Ministerstvo financií
Slovenskej republiky

EFQM

Aims fulfillment of the National Strategy for Information Security of the Slovak Republic

6th STAR Workshop on Digital Security
March 30, 2012

Ján Hochmann
Ministerstvo financií SR

Petra Hochmannová
CSIRT.SK / DataCentrum

Content of the presentation:

1. Global environment and framework
2. State analysis in the area of IS in the SR (till 2008)
3. Regulatory framework – legislation at the national level
4. Strategic documents
5. Action plan
6. Other important tasks
7. Critical Information Infrastructure Protection Exercises

1. Global environment and framework

1. Society and new activities:

- New professions (eCommerce, information exchange, information search, lottery),
- Videoconferences (long distance meetings and workshops),
- Free communication (consulting, statistics, analysis, price lists),
- Certification (new standards / norms, courses, eLearning),
- Copyrights, commerce law in the ICT environment,
- Social networks (mass media, Facebook, etc.),
- eGovernment
  - public electronic services and registers,
  - communication among public institution,
  - identification and authentication connected with providing services of the eGovernment,
  - the use of electronic signature for communication,
  - international and cross sectoral electronic interactions among European public institutions.

1. Global environment and framework

2. Internet and new technologies

- unlimited environment,
- limited regulations,
- electronic mail,
- free movement of goods and services,
- highly competitive environment (eCommerce – warehouse stock limitation, etc.),

- technologies based on Radio-frequency identification (RFID),
- biometric identification, barcode.

Usage:

Credit cards, ID cards and other chip card (eHealth, toll system, protection of goods and objects, industrial purpose, mass data processing and archives, eVouting, eCensus, etc.). It is difficult to set clear boundaries.

2. State analysis in the SR year 2008

1. Slovakia one of the weakest member of the EU
   - insufficient and inconsistent legislation,
   - insufficient proficiency of IS administrators,
   - low level of information security awareness (users and management),
   - unambiguous competence, duplicity and incompatibility of standards,
   - low level of international cooperation.
2. Information security survey in the SR 2008
   - undeveloped ISMS in public institutions,
   - absence of methodics and courses (eLearning < 4% employees; it is 3x less than the average of the EU),
   - IT processes managed by unqualified workforce,
   - inappropriate outsourcing.
3. Main task of the state – create conditions/ control mechanism!
   - creation of legislative framework, market regulation, supervision, sanctions.
   - Creation of conditions: organizational, technological, technical.
   - Awareness rising, education, competence.

3. Regulatory framework – legislation at the national level

- Act No. 215/2002 Coll. on Electronic Signature,
- Act No. 428/2002 Coll. on Protection of Personal Data ,
- Act No. 300/2005 Coll. Criminal Code,
- Act No. 618/2003 Coll. On Copyright ,
- Act No. 215/2004 Coll. on Protection of Classified Information,
- Act No. 275/2006 Coll. on Public Administration Information Systems + (Decree on Standards for Information Systems in Public Administration),
- Act No. 45/2011 Coll. on Critical Infrastructure,
- Act No. 351/2011 Coll. on Electronic Communications,

- Legislative intent of Information Security Act (anticipated term: year 2012)
- Legislative intent of eGovernment Act (anticipated term: year 2012)

4. National Strategy for Information Security of the SR (2008)

(Governmental Decree No. 570/2008)

Strategic aims:

1. prevention; adequate protection of the digital space in the SR, maximum prevention of the information security incidents,
2. preparedness; effective reaction on the information security incidents, minimization of the impact and recovery time,
3. sustainability; achievement, sustainability and development of competence in the area of information security.

Strategic priorities:

1. Protection of the human rights and freedoms in connection with the use of NIKI.
2. Increasing awareness and competence in the area of information security.
3. Creating a secure environment.
4. Effective ISMS.
5. Sufficient protection of the state ICI and ICI that supports the critical infrastructure.
6. National and international cooperation.
7. Strengthening the national competence.

4. Proposal of the System of Information Security Education in the SR

(Governmental Decree No. 391/2009)

Aim: elaboration of the specific area of the information security:

- Categorization of users: (6)
  1. Laics (cca 95%)
  2. Management
  3. Informatics – non-specialists in the area of IS
  4. Specialist in the area of IS
  5. Researchers
  6. Teachers

⇩

- Development of knowledge standard for 6 categories (2010),

⇩

- Development of methodics and syllabus (2010 / 2011),

⇩

- Pilot project – MF SR (2010 / 2011),

⇩

- Implementation into system of education in the SR - primary and secondary schools, universities, lifelong education (2012).

4. Proposal of organizational, personnel, material, technical a financial provision concerning the creation of a Computer Security Incident Response Team (CSIRT.SK) in the SR

(Governmental Decree No. 479/2009)

1. Establishment of CSIRT.SK:

- July 1st, 2009 (as a part of budgetary organization created by MF SR),
- development of statute and organizational structure,
- time horizon of the realization (2009 – 2012).

