ASPECTS REGARDING THE MEASURES AVAILABLE FOR A HIGH LEVEL OF SECURITY OF INFORMATION NETWORKS IN THE EUROPEAN UNION

Isabela, Stancea[1]

Abstract

Networks, together with computer systems and services, have a vital role to play in society. Their reliability and security are essential for economic and social activities and, in particular, for the functioning of the internal market.

The extent, frequency and impact of security incidents are increasing and are a serious threat to the functioning of networks and information systems. Those systems may also become a target for deliberate harmful actions aimed at affecting or interrupting the operation of systems. Such incidents can hamper the conduct of economic activities, generate substantial financial losses, undermine users' confidence and cause major damage to the Union's economy.

Networks and information systems and, in particular, the Internet play an essential role in facilitating the cross-border circulation of products, services and people. Due to their transnational nature, a major disruption of these systems, whether intentional or unintentional, and wherever they happen, can affect each individual Member State and the Union as a whole. Therefore, the security of networks and information systems is essential for the smooth functioning of the internal market.

Key words: *computer systems, computer networks, users.*

Networks, together with computer systems and services, have a vital role to play in society. Their reliability and security are essential for economic and social activities and, in particular, for the functioning of the internal market.

The extent, frequency and impact of security incidents are increasing and are a serious threat to the functioning of networks and information systems. Those systems may also become a target for deliberate harmful actions aimed at affecting or interrupting the operation of systems. Such incidents may hamper the conduct of economic activities, generate substantial financial losses, undermine the confidence of users and cause major damage to the Union's economy[2].

Networks and information systems and, in particular, the Internet play an essential role in facilitating the cross-border circulation of products, services and people. Because of their transnational nature, a major disruption of these systems, whether intentional or unintentional, and wherever they happen, can affect each individual Member State and the Union as a whole. Therefore, the security of networks and information systems is essential for the smooth functioning of the internal market.

Existing capacities are not sufficient to ensure a high level of security of the networks and information systems in the Union. Member States have very different training levels, which has led to a fragmented approach in the Union. This leads to uneven levels of consumer and business protection and undermines the overall level of security of the networks and information systems in the Union. In turn, the absence of common requirements for essential service providers and digital service providers make it impossible to set up a general and effective Union-wide cooperation mechanism. Universities and research centers play a decisive role in fostering research, development and innovation in these areas.

Therefore, in order to respond effectively to the challenges in the area of network and information security, a global approach at EU level is required, which includes common requirements for minimum capacity building and planning, information sharing, cooperation and common security requirements for essential service providers and digital service

[1] Lecturer PhD, "Constantin Brâncoveanu" University of Pitesti

[2] Directive (Eu) 2016/1148 Of The European Parliament And Of The Council of 6 July 2016 on measures for a high common level of network and information security in the Union.

providers. However, essential service providers and digital service providers shall not be prevented from implementing security measures which are stricter than those provided for under this Directive.

The processing of personal data shall be carried out in accordance with Directive 95/46 / EC.

By 9 November 2018, for each sector and subsector, Member States shall identify key service providers with headquarters in their territory.

The criteria for identifying the key service providers mentioned are as follows:

(a) an entity provides an essential service to support the most important societal and / or economic activities;

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

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

Member States shall periodically and at least every two years from 9 May 2018 review and, where appropriate, update the list of identified essential service providers.

By 9 November 2018 and every two years thereafter, Member States shall provide the Commission with the information necessary to enable it to assess the implementation of this Directive, in particular the consistency of Member States' approaches to the identification of key service providers. This information shall include at least the following:

(a) national measures to identify key service providers;

(b) the list of services mentioned;

(c) the number of key service providers identified for each sector listed in Annex II and an indication of their importance in relation to that sector;

(d) limits, where available, for determining the relevant level of supply in relation to the number of users relying on that service.

Each Member State shall adopt a national strategy for network and information security which defines the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of network and information security and covering at least those sectors in Annex II and the services listed in Annex III. The national strategy on network and information security concerns, in particular, the following:

(a) the objectives and priorities of the national strategy on network and information security;

(b) a governance framework for achieving the objectives and priorities of the national strategy on network and information security, including the roles and responsibilities of government bodies and other relevant actors;

(c) identification of measures on preparedness, response and recovery, including public-private cooperation;

(d) indication of training, awareness and training programs related to the national strategy on network and information security;

(e) indication of research and development plans related to the national strategy on network and information security;

(f) a risk assessment plan for the identification of risks;

(g) a list of the different actors involved in the implementation of the national strategy on network and information security.

Member States shall communicate their national network and information security strategies to the Commission within three months of their adoption. From this communication, Member States can exclude elements of the strategy related to national security.

Each Member State shall designate one or more national competent authorities responsible for network and information security covering at least the sectors and services envisaged. Member States may assign this role to an existing authority or authority.

Each Member State designates a single national contact point for network and information security ("single point of contact"). Member States can assign this role to an

existing authority. Where a Member State designates a single competent authority, it also serves as a single point of contact.

Member States shall ensure that the competent authorities and points of single contact have adequate resources to carry out their tasks effectively and effectively and thus achieve the objectives of this Directive. Member States shall ensure the effective, efficient and secure cooperation of the designated representatives in the cooperation group.

