Government Decree 271/2018 (XII.20.)

on the functions and powers of incident response centres, and the rules for security incident response and technical investigation, and for conducting vulnerability testing

The Government,

acting on the basis of authorization by Section 24 (1) *e)*, *j)* and *k)* of the Act L of 2013 on the electronic information security of state and municipal bodies and

by Section 17 (1a) *b)* and *c)* of Act CVIII of 2001 on certain aspects of electronic commerce services and information society services,

acting within its function laid down in Article 15 (1) of the Fundamental Law,

orders as follows:

1. Interpretative provisions

Section 1 For the purpose of this Decree:

1. '*IT security investigation with administration privileges'* means a security investigation procedure in the course of which the investigating person has the administrator's right and the purpose of this procedure is to check the condition of the entire IT system of the body concerned on the basis of compliance lists;

2. '*operator of essential services'* means the service provider identified as an operator of essential services under the Act CLXVI of 2012 on the identification, designation and protection of critical systems and facilities (hereinafter referred to as 'Hungarian CIP Act');

3. '*automated investigation'* means the security investigation procedure in the course of which the vulnerabilities of the IT system of the body concerned are mapped by means of a target software;

4. *'digital service provider'* means the service provider providing the service under Section 2 *j)* of the Act CVIII of 2001 on certain aspects of electronic commerce services and information society services (hereinafter referred to as 'Hungarian Electronic Commerce Act');

5. *'internal IT security investigation'* means a security investigation procedure in the course of which the vulnerability testing of the IT system of the body concerned is carried out directly from the internal network termination point;

6. *'security incident response agent'* means a person with a mandate for security incident investigation, issued by the head of the body concerned under Section 11 (6) of the Act L of 2013 on the electronic information security of state and municipal bodies (hereinafter referred to as 'Hungarian Cyber Security Act');

7. *'target software'* means a software developed for the implementation of the certain phases of vulnerability testing in the course of the security investigation procedure;

8. '*CSIRTs network'* is a network of bodies responding to national computer security incidents established by the 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;

9. *'body concerned'* means the body concerned by security investigation or vulnerability testing which operates an electronic information system;

9a.[1] *'user documentation'* means a document containing a brief summary description of the IT system or service to be investigated and the detailed description of its functions;

9b.[2] *'user permissions matrix'* means a document describing the permissions of the users of an IT system or service to be investigated, the levels applied for permissions and the conditions under which they are interoperable;

9c.[3] '*function testing plan'* means a document which sets out a detailed testing process for each function of an IT system or service to be investigated or the results of a test carried out;

10. *'manual IT security investigation'* means a security investigation procedure in the course of which the vulnerabilities of the IT system of the body concerned are identified by using individually and manually established queries carried out by the investigator;

11. *'intermediary service provider'* means the service provider under Section 2 *l)* of the Hungarian Electronic Commerce Act;

12. *'external IT security investigation'* is an external vulnerability testing of the IT system from the side of the Internet, in the course of which free search, targeted information collection in public databases available on the Internet and the identification of the services, vulnerabilities of available computers are mapped;

13. *'IT security investigation without registered user permission'* is a security investigation procedure in the course of which the investigator does not have any prior information on the IT system of the body concerned and has no user permission to the system;

14. *'IT security investigation with registered user permission'* is a security investigation procedure in the course of which the investigator carries out the investigation with to a specific user permission created for the investigator;

15. '*psychological manipulation'* is the overall types of activity, techniques and methods which enable the acquisition of confidential information or the spread and operation of a malware based on influencing people;

15a.[4] *'system plan'* means the up-to-date document which contains the description of the system, the development, implementation and operational documentation, as well as the plans to introduce and install the system or service concerned;

16. *'encryption procedure'* is a procedure which restricts the availability of the data by converting the data into a series of signs by means of an algorithm that are illegible to the person who does not have the key with unique sequence of signs required for reconstitution;

17. *'encryption key'* means a sequence of signs applied during the encryption procedure with the knowledge of which the classified file can become available;

18. '*web investigation'* is a security investigation procedure in the course of which the vulnerabilities of web applications are discovered by automated and manual investigations;

19. *'wireless network IT security investigation'* is a security investigation procedure in the course of which the search, identification of wireless access points and the connections, the assessment of encryption procedures, the verification of decryption of encryption keys is carried out by means of target software programs and manual investigation.

