COMMISSION IMPLEMENTING REGULATION (EU) 2018/151

of 30 January 2018

laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [1], and in particular Article 16(8) thereof,

Whereas:

(1) In accordance with Directive (EU) 2016/1148, digital service providers remain free to take technical and organisational measures they consider appropriate and proportionate to manage the risk posed to the security of their network and information systems, as long as those measures ensure an appropriate level of security and take into account the elements provided for in that Directive.

(2) When identifying the appropriate and proportionate technical and organisational measures, the digital service provider should approach information security in a systematic way, using a risk-based approach.

(3) In order to ensure the security of systems and facilities, digital service providers should perform assessment and analysis procedures. These activities should concern the systematic management of network and information systems, the physical and environmental security, the security of supplies and the access controls.

(4) When carrying out a risk analysis within the systematic management of network and information systems, digital service providers should be encouraged to identify specific risks and quantify their significance, for example by identifying threats to critical assets and how they may affect the operations, and determining how best to mitigate those threats based on current capabilities and resource requirements.

(5) Policies on human resources could refer to the management of skills, including aspects related to the development of security related skills and awareness-raising. When deciding on an appropriate set of policies on security of operation, the digital service providers should be encouraged to take into account aspects of change management, vulnerability management, formalisation of operating and administrative practices and system mapping.

(6) Policies on security architecture could comprise in particular the segregation of networks and systems as well as specific security measures for critical operations such as administration operations. The segregation of networks and systems could enable a digital service provider to distinguish between elements such as data flows and computing resources that belong to a client, group of clients, the digital service provider or third parties.

(7) The measures taken with regard to the physical and environmental security should ensure the security of an organisation's network and information systems from damage caused by incidents such as theft, fire, flood or other weather effects, telecommunications or power failures.

(8) The security of supplies such as electrical power, fuel or cooling could encompass the security of the supply chain that includes in particular the security of third party contractors and subcontractors and their management. The traceability of critical supplies refers to the ability of the digital service provider to identify and record sources of those supplies.

(9) The users of digital services should encompass natural and legal persons who are customers of or are subscribers to an online marketplace or a cloud computing service, or who are visitors to an online search engine website in order to undertake keyword searches.

[1] OJ L 194, 19.7.2016, p. 1.

(10) When defining the substantiality of the impact of an incident, the cases laid down in this regulation should be considered as a non-exhaustive list of substantial incidents. Lessons should be drawn from the implementation of this Regulation and from the work of the Cooperation Group as regards the collection of best practice information on risks and incidents and the discussions on modalities for reporting notifications of incidents as referred to in points (i) and (m) of Article 11(3) of Directive (EU) 2016/1148. The result could be comprehensive guidelines on quantitative thresholds of notification parameters that may trigger the notification obligation for digital service providers under Article 16(3) of Directive (EU) 2016/1148. Where appropriate, the Commission could also consider reviewing the thresholds currently laid down in this Regulation.

(11) In order to enable competent authorities to be informed about potential new risks, the digital service providers should be encouraged to voluntarily report any incident whose characteristics have been previously unknown to them such as new exploits, attack-vectors or threat actor, vulnerabilities and hazards.

(12) This Regulation should apply on the day following the expiry of the deadline for transposition of Directive (EU) 2016/1148.

(13) The measures provided for in this Regulation are in accordance with the opinion of the Network and Information Systems Security Committee referred to Article 22 of Directive (EU) 2016/1148,

HAS ADOPTED THIS REGULATION:

Article 1

Subject matter

This Regulation specifies further the elements to be taken into account by digital service providers when identifying and taking measures to ensure a level of security of network and information systems which they use in the context of offering services referred to in Annex III to Directive (EU) 2016/1148 and specifies further the parameters to be taken into account to determine whether an incident has a substantial impact on the provision of those services.

Article 2

Security elements

1. Security of systems and facilities referred to in point (a) of Article 16(1) of Directive (EU) 2016/1148 means the security of network and information systems and of their physical environment and shall include the following elements:

(a) the systematic management of network and information systems, which means a mapping of information systems and the establishment of a set of appropriate policies on managing information security, including risk analysis, human resources, security of operations, security architecture, secure data and system life cycle management and where applicable, encryption and its management;

(b) physical and environmental security, which means the availability of a set of measures to protect the security of digital service providers' network and information systems from damage using an all-hazards risk-based approach, addressing for instance system failure, human error, malicious action or natural phenomena;

(c) the security of supplies, which means the establishment and maintenance of appropriate policies in order to ensure the accessibility and where applicable the traceability of critical supplies used in the provision of the services;

(d) the access controls to network and information systems, which means the availability of a set of measures to ensure that the physical and logical access to network and information systems, including administrative security of network and information systems, is authorised and restricted based on business and security requirements.

