ACT ON CYBER SECURITY

March 2016

Mgr. Jiri Maly
Head of the Legal Department
National Security Authority
Czech Republic

Responsibility for cyber security

Government Resolution no. 781, issued on 19 October 2011:

- assignes the responsibility for the cyber security to the NSA,
- establishes the Cyber Security Council,
- approves setting up of National Cyber Security Centre, which is part of the NSA.

Responsibility for cyber security

It gives tasks to the director of the NSA, which are:

- until 31 March 2012 make and submit the proposal of the legislative intent of the Act on cyber security,
- until 31 December 2015 build up fully functioning National Cyber Security Centre and Government CERT,
- until 31 July 2013 submit to the Government the proposal of the Act on cyber security (in co-operation with Minister of the Interior, Minister of the Defence and director of the National Security Service).

Moreover, the heads of central public authorities and director of National Security Service are obliged to co-operate with the NSA.

Legislative intent of the Act on cyber security

- Made by the NSA and approved by the Government resolution no. 382 issued on 30 May 2012.

- GR obliges the director of the NSA to create proposal of the Act on cyber security based on this intent and submit it to the Government until 31 July 2013.

Basic Principles of the Act

- Minimization of the infringements into the rights of private entities.
- Individual responsibilities for the own network´s security.
- Technological neutrality.
- Security measures (standards).
- Reporting of cyber security incidents.
- Counter-measures.

Scope of the Act

- The Act regulates rights and obligations of natural and legal persons and sphere of authority of state bodies in the field of cyber security.

- The Act shall not apply to information and communication systems handling classified information.

- There is an exception taking into consideration activities´ specifics of the Intelligence Services of the Czech Republic and police information system handling information about criminal procedure.

Definitions

Cyber Space

Cyber Security

Cyber space means digital environment, enabling to create, process and exchange information, created by information systems and services and electronic communication networks.

(Cyber security means a complex of legal, organizational, technical and educational means leading to ensure protection of cyber space).

Definitions

Information Security

Information Security means assurence of confidentiality, integrity and availability of information.

Cyber Security Event means an event which may cause breach of security of information in information systems or breach of security of services or breach of security and integrity of electronic communication networks.

Cyber Security Incident is breach of security of information in information systems or breach of security of services or breach of security and integrity of electronic communication networks as cyber security event result.

Definitions

Critical Information Infrastructure

Critical information infrastructure means an element or system of elements of the critical infrastructure (defined by another act) in the sector of communication and information systems in the field of cyber security.

Critical information infrastructure shall be determined under the procedure given in the Crisis Act (No. 240/2000 Col.) /CII is very close to CI and elements of CI/

Definitions

Important information system

Important information system means information system administrated by a public authority, that is not critical information infrastructure, and the breach of information security within such systém may restrict or noticeably endanger execution of responsibilities of public authority.

IIS and its determination criteria shall specify the implementing legislation.

Cyber space and CERT´S

CS – spliting into 2 parts – involving private sector

1. Under supervision govermental CERT
2. Under supervision national CERT

Governmental CERT – operated by the NSA CZE

National CERT – private entity – artificial person

National CERT - ensures information sharing on national and international level in the field of cyber security; it is usually run by a private-law entity. Is authorized to perform its activity on the basis of a public-law contract concluded with the NSA.

Liable Persons

Service providers
Critical Information Infrastructure
Important Information System

State bodies and natural and legal persons (further liable persons), which have duties in the cyber security field, are as follows:

a) electronic communication service provider and entity operating electronic communication network,
b) state body or natural and legal person operating important network,
c) administrator of a critical information infrastructure information system,
d) administrator of a critical information infrastructure communication system,
e) administrator of an important information system.

The Administrator means:
- as for information systems - subject which defines the purpose of the information processing and conditions for their operation.
- as for communication systems - subject which defines the purpose of the communication system and the conditions for their operation.

Liable Persons

Summary of Obligations

1) Implementation of security measures (CII + IIS).
2) Reporting of cyber security incident (INO, CII, IIS).
3) Announcing the contact details (all types).
4) Implementation of counter-measures (generally CII + IIS exception in case of the state of cyber emergency).