---

[1] Added by Section 105 (1) of Government Decree 375/2020 (VII.30.) Effective from 31.07.2020
[2] Added by Section 105 (1) of Government Decree 375/2020 (VII.30.) Effective from 31.07.2020
[3] Added by Section 105 (1) of Government Decree 375/2020 (VII.30.) Effective from 31.07.2020
[4] Added by Section 105 (1) of Government Decree 375/2020 (VII.30.) Effective from 31.07.2020

2. Functions and powers of the Centre

Section 2 The Government designates the Special Service for National Security as the incident response centre under Section 19 (1) of the Hungarian Cyber Security Act and Section 6/B (1) of the Hungarian Electronic Commerce Act (hereinafter referred to as 'Centre').

Section 3 (1) The Centre shall respond the security incidents and threats of

a)[1] the open electronic information systems of the bodies determined in Section 2 of the Hungarian Cyber Security Act, with the exception under Section 19 (2) of the Hungarian Cyber Security Act,

b) the electronic information systems of digital service providers,

c) the electronic information systems of the operators of critical infrastructures designated as European or national critical infrastructures, with the exception of critical infrastructures for national defence,

d) the electronic information systems of centralised IT and electronic communication service providers.

(2) The Centre shall cooperate

a) with the authorities designated for supervision of electronic information systems,

b)[2] with the incident response centre under Section 19 (2) of the Hungarian Cyber Security Act (hereinafter referred to as 'incident response centre'),

c) with law enforcement agencies,

d) with the National Media and Communications Authority and the National Directorate-General for Informatics and Communications operated by it,

e) with the electronic communication service providers, the centralized IT and electronic communication service provider,

f) with the operators, designating and advisory authorities under the Hungarian CIP Act, and

g) with the Hungarian National Authority for Data Protection and Freedom of Information

to respond the security incidents and threats.

(3) The Centre shall take part in the activities of CSIRTs network regarding the electronic information systems falling within its competence.

(4) The Centre shall investigate the activities indicating security incidents or threats, and, if necessary, it shall issue warnings towards the users, the incident response centres, the authorities, the authorities supervising the electronic information systems and the single point of contact under the Government Decree 187/2015 (VII.13.) on functions and powers of the information security supervisor and the determination of closed electronic information system (hereinafter referred to as 'single point of contact'), as well as the bodies under paragraph (1).

(5) The Centre shall inform the single point of contact about its non-statutory rules of procedure for security incident response.

(6) The Centre shall perform the following tasks:

a) monitoring of security incidents at national level;

b) information related to risks and security incidents, early warning, alert, notification and information dissemination to the persons concerned;

---

[1] Amended by Section 114 a) of the Government Decree 375/2020 (VII.30.)

[2] Amended by Section 114 b) of the Government Decree 375/2020 (VII.30.)

c) reaction to the security incidents;

d) preparing dynamic risk and incident assessments, as well as situational pictures regarding security incidents;

e) conducting vulnerability testing.

(7) The Centre shall determine the procedures for security incident response and risk management, as well as the procedures and rules for classification of security incidents, risks and information. In the course of that, the Centre shall cooperate with the bodies determined in paragraph (1).

Section 4 Within the competence of security incident response, the Centre is responsible for

a) the immediate information of the persons concerned about the security incident, which it has become aware of,

b) keeping a record about security incidents which shall contain the measures taken related to the security incidents and their results, as well as

c) the operation of early warning system according to a separate government decree.

Section 5 (1) For the prevention of security incidents, the Centre shall perform the information and awareness-raising tasks regarding the threats to electronic information systems of the bodies under Section 3 (1) according to paragraphs (2) to (4).

