European Cyberlaw handout – ISP Cyberssecurity

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

Article 4 Definitions

For the purposes of this Directive, the following definitions apply:

(1) 'network and information system' means:

(a)an electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC;

(b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or

(c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;

(2) 'security of network and information systems' means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems;

(3) 'national strategy on the security of network and information systems' means a framework providing strategic objectives and priorities on the security of network and information systems at national level;

(4) 'operator of essential services' means a public or private entity of a type referred to in Annex II, which meets the criteria laid down in Article 5(2);

(5) 'digital service' means a service within the meaning of point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council (17) which is of a type listed in Annex III;

(6) 'digital service provider' means any legal person that provides a digital service;

(7) 'incident' means any event having an actual adverse effect on the security of network and information systems;

(8) 'incident handling' means all procedures supporting the detection, analysis and containment of an incident and the response thereto;

(9) 'risk' means any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems;

(10) 'representative' means any natural or legal person established in the Union explicitly designated to act on behalf of a digital service provider not established in the Union, which may be addressed by a national competent authority or a CSIRT instead of the digital service provider with regard to the obligations of that digital service provider under this Directive;

(11) 'standard' means a standard within the meaning of point (1) of Article 2 of Regulation (EU) No 1025/2012;

(12) 'specification' means a technical specification within the meaning of point (4) of Article 2 of Regulation (EU) No 1025/2012;

(13) 'internet exchange point (IXP)' means a network facility which enables the interconnection of more than two independent autonomous systems, primarily for the purpose of facilitating the exchange of internet traffic; an IXP provides interconnection only for autonomous systems; an IXP does not require the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic;

(14) 'domain name system (DNS)' means a hierarchical distributed naming system in a network which refers queries for domain names;

(15) 'DNS service provider' means an entity which provides DNS services on the internet;

(16) 'top-level domain name registry' means an entity which administers and operates the registration of internet domain names under a specific top-level domain (TLD);

(17) 'online marketplace' means a digital service that allows consumers and/or traders as respectively defined in point (a) and in point (b) of Article 4(1) of Directive 2013/11/EU of the European Parliament and of the Council (18) to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace;

(18) 'online search engine' means a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the

basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found;

(19) 'cloud computing service' means a digital service that enables access to a scalable and elastic pool of shareable computing resources.

Article 9

Computer security incident response teams (CSIRTs)

1. Each Member State shall designate one or more CSIRTs which shall comply with the requirements set out in point (1) of Annex I, covering at least the sectors referred to in Annex II and the services referred to in Annex III, responsible for risk and incident handling in accordance with a well-defined process. A CSIRT may be established within a competent authority.
2. Member States shall ensure that the CSIRTs have adequate resources to effectively carry out their tasks as set out in point (2) of Annex I.

Member States shall ensure the effective, efficient and secure cooperation of their CSIRTs in the CSIRTs network referred to in Article 12.
3. Member States shall ensure that their CSIRTs have access to an appropriate, secure, and resilient communication and information infrastructure at national level.
4. Member States shall inform the Commission about the remit, as well as the main elements of the incident-handling process, of their CSIRTs.
5. Member States may request the assistance of ENISA in developing national CSIRTs.

Article 12 CSIRTs Network

1. 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.
2. 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. ENISA shall provide the secretariat and shall actively support the cooperation among the CSIRTs.
3. The CSIRTs network shall have the following tasks:
(a) exchanging information on CSIRTs' services, operations and cooperation capabilities;
(b) at the request of a representative of a CSIRT from a Member State potentially affected by an incident, exchanging and discussing non-commercially sensitive information related to that incident and associated risks; however, any Member State's CSIRT may refuse to contribute to that discussion if there is a risk of prejudice to the investigation of the incident;
(c) exchanging and making available on a voluntary basis non-confidential information concerning individual incidents;
(d) at the request of a representative of a Member State's CSIRT, discussing and, where possible, identifying a coordinated response to an incident that has been identified within the jurisdiction of that same Member State;
(e) providing Member States with support in addressing cross-border incidents on the basis of their voluntary mutual assistance;
(f) discussing, exploring and identifying further forms of operational cooperation, including in relation to:
(i) categories of risks and incidents;
(ii) early warnings;
(iii) mutual assistance;
(iv) principles and modalities for coordination, when Member States respond to cross-border risks and incidents;
(g) informing the Cooperation Group of its activities and of the further forms of operational cooperation discussed pursuant to point (f), and requesting guidance in that regard;
(h) discussing lessons learnt from exercises relating to the security of network and information systems, including from those organised by ENISA;
(i) at the request of an individual CSIRT, discussing the capabilities and preparedness of that CSIRT;
(j) issuing guidelines in order to facilitate the convergence of operational practices with regard to the application of the provisions of this Article concerning operational cooperation.
4. For the purpose of the review referred to in Article 23 and by 9 August 2018, and every year and a half thereafter, the CSIRTs network shall produce a report assessing the experience gained with the operational cooperation, including conclusions and recommendations, pursued under this Article. That report shall also be submitted to the Cooperation Group.
5. The CSIRTs network shall lay down its own rules of procedure.