System for ensuring the Cyber Security

System to ensure cyber security consists of the following elements:

- **Security measures**
- **Reporting of the cyber security incidents**
- **Counter-measures**
- **Contact details notifications**
- **Activities of National and Government CERTs**

System for ensuring the Cyber Security

Security Measures – I. pillar

Security measures means a complex of activities, the purpose of which is to ensure information security in information systems and availability and reliability of services and electronic communication networks in cyber space.

These measures are obligatory for liable persons under letters c) to e). Their further specification is given by the implementing legislation.

Types of Security Measures:

- **Organisational Measures**
- **Technical Measures**

Organisational measures (e.g.)

- Information security management system
- Risk management
- Security policy
- Cyber security events and cyber security incident management
- Security requirements on suppliers setting
- Critical information infrastructure and important information systems control and audit
- Access of persons to critical information infrastructure or to important information system management

Technical measures (e.g.)

- Physical security
- Cryptographic devices
- Industrial and management systems´ security
- Cyber security event detection tools
- Collection and evaluation of cyber security events tools
- Counter malicious code protection tools
- Critical information infrastructure and important information systems, their users and administrators activities recording and monitoring tools

System of ensuring Cyber Security - security measures

- There is different scope of application of security measures for CIS and IIS.
- The administrators of CIS shall operate all technical and organizational measures. The administrators of IIS only some of them.
- Security measures are enlisted in security documentation. Structure of security documentation does not have to strictly follow the regulation, but the administrator has to prove, that the content is maintained, although in some other form.
- This duty is also fullfiled, when the administrator proves, that the IS is certificated under ISO/IEC 27001/2013 and submit appropriate documentation.

System for ensuring Cyber Security
Notification of incidents II. pillar

Obligation to detect Cyber Security Event and notify Cyber Security Incident is given by the Act (not for all Liable persons).

- Liable persons under letter b) - INOperators notify incidents to the national CERT.

- Liable persons under letters c) to e) notify incidents to the NSA/Government CERT.

Record keeping

The NSA CZE keeps cyber security incidents records, which contain:

- notification of the incident,
- IS´ identification data,
- data about origin of the incident,
- incident handling procedures, their results and countermeasures,
- data collected by the national CERT.

Incident record data are protected. Employees of the NSA CZE are bound by confidentiality about incident record´s data. Hovewer, the NSA may provide incident record´s data to the public authorities, the national CERT, bodies performing authority in the field of cyber security abroad and to other entities acting in the field of cyber security, to the extent necessary for ensuring protection of cyber space.

System for ensuring Cyber Security

Counter- Measures III. pillar

Counter-measures means the acts needed to protect information systems or services and electronic communication networks from threat in the field of cyber security or from cyber security incident or to solve actual cyber security incident.

Types of Counter-measures:

- **Warning**
- **Reactive Measure**
- **Protective Measure**

Warning

- The NSA shall issue warning in case it finds that the threat in the field of cyber security occurs.
- Warning is not legally binding.
- Warning shall be published by the NSA on its internet websites and shall be notified to liable persons via contact details from contact details evidence.

Reactive measures

- The NSA shall issue reactive measure to solve cyber security incident or to protect information systems or networks and electronic communication services from a cyber security incident.
- Reactive measure shall be issued in the form of decision or in the form of measure of general nature.
- Reactive measure is legally binding. It gives the duty to notify the execution of reactive measure and its result to the NSA.

Protective measures

- The NSA CZE shall issue protective measure in order to increase protection of information systems or networks and electronic communication services on the basis of already solved cyber security incident analysis.
- Protective measure shall be issued in the form of measure of general nature.
- Protective measure is legal binding.

System to Ensure Cyber Security
Contact details

- Liable persons shall be obliged to announce their contact details to the National CERT or to the NSA CZE. They will be obliged to announce also all changens in these contact details.

- Contact details means identification of liable person (e.g. name, address, identification number) and data of that natural person, who is authorized to act on behalf of the liable person in issues indetified by the Act (his/her name, phone number and e-mail address).