The competent authorities and the point of single contact shall consult and cooperate, as appropriate and in accordance with national law, with national law enforcement authorities and relevant national data protection authorities.

Each Member State shall without delay notify the Commission of the designation of the competent authority and of the single point of contact, their tasks and any subsequent amendments thereto. Each Member State shall make public the designation of the competent authority and of the single point of contact. The Commission shall publish the list of designated points of contact designated.

Each Member State shall designate one or more CSIRT (cyber security intervention teams) that comply with the requirements laid down by European legislation responsible for risk and incident management in accordance with a well-defined procedure. A CSIRT team may be set up within a competent authority.

A cooperation group is set up to support and facilitate strategic cooperation and exchange of information between Member States in order to strengthen confidence and achieve a high common level of network and information security in the Union.

The Cooperation Group has the following tasks:

(a) provide strategic guidance for the activities of the CSIRT network;

(b) participate in the exchange of best practice on the exchange of information on incident notification;

(c) participate in the exchange of best practices between Member States and, in cooperation with ENISA, assist Member States in enhancing their capacity in network and information security;

(d) discuss Member States' capacities and preparedness and, on a voluntary basis, assess national strategies on network and information security and the effectiveness of the CSIRT teams and identify best practices;

(e) participate in the exchange of information and good practice on awareness-raising and training;

(f) participate in the exchange of information and best practices on research and development related to network and information security;

(g) where appropriate, participate in the exchange of experience on network and information security issues with relevant Union institutions, bodies, offices and agencies;

(h) discuss standards and specifications with representatives of relevant European standardization organizations;

(i) collect information on best practice on risks and incidents;

(j) examine the summary reports on an annual basis;

(k) discussing work on network and information security exercises, education and training programs, including ENISA;

(l) assisted by ENISA, shall participate in the exchange of good practices on the identification of key service providers by Member States, including on cross-border risk and security incidents.

By 9 February 2018 and every two years thereafter, the Cooperation Group shall establish a work program on the actions to be taken to implement its objectives and tasks, which are in line with the objectives of the Directive.

To help build confidence between Member States and to promote rapid and effective operational cooperation, a network of national CSIRT teams is set up.

The CSIRT network is composed of representatives of the CSIRT teams of the Member States and of the CERT-EU. The Commission participates in the CSIRT network as an observer. ENISA provides the secretariat and actively supports cooperation between CSIRT teams.

The CSIRT network has the following tasks:

(a) participate in the exchange of information on the services, operations and cooperation capacities of the CSIRT teams;

(b) at the request of a representative of a CSIRT team of a Member State potentially affected by an incident, exchange and discuss non-commercial sensitive information relating to the incident and the associated risks; however, any CSIRT team of a Member State may refuse to contribute to that discussion if there is a risk of prejudice to the investigation of the incident;

(c) participate in the exchange of information and make available on a voluntary basis non-confidential information on individual incidents;

(d) at the request of the representative of a CSIRT team in a Member State, discuss and, where appropriate, identify a coordinated response to an incident that has been identified in the jurisdiction of that Member State;

(e) give Member States support in addressing cross-border incidents on the basis of their voluntary mutual assistance;

(f) discuss, explore and identify new forms of operational cooperation, including in relation to: risk and incident categories, early alerts, mutual assistance, coordination principles and modalities, when Member States respond to cross-border risks and incidents;

(g) inform the cooperative group of its activities and of the new forms of operational cooperation discussed in accordance with point (f) and seek guidance on them;

(h) discuss the lessons learned from exercises concerning the security of computer networks and systems, including those organized by ENISA;

(i) at the request of a specific CSIRT team, discuss the capabilities and level of training of the same CSIRT team;

(j) issue guidelines to facilitate the convergence of operational practices in the application of the provisions of this Article on operational cooperation.

The CSIRT network shall, by 9 August 2018 and every 18 months thereafter, produce an evaluation report on the experience gained through operational cooperation under this Article, including conclusions and recommendations. The report shall also be forwarded to the cooperation group.

Member States shall ensure that digital service providers identify and take appropriate and proportionate technical and organizational measures to manage network and information security risks that they use across the Union. In the light of the most advanced knowledge in the field, those measures shall ensure a level of network and information security appropriate to the risk involved and shall take account of the following elements:

(a) the security of systems and installations;

b) incident management;

c) management of the continuity of the activity;

d) monitoring, auditing and testing;

e) compliance with international standards. Member States shall ensure that digital service providers notify without undue delay to the competent authority or the CSIRT team of any incident having a substantial impact on the provision of a service as referred to in Annex III which it offers within the Union. Notifications include information to enable the competent authority or the CSIRT team to determine the importance of any cross-border impact.

The notification does not expose the notifying party to increased liability. To determine if the impact of an incident is important, the following parameters are especially taken into account:

(a) the number of users affected by the incident, in particular users who rely on the service to provide their own services;

b) the duration of the incident;

c) geographical distribution of the area affected by the incident;

d) the extent of disturbance of the operation of the service;

e) the extent of impact on economic and societal activities.

Where a digital service provider has its principal place of business or a representative in a Member State but its computer networks and systems are located in one or more other Member States, the competent authority of the Member State where the head office or the representative is located and the competent authorities of those other Member States shall cooperate and provide mutual assistance as appropriate. Such assistance and cooperation may include exchanges of information between the competent authorities concerned and requests for surveillance measures.