <p>The center is working on a project called Policy-based Security Tools and Framework (POSITIF) under the 6th Frame Programme of European Union. WCSO is responsible for management of the test bed for other project partners, workshops organization, knowledge dissemination in the security sector, and conducting scientific research on high-speed networks' security systems.</p>	

### Other bodies and organisations active in network and information security

Others	Role and responsibilities	Website
24. ISSA PL	<p>The Information Systems Security Association (ISSA) is a not-for-profit, international organization of information security professionals and practitioners. The mission of the ISSA is to enhance the knowledge and skills of its, encourage exchange of information security techniques, approaches, and problem solving, be the global voice of the information security professional, and promote best practices in information security.</p> <p>The Poland ISSA Chapter (ISSA PL) is an independent chapter of the Information Systems Security Association (ISSA). It facilitates, among other things, knowledge sharing events on various information security topics throughout the year in Poland.</p>	<a href="http://www.issa.com.pl/">www.issa.com.pl/</a>
25. OWASP PL	<p>The Open Web Application Security Project (OWASP) is an open-source application security project with local chapters. The OWASP community includes corporations, educational organizations, and individuals from around the world. This community works to create freely-available articles, methodologies, documentation, tools, and technologies. OWASP advocates approaching application security by considering the people, process, and technology dimensions. The chapter in Poland organizes local events such as the OWASP PL chapter meetings and specific events.</p>	<a href="http://www.owasp.org/index.php/Poland#OWASP_Poland_Local_Chapter">www.owasp.org/index.php/Poland#OWASP_Poland_Local_Chapter</a>
26. ISACA PL	<p>ISACA is a Worldwide association of IS professionals dedicated to the knowledge and good practices regarding audit, control, and security of information systems.</p> <p>The chapter in Poland organizes local events such as education and training, workshops, roundtables and other specific events</p>	<a href="http://www.isaca.org.pl">www.isaca.org.pl</a>
27. Nobody's Children Foundation (Polish Awarenode)	<p>The organisation is coordinator of Awarenode ('Safer Internet action plan' project together with NASK). Assistance to abused children, their parents, and guardians also in terms of Internet</p>	<a href="http://www.fdn.pl">www.fdn.pl</a>

Others	Role and responsibilities	Website
	abuse.	
28. Dyzurnet.pl (Polish hotline for reporting illegal content in the Internet)	Operating within NASK, Dyzurnet.pl is the hotnode within the 'Safer Internet action plan'. It is a member of INHOPE. Dyzurnet.pl responds to reports about illegal content on the Internet in Poland.	<a href="http://www.dyzurnet.pl/en">www.dyzurnet.pl/en</a>
29. SIC	Part of the European 'Insafe' Internet safety network under the 'Safer Internet' programme which aims to promote safer use of the Internet and new online technologies, particularly for children. Its goal is also to fight against illegal content and content unwanted by the end-user. The initiative is part of the EU's coherent approach.	<a href="http://www.saferInternet.pl/en">www.saferInternet.pl/en</a>
30. Kidprotect.pl Foundation	The Kidprotect.pl Foundation is the first organization in Poland that is dedicated to the safety of children on the internet. Active since 2002, Kidprotect.pl is a non-profit organization, depending on sponsor support and the work of volunteers. The Foundation does not use any public funds and does not pursue any business activity.  As part of carrying out the program Safe Internet ( <a href="http://www.bezpiecznyinternet.org">www.bezpiecznyinternet.org</a> ), it also conducts trainings for teachers, parents, educators, and crime prevention officers, as well as classes for children to learn how to practice internet safety.	<a href="http://www.kidprotect.pl/">www.kidprotect.pl/</a>
31. TP Group Foundation ( <i>Fundacja Grupy TP</i> )	This foundation is part of the European internet safety network INSAFE within the framework of the Safer Internet Programme, which aims to promote safer use of the Internet and new online technologies, particularly for children, and to fight against illegal and unwanted content, as part of a coherent approach by the European Union.	<a href="http://www.fundaciagrupytp.pl">www.fundaciagrupytp.pl</a>
32. FK (Polish Consumer Federation National Council)	A consumer organisation, its aim is to protect and educate consumers	<a href="http://www.federacja-konsumentow.org.pl">www.federacja-konsumentow.org.pl</a>

## 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](http://www.enisa.europa.eu/doc/pdf/deliverables/is_awareness_financial_organisations.pdf).
- Poland - ENISA CERT Directory: <http://www.enisa.europa.eu/act/blue/background/inv/certs-by-country/poland>.
- The Strategy for the Development of the Information Society in Poland until 2013 available in polish at [http://www.ezdrowie.lodzkie.pl/pliki/PL-MNiI-2005-Strategia\\_kierunkowa\\_rozwoju\\_informatyzacji\\_Polski\\_do\\_roku\\_2013.pdf](http://www.ezdrowie.lodzkie.pl/pliki/PL-MNiI-2005-Strategia_kierunkowa_rozwoju_informatyzacji_Polski_do_roku_2013.pdf) .
- More details about The Digital Agenda for Europe available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF> .
- The National Development Strategy available at <http://www.mrr.gov.pl/english/Strategies/srk/Documents/SRKwangielska0607.zip>.
- The National Computerisation Plan for the Period 2007-2010 available at <http://www.mswia.gov.pl/download.php?s=1&id=2674> .
- The Act on the Computerisation of the Operations of the Entities Performing Public Tasks available at [http://www.mswia.gov.pl/portal/pl/589/3886/Ustawa\\_o\\_informatyzacji\\_dzialalnosci\\_podmiotow\\_realizujacych\\_zadania\\_publiczne.html](http://www.mswia.gov.pl/portal/pl/589/3886/Ustawa_o_informatyzacji_dzialalnosci_podmiotow_realizujacych_zadania_publiczne.html) .
- The Act on the Protection of Personal Data available at [http://www.giodo.gov.pl/data/filemanager\\_en/61.pdf](http://www.giodo.gov.pl/data/filemanager_en/61.pdf) .
- The Telecommunication Law available at [http://www.en.uke.gov.pl/gallery/10/75/1075/Telecommunications\\_Law.pdf](http://www.en.uke.gov.pl/gallery/10/75/1075/Telecommunications_Law.pdf) .
- The Vision of Polish Armed forces 2030 available at [http://www.wp.mil.pl/pliki/File/vision\\_of\\_paf\\_2030.pdf](http://www.wp.mil.pl/pliki/File/vision_of_paf_2030.pdf) .
- More information about the eChallenges e-2010 website available at <http://www.echallenges.org/e2010/> .
- The 4th International Conference "Keeping Children and Young People Safe Online details available at [http://www.saferinternet.pl/konferencja\\_en/articles-2010/4rd\\_international\\_conference\\_keeping\\_children\\_and\\_young\\_people\\_safe\\_online.html](http://www.saferinternet.pl/konferencja_en/articles-2010/4rd_international_conference_keeping_children_and_young_people_safe_online.html).