(2) In the context of vulnerabilities and threatening risks to electronic information systems, the Centre is responsible for

a) notifying the information security officers,

b) notifying the authorities and incident response centres, as well as

c) the regular information on its website about vulnerabilities and threats, as well as the proposed security measures.

(3) The Centre shall

a) prepare analyses and reports about Hungarian and international information security tendencies,

b) prepare a report about the security incidents falling within its competence to the National Cyber Security Coordination Council on a quarterly basis and

c) annually prepare a report about its activity to the minister responsible for civilian national security services.

(4) The Centre

a) may issue non-binding resolutions, recommendations,

b) may hold sessions on security incident response, may take part in the awareness-raising program of the institutions responsible for raising awareness of information security, may perform expert- and education activities,

c) may operate a cooperation forum for government information technology and security incident response and

d) shall take part in preparation in the strategies and regulations on ICT security.

3. Functions and powers of the incident response centres

Section 6 (1) Based on Section 19 (2) of the Hungarian Cyber Security Act, the Government designates the Military National Security Service for security incident response and risk management of the electronic information systems for national defence purposes. The Military National Security Service shall carry out the security incident response and risk management together with the incident response centres under its professional management and coordination, separated under specific tasks, which function at an organization or a body under the management or governance of the minister responsible for national defence.

(2)[1]

(3)[2] As regards the electronic information systems falling within its competence, the incident response centre shall

a) perform the tasks of the Centre under Section 4 within its competence of security incident response,

b) perform the tasks of the Centre under Sections 5 (2) *b)* and 5 (3) *c)* within its competence of notification,

c) perform the tasks of the Centre under Section 5 (4) *a)* to *c)* within its competence of awareness-raising activity.

(4)[3] The incident response centre shall send the report under Section 5 (3) *c)* to the minister responsible for national defence.

Section 7[4] (1) As regards the electronic information systems falling within its competence, the incident response centre shall

a) keep a record about contact details for liaising with bodies falling within its competence and

b) immediately inform the Centre about the security incidents detected or learnt.

(2) The incident response centre shall inform the Centre about the start of its operation at least 5 days before the planned start, and shall announce the data necessary to contact and the change in contact data to the Centre immediately.

(3) Sections 3 (7), 14 to 18, 20 to 21 and 23 to 29 shall be applied to the procedure of the incident response centre.

4. Notification of security incidents

Section 8 (1) The bodies under Section 19 (1) *b)* to *c)* of the Hungarian Cyber Security Act and the intermediary service providers shall immediately notify the security incidents occurred in their electronic information systems to the Centre.

(2) The body concerned shall notify the security incidents and threats to the electronic information systems for national defence purposes to the incident response centre designated in Section 6 (1) according to the internal provisions of the minister responsible for national defence.

---

[1] Repealed by Section 114 second b) of Government Decree 375/2020 (VII.30.) Ineffective from 31.07.2020
[2] Declared by Section 106 (1) of Government Decree 375/2020 (VII.30.) Effective from 31.07.2020
[3] Added by Section 106 (2) of Government Decree 375/2020 (VII.30.) Effective from 31.07.2020
[4] Declared by Section 107 of Government Decree 375/2020 (VII.30.) Effective from 31.07.2020

Section 9 (1) The operators of essential services shall notify the security incidents with a significant effect on the continuity of essential services provided by them, to the Centre without undue delay.

(2) For determining the significance of the effect of the security incident, the notification of the operator of essential services shall contain the following data as well:

a) the number of users affected by the disruption of the essential service,

b) the duration of the security incident,

c) the geographical spread of the area affected by the security incident.

(3) If an operator of essential services bases the provision of any service regarded as essential for the maintenance of critical societal and economic activities on a third party-digital service provider, the mentioned service provider shall notify all the cases when the security incident concerning the digital service provider has a significant effect on the continuity of essential services.

