CYBERWELLNESS PROFILE
SLOVAKIA

BACKGROUND

Total Population: 5 480 000
(data source: United Nations Statistics Division, December 2012)

Internet users, percentage of population: 77.88%
(data source: ITU Statistics, 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- Criminal Law (Law 300/2005) Paragraphs § 247, § 283, § 196 and 197

- European Council Convention on Cybercrime

1.1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

- For banks: Law 483/2001 & Law 747/2004

- For public administration : Law 275/2006

- For telecommunication sector: Law 351/2011

- For Personal identifiable information: Law 122/2013

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Slovakia has an officially recognized national CIRT (CSIRT Slovakia).

1.2.2 STANDARDS

Slovakia has officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards through the Standardization committee for Information Systems of public administration (ISVS). Standardization committee is responsible for setting standards for ISVS on security, technical standards, data standards and project management standards.

1.2.3 CERTIFICATION

The national cybersecurity framework for accreditation and certification of information systems is regulated by the National Security Authority which is the main body of the state administration for the protection of classified information, and electronic signature.

The officially approved national cybersecurity framework for the certification of information systems used for the protection of classified information is regulated in the Act on the protection of Classified Information.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Slovakia has an officially recognized national cybersecurity strategy through the National strategy for Information Security (*). It defines strategic goals for Slovak Republic in various sectors such as protection of CII, awareness raising and capabilities building, ensuring secure environment, technical, operational and strategic controls, effective management of information security, protection and defence of public administration information infrastructure and national and international cooperation.

1.3.2 ROADMAP FOR GOVERNANCE

The Action plan to the [National Strategy for Information Security](#) defines tasks for various agencies in the field of information security and provides a national governance roadmap for cybersecurity in Slovakia.

1.3.3 RESPONSIBLE AGENCY

The national agency responsible for implementing a national cybersecurity strategy is the Ministry of Finance of Slovak republic (information security and protection of sector information technology in critical infrastructure). Other Ministries/agencies responsible for implementing specific areas of a strategy are:

- Ministry of Interior   -Ministry of Telecommunication (ISP)
- [National Security Authority (NBU)](#) (Protection of classified information, digital signature)
 -Ministry of culture (authors' law)   -Ministry of Justice (Fight against cybercrime)

1.3.4 NATIONAL BENCHMARKING

The national CIRT ([CSIRT Slovakia](#)) is the officially recognized national or sector-specific benchmarking exercise or referential used to measure cybersecurity development.

Slovakia has participated in cyber Slovak Information Security Exercise (SISE) on 2011, 2012 and 2013.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

Slovakia has officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines through the workgroups created by the Ministry of Finance, under the Committee of Standardization for various tasks including cybersecurity.

1.4.2 MANPOWER DEVELOPMENT

Slovakia has officially recognized national educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals through the Ministry of Finance of Slovak Republic (MF SR) project on cybersecurity which consists of systematic education of non-professionals in IT, managers and security professionals in field of cybersecurity in public administration.

1.4.3 PROFESSIONAL CERTIFICATION

There is no available information concerning any public sector professionals certified under internationally recognized certification programs in cybersecurity.

1.4.4 AGENCY CERTIFICATION

There is no available information concerning any certified government and public sector agencies under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Slovakia has officially recognized partnerships with the following organizations:

-[NATO](#)   -[FIRST](#)   -[OSCE](#)   -[European Union](#)

1.5.2 INTRA-AGENCY COOPERATION

The Themis project is the officially recognized program for information sharing platform for connected organization from public administration. The national CIRT (CSIRT Slovakia) mandates the sharing of cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

Slovakia has officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector through the Themis project and the national CIRT (CSIRT Slovakia).

1.5.4 INTERNATIONAL COOPERATION

Slovakia is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Slovakia also participated in the second Central European Cyber Security Platform (CECSP).

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instruments:
-§132 and §368-370* of the Criminal Code

2.2 UN CONVENTION AND PROTOCOL

Slovakia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the Convention on the Rights of the Child.
Slovakia has signed and ratified with no declarations or reservations to articles 2 and 3, to the Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

2.3 INSTITUTIONAL SUPPORT

There is no available information concerning any officially recognized agencies that offer institutional support in child online protection.

2.4 REPORTING MECHANISM

Online illegal content can be reported in the website of Stopline (*). Incidents can be reported in the website of the Computer Security Incident Response Team of Slovakia (CSIRT (*)).