2. Aims of CSIRT.SK

- response to the information security incidents in the Slovak Republic in cooperation with the owners and providers of impacted parts of the national critical infrastructure, telecommunication operators, ISPs and other public bodies (police, investigators, courts),
- raising awareness in the certain field of information security,
- cooperation with international counterparts and organizations and representation of the Slovak Republic in the field of information security internationally.

4. Action Plan for the National Strategy for Information Security of the SR 2009 – 2013 *(Government Decree No. 46/2010)*

Basic pillars of the Action Plan

1.	Strategic aims	(3 aims from NSIS)
2.	Strategic priorities	(7 priorities from NSIS)
3.	Action plan	(8 areas)

Basic requirements:

- standardization of national legislation of Member States,
- security of products and services,
- consideration of democratic principles (citizen, entrepreneurs, public administration toward citizen).

5. Action Plan for the National Strategy for Information Security of the SR 2009 – 2013

Areas of the Action plan:

1. Prevention and preparedness:

   a) to develop national/ governmental CSIRT/CERT teams (till 2012),

   b) to adopt minimal standards in the area of information security,

   c) information sharing in the area of information security policy and the enforcement of mutual cooperation between public and private sector,

   d) to establish “Forum for information sharing“ among public institutions in the SR and later interconnection with other Member States for the purpose of information and best practices sharing in the area of security and critical infrastructures resilience.

2. Detection and reaction
   a) to create the early warning, information sharing and incident response system,
   b) effective ISMS,
   c) to establish Computer Security Incident Response Team Slovakia – CSIRT.SK,
   d) to adopt the Information Security Act (year 2011),
   e) to develop security teams CSIRT/CERT and support their mutual cooperation.

3. Mitigation and recovery
   a) to elaborate disaster recovery plans within public institutions,
   b) to organize regular national exercises on cyber security and critical infrastructure protection,
   c) to participate on international cyber exercises.

4. National and international cooperation

a) to ensure the resilience and stability of the Internet,

b) to prioritize state activities in order to ensure long-term resilience and stability of the Internet,

c) to elaborate principles and regulations for resilience and stability of the Internet,

d) to adopt the first concept of principles and regulations.

5. Criteria of critical infrastructure

a) to establish criteria for identification of critical infrastructure,

b) to elaborate methodics for ISMS,

c) to adopt the Critical Infrastructure Act and assure its interoperability with other obligatory legislative documents,

d) ISMS implementation (elaboration of methodics, conditions, best practices, recommendations).

6. Protection of human rights and freedoms

a) to analyze of the Act No. 428/2002 Coll. on Protection of Personal Data for possible modification,

b) legislative definition of the sensitive information,

c) legislative modification considering the access to personal and sensitive information.

7. Increasing awareness and competence

a) project of education and development of knowledge standard for targeted groups in the area of information security,

b) to implement the system of education for targeted groups,

c) to describe the qualification of the information security within national system of qualifications,

d) to design central access point to norms and standards.

8. Secure environment

a) to elaborate the common methodic for information and ICT systems classification,

b) novelization of the Decree on Standards for Information Systems in Public Administration,

c) to elaborate Information Security Act together with supporting documents.

6. Additional important tasks

Council Directive 2008/114/EC

of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

1. Act No. 45/2011 Coll. On Critical Infrastructure

enter into force on March 1st, 2011, responsibility – Ministry of Interior of the SR

Common, interim and final provisions

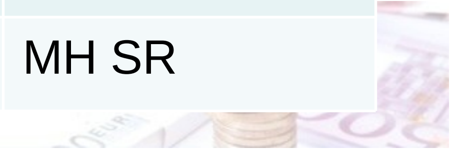
o Proposal of the sectoral criteria	May 31, 2011
o Proposal of the elements and establishment of sectors	October 31, 2011
o Risk analysis of sectors	October 31, 2012

2. Cross-departmental program on CIP

o Governmental decree No. 185 dated on March 26, 2008,	
o tasks of the Action plan	Year 2013

Sectors:

Sector	Subsector	Organization
1. Transport	Road, air, water, rail,	MTCRD SR
2. Electronic Communication	Satelite communication, Networks and stable and mobile services of electronic communications	**MTCRD SR**
3. Energetics	Mining, Electricity, Gas, Crude oil	ME SR
4. Information and Communication Technologies	Information Systems and Networks, Internet	**MF SR**
5. Post	Post services, system of payments and procurement activities	MTCRD SR
6. Industry	Pharmaceutical, metallurgical, chemical,	ME SR
7. Water and atmosphere	Meteorology, water construction, drinking water	ME SR
8. Health		MH SR



