Critical information infrastructure remarks

Josef Kaderka
University of Defence, Department of CIS,
Kounicova 65, 662 10 Brno, Czech Republic

josef.kaderka@unob.cz

Abstract. The cyber security law no. 181/2014 which came into effect since 1 January 2015 in the Czech Republic. It defines several terms and ordered to adopt rules for the organizations which deal with critical information infrastructure. The National Security Authority has been set as responsible body, inside which the the National Cyber Security Centre has been created. University of Defence has to respect mentioned law, so more measures were accepted as depicted.

Keywords: critical information infrastructure, cyber defence, CERT, CIRC

1 Introduction

Over the past 25 years, the society in terms of exchange of information has completely changed. Specialized systems such as telex or analog telephone, either completely disappeared or recede into the background. Today is the basis of the functioning of it the information infrastructure, which is based on several basic areas. These are especially computer networks (using IPv4; yet not IPv6) and associated network equipment - for the backbone networks supplied by a few manufacturers. Furthermore, there are end devices with some operating systems like Android, iOS, Linux / Unix or Windows and application software. Malfunctioning merely of the part of the information infrastructure can suddenly affect a wide range of spheres, which would not happen before. Therefore, it is necessary to pay care information infrastructure protection at the country level, which requires legislative support.

The Czech Republic has specified the term "critical information infrastructure" in law no. 181/2014 Coll. (cyber security law) [1], which came into effect from 1 January 2015. In it, it says that "critical information infrastructure is an element or a system of elements of the critical infrastructure in the branch of the communications and information systems". This law does not apply to information or communications systems that handle classified information.

2 Fundamental cyber security law impacts

The National Security Authority (Národní bezpečnostní úřad in Czech language) has been previously designated by the government resolution as a coordinator for cyber security issues as well as national authority for this area. The resolution further decided to establish the National Cyber Security Centre, as part of the National Security Authority, based in Brno. The main areas of Centre activity are:

- Operate Governmental CERT Czech Republic (GovCERT.CZ),
- Cooperation with other CERT teams and CSIRT teams,
- Cooperation with international CERT teams and CSIRT teams,
- Preparation of security standards for various categories of organizations in the Czech Republic,
- Raising awareness and promoting education in cyber security,
- Research and development in cyber security.

The cyber security law also envisages the creation of a National CERT, which among other things ensures the sharing of information on national and international level in the field of cyber security. Any legal entity which meets the requirements of the law can become an operator of the National CERT. At present, the organization CZ.NIC gives patronage for the National CERT. The law also envisages the possibility of declaring a state of cyber endangerments and appropriate steps.

This law is complemented by two decrees of the National Security Office, no. 316/2014 Coll., "On security measures, cyber security incidents, reactive measures and establishing the requirements for filing in cyber security" [2], as well as no. 317/2014 Coll., "On important information systems and their underlying criteria" [3].

Cyber security law regulates the rights and obligations of the parties as well as the powers and responsibilities of public authorities in the field of cyber security. Its main purpose is to protect the functioning of national part of the cyberspace. It differentiates cyber security measures on technical and organizational ones; especially the organizational measures need to be addressed.

One of the objectives of the cyber security law is to establish an approach to the mutual communication among entities. An exchange of information cyber security related information should be unified both in the governmental and also private spheres; the law directly establishes essential fashion of their conjunctive communication. Already mentioned National Cyber Security Centre has supervisory and executive powers. It unifies the cyber security of the country, so it should be easier to not only recognize, but to actively face the attacks on cyber level.

The minimum intervention into private sphere and the responsibility of the entities for their systems security are the focal principles the cyber security law. It is conceived on three basic institutes:

- Security measures standardization
- Cyber security incidents reporting
- Countermeasures (computer emergency response, attack or the occurrence of the incident)

The standards are set in the form of organizational security measures, which go mainly to the procedural matters, as well as technical measures, which use primarily system and technological solutions.

The decree on security measures defines 21 sets of security policies, of which 10 are common to all required subjects. The specified liable subject establishes the security policies in following areas:

- Information Security Management System,
- Organizational security,
- Supplier management
- Classification of assets that includes rules for the secure disposal of the assets,
- Human resources security
- Traffic management and communications,
- Access control,
- Secure user behavior,
- Use cryptographic protection, and
- Deployment and use of tools for detecting cyber security incidents.