Section 10 According to Section 11 and the government decree on the supervision of the electronic information security of the services related to information society and on the rules of procedure for security incidents, the digital service provider shall immediately notify the security incidents occurred in its electronic information systems to the Centre which have a significant effect on the provision of digital services provided by it within the European Union.

Section 11 (1) The notification of security incidents shall be submitted primarily by electronic means; however, if the electronic information system is damaged to the extent that it is not possible, the notification may be submitted in any other way.

(2) The notification shall contain at least

a) a brief description of the security incident, its status,

b) the extent of the disruption in the functioning of the service,

c) contact details of the contact person and the body designated by the operator for incident response,

d) the criteria for determining the effect of the security incident and

e) in the event of involvement of an intermediary service provider, the name and contact details of the intermediary service provider.

Section 12 (1) Based on the notifications under Section 9 (1) and 10, the Centre shall investigate the cross-border effect of the security incidents with a significant disruptive effect on the services of operators of essential services and digital service providers, and shall - in justified cases - inform directly or through the single point of contact the other Member States concerned, about the security incidents with a significant disruptive effect.

(2) In the course of the information provision under paragraph (1), the Centre shall ensure the security of the service providers and shall ensure that the confidentiality of their commercial interests and the confidentiality of the information contained in the notification is not compromised.

5. Voluntary notification

Section 13 (1) The sectoral actors under the Hungarian CIP Act who are not identified as operators of essential services may notify those security incidents to the Centre on a voluntary basis which have a significant effect on the continuity of the services provided by them. This provision shall not be applied to the infrastructures designated as European or national critical ones according to the Hungarian CIP Act.

(2) The digital service providers may notify every incident on a voluntary basis whose characteristics have been previously unknown to them, including, in particular, the new methods exploiting vulnerability, the data of exploits, the vulnerable points or threats.

(3) The Centre may prefer the processing of notifications to be investigated on a compulsory basis to voluntary notifications. Voluntary notifications shall be processed only in the case, if it does not constitute a disproportionate or undue burden on the Centre.

(4) Voluntary notification shall not result in the imposition upon the notifying body of any obligations to which it would not have been subject had it not given that notification.

6. Rules for security incident response and for its technical investigation

Section 14 In the investigation of the security incidents concerning the electronic information systems of state and municipal bodies, primarily

a) the information security officer,

b) the security incident response agent and

c) the competent incident response centre

may be involved.

Section 15 (1)[1] With the exception of the bodies determined in Section 6 (1), the head of the body being subject to national security protection shall send the data of the person indicated in the appointment or engagement to the Centre 30 days before the planned entry into force regarding

a) the appointment for the tasks in case of information security officer,

b) the engagement for the tasks in case of security incident response agent

with the consent of the person concerned for requesting opinion.

(2) The Centre shall send its opinion to the head of the body requesting opinion until the date of entry into force of the appointment or engagement for tasks.

(3) The security incident response agent shall be considered a person involved in the performance of tasks related to the security of an electronic information system determined in the Hungarian Cyber Security Act.

Section 16 (1) During the investigation of the security incident notified, the body concerned with the security incident shall cooperate with the Centre which cooperation covers:

a) the transmission of information related to the notification,

b) the transmission of technical data necessary for the identification of the persons concerned with the security incident (attacker/attacked person) to the Centre,

c) the measures to avert the consequences of security incidents upon the information of experts of the Centre and, while conducting a security incident investigation, the settings regarding the infrastructure,

d) the provision of access to the infrastructure concerned with the incident for the experts of the Centre and

e) the installation of early warning or trap systems, sensors considered necessary based on the risk analysis carried out by the Centre.

(2) Within the framework of cooperation, the operators of essential services shall share the special, sectoral characteristics related to the infrastructure concerned with the incident with the Centre.

---

[1] Amended by Section 114 c) of Government Decree 375/2020 (VII.30.)

(3) Within the framework of cooperation, the digital service providers and the operators of essential services under row 26 of Annex 4 of the Hungarian CIP Act shall, if necessary, introduce bans regarding the subscribers concerned with the incident upon the request of the Centre and shall restrict, suspend or terminate access rights (user, subscriber).