2. With regard to incident handling referred to in point (b) of Article 16(1) of Directive (EU) 2016/1148, the measures taken by the digital service provider shall include:

(a) detection processes and procedures maintained and tested to ensure timely and adequate awareness of anomalous events;

(b) processes and policies on reporting incidents and identifying weaknesses and vulnerabilities in their information systems;

(c) a response in accordance with established procedures and reporting the results of the measure taken;

(d) an assessment of the incident's severity, documenting knowledge from incident analysis and collection of relevant information which may serve as evidence and support a continuous improvement process.

3. Business continuity management referred to in point (c) of Article 16(1) of Directive (EU) 2016/1148 means the capability of an organisation to maintain or as appropriate restore the delivery of services at acceptable predefined levels following a disruptive incident and shall include:

(a) the establishment and the use of contingency plans based on a business impact analysis for ensuring the continuity of the services provided by digital service providers which shall be assessed and tested on a regular basis for example, through exercises;

(b) disaster recovery capabilities which shall be assessed and tested on a regular basis for example, through exercises.

4. The monitoring, auditing and testing referred to in point (d) of Article 16(1) of Directive (EU) 2016/1148 shall include the establishment and maintenance of policies on:

(a) the conducting of a planned sequence of observations or measurements to assess whether network and information systems are operating as intended;

(b) inspection and verification to check whether a standard or set of guidelines is being followed, records are accurate, and efficiency and effectiveness targets are being met;

(c) a process intended to reveal flaws in the security mechanisms of a network and information system that protect data and maintain functionality as intended. Such process shall include technical processes and personnel involved in the operation flow.

5. International standards referred to in point (e) of Article 16(1) of Directive (EU) 2016/1148 mean standards that are adopted by an international standardisation body as referred to in point (a) of Article 2(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council [1]. Pursuant to Article 19 of Directive (EU) 2016/1148, European or internationally accepted standards and specifications relevant to the security of network and information systems, including existing national standards, may also be used.

6. Digital service providers shall ensure that they have adequate documentation available to enable the competent authority to verify compliance with the security elements set out in paragraphs 1, 2, 3, 4 and 5.

Article 3

Parameters to be taken into account to determine whether the impact of an incident is substantial

1. With regard to the number of users affected by an incident, in particular users relying on the service for the provision of their own services referred to in point (a) of Article 16(4) of Directive (EU) 2016/1148, the digital service provider shall be in a position to estimate either of the following:

(a) the number of affected natural and legal persons with whom a contract for the provision of the service has been concluded; or

(b) the number of affected users having used the service based in particular on previous traffic data.

2. The duration of an incident referred to in point (b) of Article 16(4) means the time period from the disruption of the proper provision of the service in terms of availability, authenticity, integrity or confidentiality until the time of recovery.

3. As far as the geographical spread with regard to the area affected by the incident referred to in point (c) of Article 16(4) of Directive (EU) 2016/1148 is concerned, the digital service provider shall be in a position to identify whether the incident affects the provision of its services in specific Member States.

4. The extent of disruption of the functioning of the service referred to in point (d) of Article 16(4) of Directive (EU) 2016/1148 shall be measured as regards one or more of the following characteristics impaired by an incident: the availability, authenticity, integrity or confidentiality of data or related services.

---

[1] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p. 12).

5. With regard to the extent of the impact on economic and societal activities referred to in point (e) of Article 16(4) of Directive (EU) 2016/1148, the digital service provider shall be able to conclude, based on indications such as the nature of his contractual relations with the customer or, where appropriate, the potential number of affected users, whether the incident has caused significant material or non-material losses for the users such as in relation to health, safety or damage to property.

6. For the purpose of paragraph 1, 2, 3, 4 and 5, the digital service providers shall not be required to collect additional information to which they do not have access.

Article 4

Substantial impact of an incident

1. An incident shall be considered as having a substantial impact where at least one of the following situations has taken place:

(a) the service provided by a digital service provider was unavailable for more than 5 000 000 user-hours whereby the term user-hour refers to the number of affected users in the Union for a duration of 60 minutes;

(b) the incident has resulted in a loss of integrity, authenticity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via a network and information system of the digital service provider affecting more than 100 000 users in the Union;

(c) the incident has created a risk to public safety, public security or of loss of life;

(d) the incident has caused material damage to at least one user in the Union where the damage caused to that user exceeds EUR 1 000 000.

2. Drawing on the best practice collected by the Cooperation Group in the exercise of its tasks under Article 11(3) of Directive (EU) 2016/1148 and on the discussions under point (m) of Article 11(3) thereof, the Commission may review the thresholds laid down in paragraph 1.

Article 5

Entry into force

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

2. It shall apply from 10 May 2018.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 30 January 2018.

For the Commission

The President

Jean-Claude JUNCKER