System for ensuring Cyber Security

Government CERT

- Receives the contact details notice from liable persons (CII and IIS).
- Receives cyber security incident reports from liable persons (CII and IIS).
- Evaluates cyber security incident data and cyber security event data of critical information infrastructure and important information systems.
- Cooperates with liable persons during cyber security incidents and cyber security events.
- Receives impulses and notifications from subjects, which are not liable persons, and analyses this data.
- Receives data from the National CERT and analyses this data.
- Receives data from bodies, performing authority in the field of cyber security abroad, and analyses this data.
- Provides the National CERT, bodies performing authority in the field of cyber security abroad and other entities acting in the field of cyber security with incidents record data.
- Analyses the vulnerabilities.

System to Ensure Cyber Security

Activities of CERT´S - National CERT

The administrator of the National CERT may be only:

- legal entity, which has experience with operating of IS and services and networks of electonic communications,
- has never acted againt the Czech Republic´s interest,
- fulfils technical requirements in cyber security field,
- participates in international cooperation with organizations functioning in cyber security field abroad (is a member of supranational organization acting in cyber security field),
- fulfils financial obligations against state, natural and legal entities,
- is irreproachable.

System for ensuring Cyber Security
Activities of CERT´S - National CERT

- Receives the contact details notice from liable person (not from CII and IIS), records and stores them.
- Receives cyber security incident report from liable person (only state body or natural or legal persons operating important network), records, stores and protects them.
- Evaluates cyber security incident of liable person (only state body or natural or legal persons operating important network).
- Acts as point of contact for liable persons and cooperates with them when cyber security incident occurs.
- Transmits to the NSA CZE the cyber security incident data without disclosing the announcer of the cyber security incident.

System to Ensure Cyber Security - State of Cyber Emergency

= a state, during which information security in IS or services or electronic communication networks security is seriously threatened and the interest of the Czech Republic may be violated or endangered.

- Enunciated by the NSA CZE Director.
- Valid for 7 days; may be extended by the NSA CZE Director, but total time period of a declared state of cyber emergency shall not exceed 30 days.
- Under the state of cyber emergency, the NSA is entitled to issue reactive measures to all types of liable persons.
- If it is not possible to avert the threat to information security in information systems or to security of services or electronic communication networks within the framework of the state of cyber emergency, the NSA CZE Director shall promptly ask the Government CZE to declare state of emergency (under the security act).

Control and Administrative offences

The NSA shall perform control in the field of cyber security.

The NSA determines how liable persons fulfil duties given by the Act, decisions and measures of general nature issued by the NSA and how they respect the implementing acts in the field of cyber security.

The control will be operated under the Control Order.

Determination of Critical Information Infrastructure

Determination under cross-cutting and sectoral criteria, which are in Government Regulation no. 432/2010 Col.

New section of the cyber security in Chapter VI.:

a) information system, which significantly or fully influences functioning of the determined element of critical infrastructure and which is replaceable only with disproportionate expenses or in time period longer than 8 hours,

b) communication system, which significantly or fully influences functioning of the determined element of critical infrastructure and which is replaceable only with disproportionate expenses or in time period longer than 8 hours,

c) information system administrated by the public authority, which contains personal data about more than 300 000 persons,

d) communication system enabling connection or link of the element of critical infrastructure, which capacity of guaranteed data transfer is at least 1 Gbit,

e) proportionate use of sectoral criteria mentioned in letters A. to F., if the protection of the element fullfiling these criteria is necessary for assurence of cyber security.

Important information systems

ISS named in Annex I of this regulation

All ISS has to fulfil determining criteria given by this regulation, which are divided to:

a) impact-determining and
b) sectoral.

ISS in Annex I are for example:

a) basic registers,
b) agenda information systems,
c) public administration portal,
d) IS of data mailboxes,
e) crime evidence, central car evidence, central drivers evidence etc.

Nowadays it includes more than 100 systems.

Transitional provisions

The Act formulates transitional period in which the liable persons are required to implement all the required measures.

Generally

- Liable persons are obliged to notify contact details within 30 days from entering into force of the Act or from their designation as liable person.
- Liable persons are obliged to implement security measures and implement cyber security incident report within 1 year from entering into force of the Act or from their designation as liable person.