Section 17 (1) Upon the request of the Centre, the body concerned with the security incident - with the exception of paragraph (2) - shall collect the technical data, information necessary for security incident response and transmit them in electronic format or make them available in another way.

(2) If the body concerned with the security incident - with the exception of paragraph (3) - is unable to collect the data under paragraph (1) for any reason, the Centre may collect the data. The body concerned with the security incident shall ensure that the Centre has access to the data.

(2a)[1] The Information Office shall transmit the technical data, information under paragraphs (1) and (2), necessary for security incident response or make them available in another way, that it shall not result in recognition of the data stored in the electronic information system, by the Centre.

(3) If the digital service provider concerned with the security incident is unable to collect the data under paragraph (1) for any reason, the representative of the incident response centre shall make a proposal for the method of collection and provision of the data necessary within the framework of an on-site consultancy with the involvement of the experts of the body concerned. The digital service provider concerned with the security incident shall ensure that the incident response centre has access to the data.

(4) The body concerned with the security incident - with the exception of paragraph (5) - shall make data, documents, tools and other information necessary for the investigation available to the Centre.

(5) The digital service provider concerned with the security incident shall make the bit-by-bit copies containing data, documents, tools and other information necessary for the investigation available to the Centre.

(6) The Centre - with the exception of paragraph (7) - shall develop the measures necessary to eliminate security incidents in cooperation with the body concerned with the security incident, which shall be implemented by the body concerned with the security incident.

(7) The digital service provider concerned with the security incident shall develop the measures necessary to eliminate the security incident and shall immediately implement them. The Centre shall support the digital service provider concerned with the security incident in developing the measures necessary to eliminate security incidents.

(8) The digital service provider concerned with the security incident shall review the completeness of risk analysis and risk management of its electronic information systems after the elimination of the incident and shall implement the necessary modifications.

(9) The Centre shall keep closed technological logs about security incidents, which contain the measures taken during the support of the investigation of security incidents and their results as well.

Section 18 (1) Based on the information and data requested and compulsorily transmitted from the bodies and incident response centres operating the electronic information system falling within its competence, the Centre shall analyse, assess the signs indicating security incidents and threats concerning electronic information systems and shall inform the operator of the electronic

[1] Added by Section 108 of Government Decree 375/2020 (VII.30.) Effective from 31.07.2020

information system about the danger of occurrence of a security incident or its existence, as well as about the proposed measures, through its continuous emergency service system.

(2) The Centre may prepare an assessment by monitoring continuously the technical data and information taken from the centralized IT and electronic communication service provider and may search for signs indicating security incidents and threats affecting the operation of networks and services.

(3) In the course of security incident response by the Centre, the centralized IT and electronic communication service provider shall

a) transmit the technical data necessary for the identification of the persons concerned with the security incident, the attacker and the attacked persons, to the Centre,

b) apply security measures, technical solutions against known threats,

c) provide the data under Section 17 (1) upon the request of the Centre to analyse and assess the signs indicating intervention to network traffic and

d) cooperate in the tasks determined by the Centre, regarding security incidents.

Section 19 (1) In the course of security incident investigation, the incident response centre may, if necessary, familiarize itself with the different regulations, rules of procedures ensuring the service- or business continuity of the intermediary service providers, including, in particular, their business continuity plan, their disaster recovery plan.

(2) Within the framework of the cooperation with the incident response centre, the intermediary service provider concerned with the security incident shall provide data necessary for the identification of the persons concerned with the security incident, the attacker and the attacked person to the Centre, upon the request of the incident response centre for the purpose of specified security incident response, and shall, if necessary, introduce bans regarding the subscribers concerned with the incident and shall restrict, suspend or terminate user or subscriber access rights.

(3) In case of provision of service considered as dangerous or harmful, the incident response centre may oblige the intermediary service provider to prohibit the given service.

