Unofficial translation

Issuer: Minister of Entrepreneurship and Information Technology
Type: regulation
Type of text: original text - single text
In force from: 13.07.2018
Publication citation: RT I, 10.07.2018, 6

Requirements for risk analysis of network and information systems and description of security measures

Passed 05.07.2018 No. 40

The regulation is established under § 7 (4) of the Cybersecurity Act

§ 1. Scope of application

This regulation establishes the requirements for the preparation of a risk assessment of the network and information systems (hereinafter *systems*) used for the provision of services set out in subsection 3 (1) of the Cybersecurity Act and a description of the organisational, IT, and physical security measures (hereinafter *security measures*).

§ 2. Definitions

(1) For the purposes of the regulation, the risk assessment of systems means a description of the risks compromising the security of the systems and the continuity of the services, as well as the measures implemented to manage them.

(2) For the purposes of the regulation, resources are means used for system maintenance and tools affecting their operation, including premises, the ventilation, cooling, and heating equipment of the rooms, equipment supplying the premises and systems with electricity, the software used to run the systems, and the staff of the service provider.

(3) For the purposes of the regulation, a critical activity is an activity which is carried out by the service provider, which depends on at least one system and which is essential for the provision of the service, and in the absence of which the service may be interrupted.

(4) For the purposes of the regulation, a weakness means a lack of security of the systems or the resources related to the systems which makes the systems or the resources related to the systems vulnerable to threat.

(5) For the purposes of this regulation, a threat means an event or circumstance which may exploit the weakness of the systems or the resources related to them.

(6) For the purposes of this regulation, risk means an estimated definition determined as the combination of the likelihood of the threat exploiting the weakness and the possible effects of a cyber incident.

§ 3. Requirements for the risk assessment of systems

(1) The service provider shall provide at least the following information in the risk assessment of the systems:

1) a brief description of the methodology used in the risk analysis of the systems and references to additional documentation related to the risk analysis;

2) a list of critical activities necessary for the provision of the service, together with the systems necessary for their operation;

3) a list of resources related to the systems;

4) a list of threats;

5) a list of weaknesses;

6) an assessment of the likelihood of the realisation of threats, considering the identified weaknesses and the measures implemented;

7) an assessment of the consequences of a possible cyber incident and the severity of the consequences, considering the criteria for determining the severity of the consequences: the approximate number of persons affected by the cyber incident, the duration of service interruptions, the extent of the area affected by the cyber incident, possible damage type and rate, and the complexity of restoration of system security or service continuity;

8) a list of risks with the criticality of each risk;

9) a description of hedging measures.

(2) The service provider shall ensure the continuous monitoring of the risks and the updating of the risk assessment of the systems in the event of any new risk that the service provider considers significant.

(3) The service provider may compile a risk analysis of the systems as part of a document to be prepared on the basis of another legal act.

§ 4. Description of security measures to ensure the security of systems

(1) The service provider shall cover with the security measures the following:

1) procedures, resources, activities, and the procedure for responding to cyber incidents approved by the management body of the service provider;

2) tasks and responsibilities of the staff approved by the management body of the service provider.

(2) The security measures shall provide for at least:

1) the management of system access rights and the identification and authorisation of system users;

2) regular back-ups of the data necessary for the provision of the service and the procedures for restoring the data from the back-ups;

3) the timeliness of the software operating the systems and the software operated in the systems;

4) the keeping of system log files with the executor of the activity, the type of activity, and the time of execution of the activity;

5) the software and hardware solutions to detect and control the activities and software threatening the security of the systems;

6) the procedures for restoring system security or service continuity.

(3) The service provider shall implement, monitor, and update security measures to ensure the management of risks listed in the risk analysis of systems compiled under section 3.

§ 5. Implementation of regulation

The service provider shall compile a risk analysis of the systems on the basis of section 3 by 31 December 2018 at the latest.