UDC 004.056.5

CONCERNING MEASURES FOR A HIGH COMMON LEVEL OF SECURITY OF NETWORK AND INFORMATION SYSTEMS ACROSS EU

Libor Dostalek
University of South Bohemia, Ceske Budejovice, Czech Republic, DsC., professor

The base of EU cooperation is free market. The possibilities of free market becomes larger. Typical example are payment services. In case of retail, they are practically limited to national states because numbers of barriers limits them. Such barriers are e.g.:

- Every bank uses proprietary electronic banking
- Possibility to open the first account in foreign bank without the physical presence there is very complicated.

EU wants to reduce barriers of the common market, it has issued many legislative standards, which are already being implemented on a software basis:

- Directive PSD2 [1] separates payment services from electronic banking (similar to separation of the electric energy production from its distribution).
- Directive AMLD4 [2] enables to create first accounts of physical persons remotely if these persons will authenticate themselves with the electronic identification based on the eIDAS Directive [3].

Software suppliers are developing software, which enables clients to have accounts of many banks within one electronic banking. It is assumed that most of these accounts will be created remotely outside this software. Particular EU member states should enable such communication within two years.

Constantly increasing liberalization of the European market requires introduction of various defence mechanisms against cyber-attacks.

For these reasons, the "Directive EU 2016/1148 concerning measures for a high common level of security of network and information systems across the Union" [4] was created.

We have to remember that the EU can only address security in areas where it allows the Treaty on the Functioning of the European Union (TFEU). In accordance with Article 346 of the TFEU, no Member State is to be obliged to supply information the disclosure of which it considers to be contrary to the essential interests of its security.

From the point of view of national states, some areas are addressed globally and some are addressed at a national level. For example in the military area, the EU has no competence; this area is solved completely independently (but it can use similar mechanisms, e.g. at NATO level of cooperation).

Directive EU 2016/1148

The magnitude, frequency and impact of security incidents are increasing, and represent a major threat to the functioning of network and information systems. Those systems may also become a target for deliberate harmful actions intended to damage or interrupt the operation of the systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union.

To that end, this Directive provides for the assessment of the entities active in specific sectors and subsectors, the establishment of a list of essential services, the consideration of a common list of cross-sectoral factors to determine whether a potential incident would have a significant disruptive effect, a consultation process involving relevant Member States in the case of entities providing services in more than one Member State, and the support of the Cooperation Group in the identification process.

Directive define:

- "Digital service" - means any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.
- "Essential services" and "operators of essential service". The criteria for the identification of the operators of essential services, shall be as follows:

(a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;

(b) the provision of that service depends on network and information systems; and

(c) an incident would have significant disruptive effects on the provision of that service.

Directive EU 2016/1148 (in Article 1):

(a) lays down obligations for all Member States to adopt a national strategy on the security of network and information systems;

(b) creates a Cooperation Group in order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence amongst them;

(c) creates a computer security incident response teams network ('CSIRTs network') in order to contribute to the development of trust and confidence between Member States and to promote swift and effective operational cooperation;

(d) establishes security and notification requirements for operators of essential services and for digital service providers;

(e) lays down obligations for Member States to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information systems.

Each Member State shall designate one or more national competent authorities on the security of network and information systems ('competent authority') and national single point of contact on the security of network and information systems ('single point of contact'). The single point of contact shall exercise a liaison function to ensure cross-border cooperation of Member State authorities and with the relevant authorities in other Member States and with the Cooperation Group.

Each Member State shall designate one or more Computer security incident response teams (CSIRTs) responsible for risk and incident handling in accordance with a well-defined process. A CSIRT may be established within a competent authority mentioned in previous paragraph.

In order to contribute to the development of confidence and trust between the Member States and to promote swift and effective operational cooperation, a network of the national CSIRTs is hereby established. The CSIRTs network shall be composed of representatives of the Member States' CSIRTs and CERT-EU. The Commission shall participate in the CSIRTs network as an observer. European Union Agency for Network and Information Security (ENISA) shall provide the secretariat and shall actively support the cooperation among the CSIRTs.

In order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence, and with a view to achieving a high common level of security of network and information systems in the Union, a Cooperation Group is hereby established. The Cooperation Group shall be composed of representatives of the Member States, the Commission and ENISA.

Member States shall ensure that (Article 14):

- Operators of essential services take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed.
- Operators of essential services take appropriate measures to prevent and minimize the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services.
- Operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident. Notification shall not make the notifying party subject to increased liability.

Act on Cyber Security of Czech Republic

Czech Act No. 181/2014 can be understood as part of national strategy on the security of network and information systems. This Act introduce two Czech CSIRTs: 'National CERT' and 'Governmental CERT'.

Act define 'Critical information infrastructure', which means an element or system of elements of the critical infrastructure in the sector of communication and information systems within the field of cyber security. In additional define 'Important information system' which means an information system administrated by a public authority, that is not critical information infrastructure and which may endanger or noticeably limit the performance of public administration in case of information security breach.

But the devil is hidden in detail. To this law, there are relatively detailed regulations that define the requirements for unilateral measures that divide into organizational and technical.

Act require organizational measures are as follows:

a). Information security management system,
b). Risk management,
c). Security policy,
d). Organisational security,
e). Security requirements on suppliers setting,
f). Assets management,
g). Human resources security,
h). Critical information infrastructure or important information system operation and communication management,
i). Access of persons to critical information infrastructure or to important information system management,
j). Acquisitions, development and maintenance of critical information infrastructure and important information systems,
k). Cyber security events and cyber security incidents management,
l). Business continuity management and
m). Critical information infrastructure and important information systems control and audit.

Define Technical measures are as follows:

a) Physical security,
b) Communication networks integrity protection tools,
c) Users' identity verification tools,
d) Access authorization management tools,
e) Counter malicious code protection tolls,
f) Critical information infrastructure and important information systems, their users and administrators activities recording tools,
g) Cyber security events detection tools,
h) Collection and evaluation of cyber security events tools,
i) Application security,
j) Cryptographic devices,
k) Tools for ensuring the levels of information availability and
l) Industrial and management systems security.

Conclusion

Providing of adequate security requires accepting of necessary measures. However, such measures increase costs both in state and private spheres. That is why that many systems considered as 'Essential services', 'Important information system' or 'Critical information infrastructure' are operated by private subjects.

References

1. „DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC," Official Journal of the European Union, 2015. [Online]. Available: http://eur-lex.europa.eu/.
2. „DIRECTIVE (EU) 2015/849 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012," Official Journal of the European Union, 2015. [Online]. Available: http://eur-lex.europa.eu.
3. „REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC," 23 July 2014, THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION.
4. „DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures for a high common level of security of network and information systems across the Union," Official Journal of the European Union, 2016. [Online]. Available: http://eur-lex.europa.eu.