(4) The Centre shall inform the authority under Section 6/B (3) of the Hungarian Electronic Commerce Act, if the intermediary service provider fails to perform its cooperation obligations.

Section 20 The purpose of the technical investigation of the data related to security incidents is that that the Centre

a) explores the reasons, circumstances of occurrence of the security incident, the extent of the damage caused,

b) determines the scope of electronic information systems and system elements concerned with the security incident,

c) makes a proposal to eliminate damage caused by the security incident and

d) informs the other bodies and authority concerned with the security incident about the lessons learnt from security incident occurred, in order that the occurrence of the security incident can be prevented in the future

through investigation of security incidents occurred.

Section 21 The body not performing its notification, information or cooperation obligations shall be reported by the Centre to the authority supervising the given electronic information system.

7. Vulnerability testing

Section 22 (1) The vulnerability testing of electronic information systems of the state and municipal bodies being subject to national security protection, of electronic information systems of the infrastructures designated based on legal regulations as European or national critical infrastructures of the state and municipal bodies under Section 2 (1) of the Hungarian Cyber Security Act, as well as the vulnerability testing of closed electronic information systems shall be carried out - with the exception of paragraphs (2) and (3) - by the Centre. Furthermore, the Centre is entitled to carry out vulnerability testing as the state body under Section 18 (3) of the Hungarian Cyber Security Act.

(2)[1]

(3) The vulnerability testing of the electronic information systems for national defence purposes shall be carried out by the incident response centre under Section 6 (1).

(4) The business entity under Section 18 (3) *b)* of the Hungarian Cyber Security Act (hereinafter referred to as 'business entity') may carry out vulnerability testing, if

a) the person involved in vulnerability testing, acting on behalf of and employed by the business entity, has a qualification certifying the knowledge necessary to perform vulnerability testing in addition to the conditions specified in Section 18 (4) of the Hungarian Cyber Security Act and has at least two years of professional experience in this special field, as well as

b) the business entity is registered in the record of business entities entitled to perform vulnerability testing.

(5) The Constitutional Protection Office shall keep a record about business entities entitled to perform vulnerability testing. The record shall contain the data of business entities, the numbers of persons involved in vulnerability testing and the name of the qualification certifying the knowledge necessary to perform vulnerability testing and the date on which it was acquired.

(6) Regarding the data under paragraph (5), the Constitutional Protection Office shall provide information to the bodies operating electronic information systems entitled to initiate vulnerability testing based on Section 18 (2) of the Hungarian Cyber Security Act, upon individual written request, within fifteen days after the receipt thereof.

(7) The registration in the record shall be initiated by the business entity at the Constitutional Protection Office, by submitting the documents certifying the conditions specified in paragraph (4). Regarding the professional conformity of the conditions specified in paragraph (4), the statement of the Centre is governing.

(8) The Constitutional Protection Office shall refuse the request for registration in the record, if

a) the business entity has no facility security clearance set out in Section 18 (3) *b)* of the Hungarian Cyber Security Act,

b) the qualification certifying the knowledge necessary to perform vulnerability testing and at least the two years of professional experience in the special field is not met, based on the statement of the Centre, or

c) the data provided by the business entity does not correspond to the reality.

(9) The business entity entitled to perform vulnerability testing shall inform the Constitutional Protection Office about the change in the eligibility criteria and the change regarding the persons involved in vulnerability testing within eight days after the change.

---

[1] Repealed by Section 114 d) of Government Decree 375/2020 (VII.30.) Ineffective from 31.07.2020

(10) The Constitutional Protection Office is entitled to check whether the eligibility criteria are met and the data in the record are authentic. In case of failure to notify and lack of eligibility criteria, the Constitutional Protection Office shall remove the business entity from its record.

(11) The business entity registered in the record kept under paragraph (5) shall resend the documents under paragraphs (4) and (7) to the Constitutional Protection Office in every second year after the registration. The reporting shall be performed trough the chief of security until the last day of the month corresponding to the month shown in the certificate of registration issued by the Constitutional Protection Office.