The notion of critical information infrastructure, however, is subordinated to the notion of critical infrastructure, which is defined in the law no. 240/2000 Coll. on crisis management [5] as follows: "Critical infrastructure (is) an element of critical infrastructure system or elements of critical infrastructure, disruption of the function of which would have a serious impact on national security, on basic living needs of the population provisioning, human health or the economy of the country." Specifically, it also mentions information and communication systems, but without particular elaboration.

3 Common critical infrastructure

Critical infrastructure consists of elements or systems of elements (buildings, equipment, facilities or public infrastructure) and their operators. The vital role here plays the government decree 315/2014 Coll. [6], which handles with the concepts of cross-cutting criteria and sectoral criteria. Briefly may be cited:

Cross-cutting criteria for determining critical infrastructure element:

- Victims with a limit value of more than 250 deaths or more than 2,500 people stay in hospital for longer than 24 hours,
- Economic impact results in losses to the country higher than 0.5% of gross domestic product, or
- Impact on the public to limit the extensive restrictions on the provision of essential services or other serious intervention in everyday life involving more than 125,000 people.

The sectoral criteria for determining critical infrastructure element:

- Specification of technical and operational values and extent of the impact of disruption of their function

Critical infrastructure elements determine the ministries and central administrative authorities. Their operators have to prepare the "Plan of emergency preparedness subject of critical infrastructure" for protection and recovery actions during crisis situations handle.

3.1 Critical infrastructure and critical information infrastructure

From the above text, it is apparent that although the critical information infrastructure is by the legislative standards conceived similarly like transport infrastructure or energy one, it has a completely different character. The main difference is it complexity, there is no some level of centrally management. It is composed of approximately parallel structures operated solely by private (and limited governmental) entities doing business in the field of communication and information systems, eventually carrying such systems for their own use.

For this reason the legislative standards introduce the concept of “significant information systems”, only their operators must meet the requirements of that legislation. Criteria for the classification of the significant information system among significant ones are rather extensive, as examples may be mentioned:

- Information system managed by a public authority containing personal data on more than 300 000 persons, or
- Communications system providing access to or connection among element of critical infrastructure with a guaranteed data transmission at speed at least 1 Gbps.

The number of already identified significant information systems is quite high. For example the Annex no. 1 of decree no. 317/2014 Coll. knows 92 such systems. The Czech Ministry of Defence significant information systems published here are following:

- Biological monitoring and information system,
- Information system of mobilization preparations,
- Information system of service and personnel,
- Military police information system,
- LETVIS (Automated data processing and operations of the airspace management),
- SVZ ARMS (Early warning military radiation monitoring network),
- Staff Information System
- Medical information system

3.2 Critical information infrastructure protection and vulnerabilities

The evaluation of the level of protection of communication and information infrastructure within country as a whole is a very complex stuff. For example, the true analysis of the real weaknesses of communication and information infrastructure of one entity necessitates a thorough knowledge of locations, connections routes, applied technology including software versions, power supply providing etc. Such

information is usually protected respectively it is part of internal company know-how; that is further emphasized by the cyber security law. Mentioned analysis would be needed for each communication and information infrastructure of all entities, as well as their interrelations considering etc.

We cannot expect that these bodies will provide the necessary information without legal obligation, regardless of the enormous range of sources that need to be processed. Finally, it would be necessary to decide whether such information should not be classified according law 412/2005 Coll. [7].

The surveys of vulnerabilities need some kind of penetration testing - like. It is augmented by yet another aspect - once a serious vulnerability is found, it is usually quickly patched. Such surveys have more research than operational aspects (it identical like in the case of antiviruses). Finally, it is then necessary take in account that important communication and information systems surely consider security aspects, are managed by qualified personnel, etc. Of course, the risks can rise from lack of funds or financial cuts.

It is obvious from the above that it is considerably difficult to define the general vulnerabilities of the critical information infrastructure, especially if it is understood as described in the cyber security law.

As an option seems to proceed in the form of creating an overview of threats, which would, however, had to be constantly updated. Since that review is possible to derive the requirements for countermeasures testing.

The potential vulnerability of critical information infrastructure can be outlined in the example of used technologies. For example, the number of manufacturers of high-performance network devices is fairly limited and therefore operators of communication and information systems do not have too much choice. If in a particular technology will vulnerability it is sure to affect a whole range of these operators.