7. Critical Information Infrastructure Protection Exercises

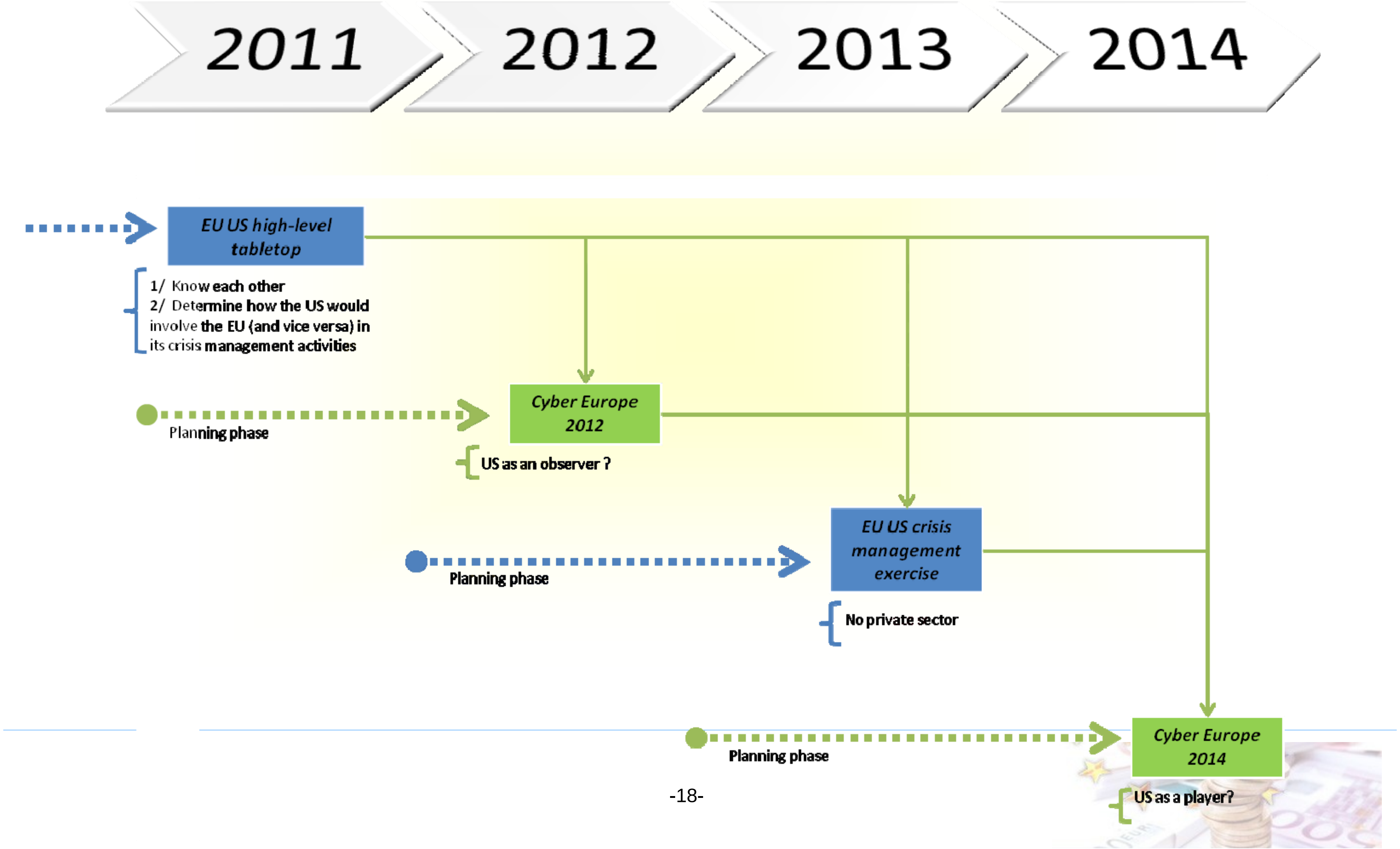
1. Cyber Europe 2010

- 1st Pan-European exercise on cyber security and Critical Information Infrastructure Protection – November 2010
- Organizer: European Network and Information Security Agency (ENISA) a Joint Research Centre and EU Member States (MS)
- Participants: 22 Member States as players and 8 Member States as observers, more than 150 experts from 70 public bodies around Europe
- Aims:
  - to establish trust in between actors within the MS, and between the MS,
  - to increase understanding of how management of incidents is done in different MS,
  - to test the communication channels, points and procedures,
  - to increase mutual support procedures during incidents or massive cyber attacks.

2. Cyber Atlantic EU – US 2011

- The first joint cyber security exercise between the EU and US was held on 3rd November in Brussels,
- Aim: to simulate cyber-crisis scenarios to explore how the EU and US would engage each other and cooperate in the event of cyber-attacks on their CII.

Plan - Cyber Atlantic EU – US 2011



7. Critical Information Infrastructure Protection Exercises

Planning and organization of „SISE 2011“

Organizer:	CSIRT.SK / Ministry of Finance of the SR
Players:	MI SR, MF SR, TRA SR, GO SR, DataCentrum, CERT.AT, CSIRT.CZ
Observers:	MD SR, CESNET-CERTS
Organized on:	November 23, 2011

- Scenario: To simulate Distributed Denial of Service Attack aimed at the availability of electronic services provided by public administration.
- Aims:
  - to verify the reaction of participating institutions on large scale security incidents,
  - to test the mutual communication,
  - to test the functionality of internal processes and procedures (disaster recovery and business continuity plans),
  - to build the trust at the national level.

Thank you for your attention

Ján Hochmann
MF SR
jan.hochmann@mfsr.sk

Petra Hochmannová
CSIRT.SK/DataCentrum
petra.hochmannova@csirt.gov.sk