(12) The Constitutional Protection Office shall check again based on the documents sent, whether the criteria under paragraph (4) are met.

(13) If the business entity fails to perform data reporting obligations specified in paragraph (11), the Constitutional Protection Office shall remove the business entity from the record.

Section 23 (1) The vulnerability testing aims to detect the weak points of electronic information systems, system elements of the body concerned, before any security incident has occurred and to develop detailed proposals for solutions regarding elimination of detected errors, for strengthening protection and the security of electronic information systems, system elements.

(2) The subject of vulnerability testing is the investigation of electronic information systems, system elements, tools, procedures and related processes used for processing data, information, as well as the investigation of general IT preparedness of the persons managing them and the investigation of the compliance with IT and information security regulations, rules used at the body concerned.

(3)[1] The Information Office shall ensure that the vulnerability testing concerning its electronic information system is carried out without the recognition of the data stored therein, by the Centre.

Section 24 (1)[2] During vulnerability testing, the following investigations shall be carried out according to the basic document establishing the procedure for vulnerability testing:

a) external IT security investigation,

b) web investigation,

c) automated investigation,

d) psychological manipulation,

e) internal IT security investigation and

f) wireless network IT security investigation.

(2) The vulnerability testing may contain three types of eligibility phases regarding the directions specified in paragraph (1) *a)* to *c)*, *e)* and *f)*:

a) investigation without registered user permission,

b) investigation with registered user permission and

c) investigation with administration privileges.

(3) According to the investigations specified in paragraph (1), the deadline of vulnerability testing is:

a) in case of external IT security investigation thirty days,

b) in case of web investigation seventy-five days,

c) in case of psychological manipulation ninety days,

d) in case of internal IT security investigation ninety days,

e) in case of wireless network IT security investigation thirty days

---

[1] Added by Section 19 of Government Decree 375/2020 (VII.30.) Effective from 31.07.2020

[2] Amended by Section 113 a) of Government Decree 375/2020 (VII.30.)

from the date of the decision of the authority or from the start date agreed in advance.

(4)[1] In case of investigation without registered user permission, the body concerned

a) shall send the data belonging to access points of the IT system and service to be investigated to the Centre, shall ensure the opportunity of physical and logical availability of access points also in case of systems with limited access,

b) shall ensure the monitoring of the IT system and service to be investigated to the Centre,

c) shall ensure the function testing plan and

d) shall ensure the documentation about the result of testing.

(5)[2] In case of investigation with registered user permission, the body concerned shall send the followings in addition to the requirements of paragraph (4) to the Centre:

a) the user eligibility matrix and

b) the user documentation.

(6)[3] In case of investigation with administrator privileges, the body concerned shall send the system plan to the Centre in addition to the requirements of paragraphs (4) and (5).

Section 25 (1)[4] While preparing for vulnerability testing, the body carrying out vulnerability testing shall prepare a basic document for vulnerability testing. In the basic document for vulnerability testing, the investigation duties, goals, technical and personal conditions, the methodology, the expected date of completion of coordination and vulnerability testing shall be stated.

(2)[5] If the vulnerability testing is ordered by the authority, the investigation duties determined in the decision shall be indicated in the basic document for vulnerability testing. In case of individually initiating vulnerability testing, the initiator may make a proposal for investigation duties about which the body carrying out vulnerability testing shall decide.

(3)[6] The basic document for vulnerability testing shall be sent to the body concerned by the body carrying out vulnerability testing. The body concerned may make observations to the content of the basic document for vulnerability testing within eight days after receipt. The observation may not affect the investigations ordered by the authority. The body carrying out vulnerability testing shall decide on the observations.

(4)[7] The vulnerability testing may not be carried out, if the conditions determined in the basic document for vulnerability testing and in this Decree are not completely met.

(5)[8] The implementation of vulnerability testing shall be suspended, if the conditions determined in the basic document for vulnerability testing and in this Decree are not completely met.