An examples are the OpenSSL problems, which is an open source implementation of the protocols of SSL and TLS. It provides a library written in C language, which includes basic cryptographic functions. OpenSSL is very frequently used means for implementing security functions of various devices including network ones for its good security features. But in the past, several serious multiyear vulnerabilities has been found, such an implementation error by Linux distribution Debian (2008) or very serious error in the implementation of the expansion of Heartbeat (2014).

Another approach could be based on the perspective of the standards required for the area of communication and information systems and the level of their fulfilment.

3.3 Threats and their classification

Example of a possible classification of threats for communication and information systems might look like this:

- Human,
- Technology,
- Caused by other factors.

Another view is then threats parting:

- Internal,
- External.

Further on:

- Intentional (willful),
- Unintentional.

Mentioned threats are closely linked to vulnerabilities. It should be borne in mind that the more complex application or the operating system are, the higher risk of programming errors is. It also means greater degree of threat and inclination to misusing by an attacker.

Mentioned division is not an exhaustive or definitive list, but it can indicate threats that do not have closely cyber character as is usually assumed. These include the use of an unauthorized device theft or loss of data storages or entire devices.

- Malicious software - particularly the threat of malware (viruses, worms, Trojan horses, etc.), affected devices can become part of a network of infected and remotely controlled devices called botnet. In addition to online mechanisms, malware can spread via external devices, today primarily through flash drives (also MP3 players, camera memory cards etc.),
- Unauthorized use of the equipment, systems or their unauthorized administration – the cause is inconsistent adherence to safety rules or policies, intentional or unintentional; a threat is unjustified confusion of roles in the system, for example due to lack of staff,
- Improper use of equipment or systems - using applications, devices or systems in any other way than as laid down, which can lead to physical damage or loss of data integrity or trustworthiness,
- Unauthorized physical access to the device - can occur when the device is stolen, causing loss of sensitive data; the risk are also equipment repairs carried out by external subjects, when confidential data can be taken off as result of omission,
- Data communications eavesdropping – the defence is rigorous encryption, classified information transfer can be executed through legally approved procedures or certified equipment,
- Identity and personal data thefts – it can be the consequences of the forgeries or fiction through theft of sensitive data or misuse of someone else's credentials,
- •Unauthorized publishing of sensitive information - the result of unauthorized access to information, insufficient erasure or destruction of discarded memory media or theft, espionage, action malware etc.,
- •Social engineering - those affecting of the victim, that he/she can expose of sensitive information or access rights to facilities or systems to an attacker, some forms are referred as a phishing,
- Improper manipulation with hardware, software, and information – it is usually a continuation of unauthorized access. It can results in loss of availability, integrity, credibility and integrity of data,

- Denial of service - putting the victim's system into status when it stops providing services to authorized users,
- Loss of data device - particularly dangerous for poorly protected mobile devices such as smartphones, tablets, laptops, flash drives, etc.,
- Loss of data - can go on environmental factors, aging of materials, power outages, human error etc.; if backups are not made out,
- Data integrity violation - archive data carriers as results of improper storage condition etc.

4 Information infrastructure protection at University of Defence

The range of the University of Defense communication and information infrastructure is proportional to the size of the institution and satisfies its needs. The manipulation with classified information is dealt with separately, takes place in accordance with relevant legal standards. Systems, where classified information is processed, are physically separated from the university computer network.

University computer network enables communication with the Internet, but also access from the Internet to selected information sources in the internal network. Some sources of information are available to the public, others only for specific users. In the second case, identification and authentication of users is then required, in that case the communication is protected by encryption either on application level or using virtual private network (VPN).

There are some unclassified information, but protected by other legislative standards available to selected users in the university computer network [4]. These include personal data, study results or a departmental data. Dedicated, centrally managed computers with more restrictive security policy serve to access to that data.

The University of Defence is in ambiguous situations from the perspective of the cyber security law. As early as first section of the law says that it "governs the rights and obligations of the parties and the scope and powers of public authorities in the field of cyber security." The university rector is taken as public authority according another law. However, the University of Defence has no, in contrary with civilian equivalents, legal independence, which belongs to the Ministry of Defence. The legislative standards issued by the Ministry of Defence are mandatory for University of Defence. These questions and others are currently under negotiation.

3.3 Areas of information infrastructure protection

Protection of [communication and] information infrastructure can be divided into several areas.

The first is the area of personnel, which is currently problematic place. Until now, all activities related to security were carried out by employees concurrently with their primary tasks. The increasing of duties imposed by legislation will likely evoke either to change or to the personal empowerment.