Publication and Entering into force

The Act on cyber security was published on 29 August and entered into force on 1 January 2015.

Thank you for your attention.

Directive concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)

Legal Department

Národní bezpečnostní úřad

MILESTONES

- February 2013 – Presented in connection with the joint communication on a European Cybersecurity Strategy
- December 2015 – Unofficial political agreement between Council, European Parliament and Commission (reached during 6th informal trilogue)
- December 2015 – Officially approved at COREPER I meeting
- 1Q/2Q 2016 – Publication in the Official Journal of the European Union

GOALS

- Achieve a high common level of security of networks and information systems within the Union;

- Improve the functioning of the internal market (Legal base Art. 114 TFEU).

MAIN ELEMENTS

This Directive:

- Lays down obligations for all Member States to adopt a national NIS strategy;
- Creates a Cooperation Group and CSIRTs Network;
- Establishes security and notification requirements for operators of essential services and for digital service providers;
- Lays down obligations for Member States to designate national competent authorities, single point of contact and CSIRTs.

TRANSPOSITION

- Transposition period is **21 months**.
- Identification of operators of essential services has to be done in 21+6 months.
- The Cooperation Group and the CSIRTs Network shall begin to perform their tasks by 6 months after the date of entry into force of this Directive.

SCOPE

- 2 types of regulated entities:
  1) Operators of essential services
  2) Digital service providers („DSP“)

- Exemptions:
  1) Electronic communications networks and services
  2) Trust service providers

OPERATORS OF ESSENTIAL SERVICES

- **Defined as a public or private entity the type of which is referred to in Annex II, which meets the criteria laid down in Article 3a(1a).**
- Identified by the Member States
- Minimum harmonization principle

OPERATORS OF ESSENTIAL SERVICES – Determination criteria

- Under Art. 3a (1a):
  - An entity provides a service which is essential for the maintenance of critical societal and/or economic activities;
  - The provision of that service depends on network and information systems; and
  - An incident to the network and information systems of that service would have significant disruptive effects on its provision.
- The operators have to fall within one of sectors (subsectors) in Annex II:
  - Energy (Electricity, Oil, Gas), Transport (Air, Rail, Water, Road), Banking, Financial market infrastructures, Health sector, Drinking water supply and distribution, Digital infrastructure

DIGITAL SERVICE PROVIDERS

- **Defined as any legal person that provides a digital service.**
- The Member States have no discretion in their identification.
- Maximum harmonization principle
- „Light touch“ approach

DIGITAL SERVICE PROVIDERS - Identification

- DSPs are the entities, which fall within the types listed in Annex III (online marketplaces, online search engines, cloud computing services); **and**
- They fall under the definition of these entities; **and**
- They are not microenterprises or small enterprises as defined in Commission Recommendation 2003/361/EC of 6 May 2003.

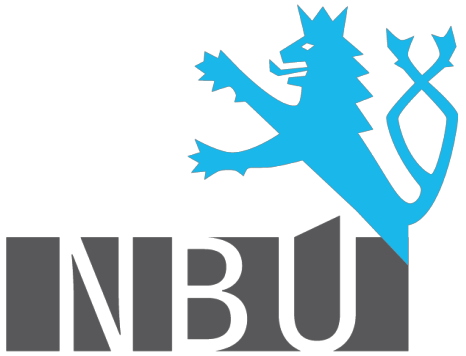
CZECH POSITION

- The Czech Republic supported this initiative in general…….
- ……apart from the DSP regulation.
- We did not support DSPs inclusion into the Directive´s scope, because:
  - Their regulation might implicate the control of the content on the Internet;
  - Most DSPs have already implemented measures to secure their networks and information infrastructures;
  - National Competent Authorities might be overloaded by administrative work;
  - DSPs regulation might disadvantage the EU´s digi market in comparison to the rest of the world.

CONCLUSION

- Therefore:
  - The Czech Republic and some other Member States opposed the DSPs regulation or required at least lighter regulation and narrower scope.
- As a compromise:
  - DSPs regulation is lighter than for operators of essential services.
  - Social networks were excluded.
  - Micro and small enterprises were excluded.

Thank you for your attention!



Národní
bezpečnostní
úřad