Section 26 (1) During vulnerability testing, the body carrying out vulnerability testing shall proceed with due diligence and care, so as not to restrict the services provided by the investigated electronic information system to a greater extent than it is absolutely necessary, and shall carry out vulnerability testing in a non-critical period regarding the service. The body carrying out vulnerability testing shall inform the body concerned, about the expected extend and duration of the restriction in advance.

---

[1] Added by Section 110 of Government Decree 375/2020 (VII.30.) Effective from 31.07.2020
[2] Added by Section 110 of Government Decree 375/2020 (VII.30.) Effective from 31.07.2020
[3] Added by Section 110 of Government Decree 375/2020 (VII.30.) Effective from 31.07.2020
[4] Amended by Section 113 b) of Government Decree 375/2020 (VII.30.)
[5] Amended by Section 113 c) of Government Decree 375/2020 (VII.30.)
[6] Amended by Section 113 d) of the Government Decree 375/2020 (VII.30.)
[7] Added by Section 111 of the Government Decree 375/2020 (VII.30.) Effective from 31.07.2020
[8] Added by Section 111 of the Government Decree 375/2020 (VII.30.) Effective from 31.07.2020

(2) In case of vulnerability testing ordered by an authority decision, the body concerned shall make the data, documents, tools and other information necessary to vulnerability testing available to the body carrying out vulnerability testing and shall suffer the reduction of service in the investigated electronic information system, resulting from vulnerability testing.

(3) In case of individual initiative, the body concerned may exclude the investigations during observation pursuant to Section 25 (3) which result in significant reduction of service.

(4) The body carrying out vulnerability testing may extend the time limit for vulnerability testing once, before the end of the term for testing, for not more than thirty days, and shall inform the body concerned and the authority thereof.

Section 27 (1) For the implementation of the vulnerability testing initiated within the own competence of the Centre, the bodies under Section 22 (1) shall notify the specific technical data, identifiers regarding the availability of web services, webpages, webservers to the Centre.

(2)[1] In case of electronic information systems for national defence purposes, the data specified in paragraph (1) shall be notified to the incident response centre under Section 6 (1).

(3) In case of changes in the availability of web services, the notification shall be given within 3 days.

(4) The Centre shall inform the body concerned about the IP address used for its investigation or other specific technical identifier, which may not be prohibited from the access to the web service by the body concerned.

Section 28 (1) The electronic information system of the body concerned significantly differs from the average, if

a) the electronic information system has

aa) a device available on an external Internet domain at more than 20 IP addresses,

ab) more than 10 web services,

ac) more than 50 servers regarding the internal network,

ad) more than 500 workstations,

ae) more than 5 wireless networks or

af) more than 500 users, or

b) the body concerned has the electronic information system concerned with the investigation on more than three sites.

(2) If the electronic information system, system element of the body concerned significantly differs from the average and therefore specific vulnerability testing is needed, the time limit for vulnerability testing may be extended with further thirty days in addition to that specified in Section 24 (3).

Section 29 (1) At the closure of vulnerability testing, the body carrying out vulnerability testing shall draw up an opinion and shall send it to the body concerned and the authority within eight days.

(2) The opinion under paragraph (1) shall contain

a) the description of investigation results and

b) the proposals for short-, medium- and long-term measures.

(3)[2] The body carrying out vulnerability testing shall send the opinion to the body concerned and the authority within 21 days, in the case any of the conditions specified in Section 28 (1) exists.

---

[1] Declared by Section 112 of the Government Decree 375/2020 (VII.30.) Effective from 31.07.2020

[2] Added by Section 112 of Government Decree 375/2020 (VII.30.) Effective from 31.07.2020

8. Final provisions

Section 30 This Decree shall enter into force on 1 January 2019.

Section 31 (1) This Decree serves the purpose of compliance with

a) the Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market,

b) the 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.

(2) This Decree lays down the provisions necessary for the implementation of the 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.

Section 32 The draft of this Decree was notified in advance according to Article 15 (7) of the Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.

Section 33