The second is an organizational area, i.e. to establish the rules for the use of communication and information infrastructure in the form of directives and

regulations. These rules reflect the general, but especially departmental legislative standards.

The third area is technical, respectively system one. It falls within the range of measures at the university, but also outside. The user's roles or categories are defined within university, from which then arise privileges to specific persons. Said identification and authentication solution utilizes mostly Microsoft solutions, which cooperate with some other information systems; then there is a link for example through RADIUS protocol. Regular user's workstations are incorporated into Microsoft domain; installing patches, updating software, etc. is therefore managed centrally. Special rules are used for students, for example maximum possible amount of data transferred by them in a certain period, or access to Eduroam network.

3.4 Details and CESNET security role

University of Defence (Brno part) is connected to the Internet through CESNET association of legal entities (university itself is a member of it) at rate of 1 Gbps with prospects of upgrade to 10Gbps. Virtual private network (in Internet) ensuring also ensure data security are used for communicate with branches in Hradec Králové, Vyškov etc.

The connection is realized through a very powerful device with the operating system Linux. In addition to routing it provides the firewall function - selective filtering operation (several thousand rules), some features like VPN gateway, monitoring etc. It is based on carefully selected computer Barebone SYS-6047R-TXRF (SuperMicro motherboard X9DRX + F, 2 Intel Xeon processors E5-2670 8C, 8GB RAM, network adapters Intel 82599ES - 10 Gb/s). It operates for very short period, but appears as a very satisfactory (details later).

Inbound and outbound traffic is also monitored by an autonomous FlowMon probe INVEA. It provides basic information on flows and allows detecting different kinds of anomalies. It has no possibility to examine the transmitted data as such.

An important part of security measures consists of e-mail security. It consists of several components, which mainly prevent the receipt of e-mails from unreliable sources (usually because a spam message), and e-mails carrying dangerous content. Unreliable sources are identified by the means of so-called greylists. Content is analysed on the basis set of signatures (for example, attachments containing executable files are disabled etc.).

The CESNET association plays very important security role for University of Defence. It has its own security software tools, methods and relevant specialists with continuous operating time. University of Defence, as a member organization takes advantage of these services - they are for it free. The information on suspicious activity as against and coming out of Defence University network are passed in real time. Information is distributed through e-mail, or by phone in emergency situation.

5 Conclusion

Protection of critical information infrastructure requires a number of measures which are generally determined by legislative standards in the Czech Republic, especially by the cyber security law. Those standards deal mainly with organizational and systemic issues such as general measures, appropriate sets of rules, means of communication and contacts, obligation to disclose incidents etc. It does not address the specific technical procedures, particular application software etc.

As the critical information infrastructure is made up of the sum of individual system operators, only a general answer can be found when requesting an analysis of its vulnerabilities.

University of Defence operates medium size communication and information infrastructure. This infrastructure is now sufficiently secured from the technical point of view, there are still problems with fulfilling of legal imperative due to unclarity.

References

1. Předpis č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti; Cyber Security Law). http://www.nbu.cz/cs/pravni-predpisy/zakon-c-4122005/, http://www.nbu.cz/download/nodeid-1014/
2. Předpis č. 316/2014 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti; Decree On Security Measures). http://www.zakonyprolidi.cz/cs/2014-316
3. Předpis č. 317/2014 Sb. Vyhláška o významných informačních systémech a jejich určujících kritériích. (Decree On Important Information Systems) http://www.zakonyprolidi.cz/cs/2014-317
4. Předpis č. 101/2000 Sb. Zákon o ochraně osobních údajů a o změně některých zákonů (Private Data Protection Law). http://www.oou.cz/pravnipredpisy/zakon101200.
5. Předpis č. 240/2000 Sb. Zákon o krizovém řízení a o změně některých zákonů (krizový zákon; Crisis Management Law). http://portal.gov.cz/zakon/240/2000
6. Předpis č. 462/2000 Sb. Nařízení vlády k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon).
7. Předpis č. 315/2014 Sb. Nařízení vlády, kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.
8. Předpis č. 412/2005 Sb. Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti (Protection of Classified Information Law). http://www.nbu.cz/cs/pravni-predpisy/zakon-c-4122005/, http://www.nbu.cz/download/nodeid-904/
9. Předpis č. 523/2005 Sb. Vyhláška o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor.
9. Předpis č. 525/2005 Sb. Vyhláška o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací.