Government Decision 1838/2018 (XII.28.)
on the Strategy for the security of network and information systems in Hungary

The Government

1. adopts the Strategy for the security of network and information systems in Hungary (hereinafter referred to as 'Strategy');

2. calls on the Minister of Interior to prepare an action plan with the involvement of the ministers concerned, to implement the measures under points 1 to 56 in the Strategy.

Responsible: Minister of Interior
ministers concerned
Deadline: 31 Marc 2019

3. This decision shall enter into force on the day following of its promulgation.

Viktor Orbán signed,
prime minister

The Strategy for the security of network and information systems

The explosion of information and communication technology (ICT) is bringing significant changes in all areas of society. The Government adopted and announced the National ICT Strategy in 2014, which aimed to develop the complete domestic digital environment on four pillars (digital infrastructure, digital economy, digital state, digital skills).
The modern state, all its organizations and citizens are necessarily becoming users of a wider range of the increasingly complex electronic infrastructures, the electronic information systems. However, besides the benefits of dynamic development of the opportunities of information society, the increase in abuses, attacks and threats is also a serious challenge in almost all areas. A series of tasks needs to be solved not only for the purpose of following the development of technology, but at the same time also in terms of the various aspects of security and threats.
Information and communication technology and devices offer opportunities in all areas of development and innovation, however they also provide an opportunity for terrorism and cybercrime. The wider the scope of these possibilities is, the more energy and attention the security and protection issues require.
The implementation of an innovative and secure cyberspace is a common interest, a common task of cyber security professionals, public- and market actors as well as citizens.

The Strategy for the security of network and information systems (hereinafter referred to as 'Strategy') covers Hungary, aims to create a free, secure and innovative cyberspace, to increase Hungary's competitiveness, to introduce and adapt innovations, new technological solutions in digitalized public administration, governmental and economic areas in a safe way, to create a more secure e-government system, to develop public services in an innovative way, as well as to raise cyber security and awareness, the level of preparedness in all areas of society.

The Strategy is considered a policy strategy under the provisions governing strategy-making pursuant to Government Decree 38/2012 (III.12.) on government strategic governance.

Background, connections

In the changed national and international environment as a result of the cyberspace's coming into being, the Government Decision 1139/2013 (III.21.) on the National Cyber Security Strategy of Hungary (hereinafter referred to as 'National Cyber Security Strategy') emphasizes the importance of creating and ensuring cyber security and states that Hungary undertakes to carry out tasks related to the protection of cyberspace with responsibility.
The basic purpose of the National Cyber Security Strategy is to ensure the development of a free, secure and innovative cyberspace by creating the cornerstones of information security and using, further developing existing tools, organizations and knowledge; to this end, it set important and fundamental goals, namely:

a) establishing an organizational system and coordination under government responsibility,
b) enhancing international cooperation,
c) developing shared public-private responsibility,
d) encouraging education and research and development programs,
e) raising awareness,
f) strengthening the role of child protection.

First in 2013, the National Cyber Security Strategy defined the decisive role of the Hungarian cyberspace in economic and societal life, as part of the global cyberspace. Along the National Cyber Security Strategy, with view of the threats coming from cyberspace and the risks involved, the preparation of Hungarian legal regulations began with the collaboration of governmental, market and social actors. Act L of 2013 on the electronic information security of state and municipal bodies (hereinafter referred to as 'Hungarian Cyber Security Act') adopted with the National Cyber Security Strategy and amended several times since then, created the legal environment which facilitated the establishment and consolidation of state organizations in the field of cyber security primarily with regard to state, administrative electronic information systems.

The Information Security Strategy Committee, which was established in early 2017 by the National Cyber Security Center as organizer and by involving IT security experts, set out guidelines for the purposes of the new strategy taking into account the available analyses and the situation assessment and SWOT analysis formulated in the Digital Welfare Program.

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 (NIS Directive) was published in the Official Journal of the European Union on 19 July 2016, which is the first piece of legislation at Community level in the field of information security, and which lays down rules and mandatory cooperation for certain institutions on a mandatory and geopolitical basis. The NIS Directive imposes an obligation on EU Member States to draw up a strategy in line with its provisions.

While drawing up the Strategy, the protection of network and information systems needs to be strengthened by maintaining the values stated in the National Cyber Security Strategy, building on its results, but responding to new challenges and threats, identifying new opportunities and goals in order to meet the challenges of the modern age in all aspects.

The Strategy functions supplemented with the declaration regarding 'Information security and cyber security' by the Government Decision 1456/2017 (VII.19.) on the 2016 monitoring report of the National ICT Strategy, the Digital Prosperity Program 2.0, namely an extension of the

Digital Prosperity Program, the adoption of its work plan for 2017-2018, further developments in digital infrastructure, competencies, the economy and public administration (hereinafter referred to as 'Digital Prosperity Program 2.0'), identifies with its content and develops in parallel. Both documents promote the achievement of Hungary's cyber security interests and goals by setting out those national goals, directions, tasks and instruments, on the basis of which Hungary can enforce its national interests in cyberspace.

The complex system of the Digital Prosperity Program 2.0 aims to optimize the societal and economic impact of digitalization in order to maximize its benefits in all areas of society and economy.

Legislation, connections to domestic strategies

This Strategy:

a) reflects the basic values formulated in the Fundamental Law (freedom, security, rule of law, international and European cooperation);

b) treats the internationally accepted principles formulated in the 2001 Budapest Convention ('Convention on Cybercrime') as a basis;

c) is in line with the NATO's Strategic Concept adopted in November 2010, the Organization's Cyber Security Policy adopted in June 2011 and its implementation plan, as well as with the cyber security principles and purposes of the Organization as set out in the documents of the NATO Summit in Lisbon on 19-20 November 2010 and in Chicago on 20-21 May 2012, as well as the 2016 NATO Summit in Warsaw;

d) is in line with the Joint Communication of the European Commission and the High Representative for the Common Foreign and Security Policy of the European Union of 7 February 2013 entitled 'Cyber Security Strategy of the European Union: An Open, Secure and Reliable Cyberspace';

e) contributes to the domestic implementation of the NIS Directive;

f) is in line with the information security purposes of the Act L of 2013 on the electronic information security of state and municipal bodies, and with the organizational structure laid down by the act;

g) takes into account the provisions governing strategy-making in Government Decree 38/2012 (III.12.) on government strategic governance;

h) details the responses to the challenges outlined in point 31 of the National Security Strategy of Hungary adopted by the Government Decision 1035/2012 (21 February);

i) responds the challenges outlined in points 33, 52 and 82 of Government Decision 1656/2012 (XII.20.) on the adoption of the National Military Strategy of Hungary;

j) is line with the information security purposes for 2014-2020 outlined in the National ICT Strategy of Hungary adopted by Government Decision 1069/2014 (II.19.);

k) uses the status assessments of the 2016 monitoring report of the National ICT Strategy and the Digital Welfare Program 2.0;

l) integrates the security goals outlined in the Digital Child Protection Strategy of Hungary established within the framework of the Digital Welfare Program, in Hungary's Digital Export Development Strategy and in Hungary's Digital Education Strategy (Digital Education Strategy, 2017).

The sectoral legislation and normative acts governing public organisations covered by the Strategy are the following:

1. the Act CVIII of 2001 on certain aspects of electronic commerce services and information

society services
2. the Act CLXVI of 2012 on the identification, designation and protection of critical systems and facilities
3. the Act CCXXII of 2015 on general rules for electronic administration and trust services
4. the Act L of 2013 on the electronic information security of state and municipal bodies
5. the Government Decree 65/2013 (III.8.) on the implementation of Act CLXVI of 2012 on the identification, designation and protection of critical infrastructures and facilities
6. the Government Decree 360/2013 (X.11.) on the identification, designation and protection of critical energy systems and facilities
7. the Government Decree 541/2013 (XII.30.) on the identification, designation and protection of critical water management infrastructures and hydraulic establishments
8. the Government Decree 185/2015 (VII.13.) on the functions and powers of Government incident response center and incident response centers, and the rules for security incident response and technical investigation of security incidents, and for conducting vulnerability testing
9. the Government Decree 187/2015 (VII.13.) on the functions and powers of the authority responsible for the supervision of electronic information systems security and the information security supervisor, as well as on the definition of closed electronic information systems
10. the Government Decree 246/2015 (IX.8.) on the identification, designation and protection of systems and facilities in healthcare
11. the Government Decree 330/2015 (XI.30.) on the identification, designation and protection of critical systems and facilities of the financial sector
12. the Government Decree 249/2017 (IX.5.) on the identification, designation and protection of critical systems and facilities of the information and communication technology sector
13. the Government Decree 410/2017 (XII.15.) on digital service providers
14. the Decree 41/2015 (VII.15.) of the Minister of Interior on the requirements relating to the technological security and secure information devices and products, and to the security classification and declaration of security levels determined in the Act L of 2013 on the electronic information security of state and municipal bodies
15. the Government Decision 1233/2018 (IV.25.) on providing the resources needed to carry out the implementation tasks of the directive concerning measures for a high common level of security of network and information systems across the Union

Interpretation of key definitions of the Strategy

'Cyberspace' means a set of globally interconnected, decentralized, ever-changing electronic information systems and societal and economic processes in the form of data and information through these systems. Hungary's cyberspace is the part of electronic information systems of the global cyberspace which is located in Hungary, and from among societal and economic processes in the form of data and information through the electronic systems of global cyberspace those which takes place in Hungary or are directed to Hungary or in which Hungary is involved.

'Cyber security' means continuous and planned use of political, legal, economic, educational, awareness-raising and technical tools to manage existing risks in cyberspace which, ensuring an acceptable level of risk in cyberspace, transform cyberspace into a reliable environment for the smooth functioning and operation of societal and economic processes.

'Security incident response' means documenting the security incident in the electronic information system, eliminating its consequences, determining the causes and responsibilities, and taking planned action to prevent the occurrence of similar security incidents in the future.

'Network and information system' means an electronic communication network as defined in the Electronic Communication Act, and any device or group of interconnected or related devices from among which one or more perform automated processing of digital data under a program; or the digital data stored, processed, retrieved or transmitted for the purpose of its operation, use, protection and maintenance.

Establishment on the justification for developing a strategy for the security of network and information systems

The opportunities offered by digital technology, which have become available to almost everyone, pose a significant cyber security risk, as threats from cyberspace disrupt the proper functioning of information and communication systems and government backbone networks, endanger the information assets and critical infrastructure elements of nation states. Large-scale cyberattacks are becoming more common. The complexity and volume of cyber threats are increasing, and also various groups and organizations are using cyberspace to spread ideologies in an increasingly intense way.

The main purpose of cybercrime is causing damage, the mass acquisition of financial and personal data, as well as economic, financial, political influencing. Beyond data theft, crippling of electronic services for damaging purposes, distribution of spams and malicious codes and the development of robotic networks (networks of infected machines that can be used for malicious purposes) are widespread. A significant threat is hacktivism that often covers ideologically motivated attacks to achieve some ideological goals or to mediate some ideology. Sophisticated covert attacks, typically for cyber espionage, pose a growing threat, which are presumably backed by state support.

Extremely sophisticated attacks are important sources of threat under which attackers can carry out their harmful activities in secret for a long time (information leakage, destruction, espionage, etc.).
Attacks on network and information systems as critical information infrastructures become more common, more complex and more sophisticated. Attacks are characterized by obstruction of the core functions necessary to sustain the functioning of society, therefore they seek to weaken the internal cohesion of society.

The number of cyberattacks against critical infrastructures shows a significant increase. This increase is supported by the fact that based on the data of the ICS-CERT for the prevention of various cyberattacks on industrial systems (critical infrastructure security organization in the USA) had to deal with only 39 security incidents in the United States in 2010, while this number was already 140 in 2011 and 290 in 2016.

According to the data of Eurostat[1], almost all businesses in the EU (98%) use computer recently, and only 32% of them have a formally defined information security policy. Regarding

[1] Sources used:
https://ec.europa.eu/eurostat/cache/infographs/ict/
https://ec.europa.eu/eurostat/web/digital-economy-and-society/data/main-tables
https://ec.europa.eu/eurostat/web/digital-economy-and-society/data/database

large companies, this proportion reached 72%, while for small and medium-sized enterprises it was less than a third (31%).

According to Eurostat's 2016 data on the IT security preparedness of companies, Hungary is lagging behind the countries of the European Union, as only 9% of the small and medium-sized enterprise sector has an information security policy, while in the case of Hungarian large companies this proportion is 53%.

Among the Hungarian companies, in the most unprepared construction sector, on average, 3% have, while even in the most prepared ICT sector only 36% have IT security policy. While in the EU, on average, more than 20% of the companies provide for protection in the event of a security incident involving the destruction or damage of data, this ratio does not reach 10% for any of the risks in the case of Hungarian companies.

According to relevant data, 75% of domestic Internet users use Windows operating system, including 10% of them, who still use the outdated, vulnerable Windows XP, which Microsoft has not supported with security updates since 2014, while its global share is barely one-fifth of that (2.2%). The proportion of Internet users on mobile phones or other smart devices is growing rapidly, the Android operating system being the most popular (38%), the safe use of which requires more attention from the users, and most device manufacturers do not provide security updates after a few years from the date of release.

According to the World Bank's 2016 data, the Hungarian Internet servers use a much lower proportion of secure encryption solutions than the average of the European Union or even OECD countries.

According to Eurostat's 2016 data on the labour market situation of IT professionals, just over a quarter of businesses across the EU employ some kind of IT professional. While this usually means own employees in the case of operational responsibilities, it is outsourced for information and data security jobs at more than half of the companies.
Among the businesses that planned to hire some kind of IT professional, more than half of the Hungarians reported difficulties, while this proportion is, on average, only 40% in the EU.

According to the latest data, the proportion of infected machines is 14.1% in Hungary, 7.8% worldwide. For comparison with some European countries this proportion is for instance 2.9% in Germany, 5.5% in France, 10.2% in Croatia, 7.6% in Slovakia.

According to the data of the Magyar Nemzeti Bank (Central Bank of Hungary - MNB), 1.3 billion forints in damage was incurred at the financial institutions in 2016 from electronic payment abuses – from the vast majority of transactions initiated via Internet and mobile phones –; although nearly 90% of the attempts detected failed, this still resulted in a reduction of only around 50% in damage value.

---

https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_enterprises

http://ec.europa.eu/information_society/newsroom/image/document/2018-20/hu-desi_2018-country-profile-lang_4AA43283-EC48-996F-09918493E34A691F_52334.pdf

These types of damage are comparable in magnitude to damage from bank card fraud; however, they far exceeded the damage caused by abuses linked to paper-based transactions or even ATMs.

The number and total value of damage attributable to electronic systems also shows an increasing trend in the period between 2008 and 2016 examined by the MNB.

According to Eurostat's data on household Internet use in 2008-2016, almost half of the Hungarians aged 16-74 (48%) has already used the Internet in order to get in contact with a public institution; this ratio gradually caught up with the EU average from 28% in 2008, despite the fact that the Hungarian population uses the Internet in a slightly smaller proportion (79%) than the EU average (82%). 71% of the EU citizens (who used the Internet in the year prior to the 2016 survey) has already shared some personal data online. The most common types are contact information (61% of the Internet users), which is followed by personal data, for instance name, birth date or ID card number (52%) and payment data, for instance credit/debit card or bank account number (40%). Nearly more than one-fifth (22%) provided other personal data, for instance photos or information on their health, employment or income.

It seems that the younger generations make their personal data more accessible: more than three-quarters (78%) of the Internet users aged 16-24 shared some personal information online, compared to 57% of the users aged 65-74.

In Hungary, 36% of the Internet users reported finding a virus or other infection on their computer.

The Hungarian Cyber Security Act prescribing IT security requirements to state and municipal institutions provides an opportunity for bodies as an interim measure to achieve the required security level gradually, at the same time it can be concluded that the institutions are significantly behind in catching up. Meeting new security requirements in an existing system requires significantly more effort, than an additional need to take the requirements into account when designing a new system. As the institutions did not have the resources to meet these additional security needs either as a subjective right or through tenders, these requirements are met only in exceptional cases where the institution managed them or took them into account in its new development.
To enforce a higher rate of compliance with security requirements, from 2016 the National Electronic Information Security Authority (hereinafter referred to as ‘National Electronic Information Security Authority’) integrated its monitoring into the tender procedure published in the call for proposals of the Public Administration Development Operational Program (PADOP). In this context, the National Electronic Information Security Authority carries out the monitoring of the compliance of the established electronic information systems financed by the PADOP projects with the information security norms and requirements, already from the planning stage. Beyond the monitoring, the National Electronic Information Security Authority also helps the stakeholders with targeted awareness-raising, information and advisory activities in order to support the successful and safe realization of the projects.

The maturity of the domestic market in the field of cyber security of business IT development projects is currently low. Hungarian companies, especially small and medium-sized enterprises (SMEs), typically pay little attention and resources to cyber security in digital development

projects. The reason for this is the low capital supply and the fact that security does not play a central role in the digital attitudes of the customers served, thus they do not even demand high cyber security requirements from service providers.
The market expects, first of all, low investment and operating costs from IT projects, secondly it focuses on meeting functional and performance requirements.
Cyber security considerations are less marginalized for those market actors, where the current legal regulations impose data protection and business continuity requirements, which are enforced by authority supervision (e.g. regarding payment service providers and insurance companies). As a result, IT security management in Hungarian digital development projects does not reach the level required by current and expected threats identified in cyberspace and the vulnerabilities of the implemented systems, as well as the resulting risks.

The following need to be recorded in relation to critical infrastructure protection. Based on the Council Directive 2008/114/EC being effective from 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, critical infrastructure status is determined according to a different methodology for each sector, but in each case, it ends with an itemized designation. The sectors in which the designation criteria have been defined by 31 December 2017 are as follows:

a) energy,
b) water,
c) agricultural economy,
d) protection of public security,
e) healthcare,
f) finance,
g) national defence,
h) information and communication technology.

Number of registered crimes according to the definitions of the European Union Working Party on General Matters including Evaluation (hereinafter referred to as 'GENVAL')

Number of registered crimes according to the definitions of the GENVAL	**In 2013**	**In 2014**	**In 2015**	**In 2016**	**In 2017**
Acts affecting only information systems, mainly related to cyberattacks	**3554**	**2398**	**2819**	**4187**	**5098**
Information system fraud	250	1398	2176	3409	4467
Violation of information systems or related data breach	823	565	520	702	586
Circumvention of technical security measures protecting information systems	580	31	15	44	8
Abuse of non-cash payment instruments	1897	388	95	20	28
Illegal data acquisition	4	16	13	12	9

Acts where computer/IT systems serve as a tool or target, especially in the case of online bank card fraud	**3959**	**917**	**873**	**23439**	**1120**
Counterfeiting non-cash payment instruments	49	118	95	392	713
Facilitating the counterfeiting of non-cash payment instruments	3	1	3	3	1
Abuse of non-cash payment instruments	3907	798	775	23044	406
Total:	**7513**	**3315**	**3692**	**27626**	**6218**

In 2016, GENVAL reviewed and assessed the practical implementation and operation of European policies concerning the prevention of and fight against cybercrime in Hungary.

As a result of the assessment, GENVAL concluded that Hungary is committed to taking effective domestic and international joint actions against cybercrime to which it also gave a number of tangible signs (Presidency Conference in 2011, Budapest Cyberspace Conference in 2012, Cyber Security Strategy, comprehensive development of institutional system and response capabilities, active participation in forms of cooperation regarding Council of Europe, UN, EU and the National Cyber Security Conference held for the third time in 2018, which aimed at promoting cooperation between the public and private sectors to a higher level).

Based on the experience of the last 5 years, it can be stated that Hungary treats the issue as a priority and supports relevant forms of EU and international cooperation and initiatives, strives to keep up with trends, technical developments. Significant progress has been made in developing the responsiveness of both the institutional system and law enforcement and crisis management mechanisms. The evaluation committee of the GENVAL Working Group made some suggestions, as for instance that a closer and more regulated cooperation is needed between areas of cyber security and cyber law enforcement.

Governance Framework for the Strategy

Current and future cyber security challenges can only be addressed effectively and require an effective national cyber governance system. Taking into account the defence commitments at NATO and at European Union level, the European and international cooperation and information-sharing agreements at various levels, the NIS Directive and horizontal issues related to cyber security.

The National Cyber Security Coordination Council (hereinafter referred to as ‘Council’) is the proposing and advisory body of the Government, which coordinates the activities of the bodies specified in the law as defined in the law and its implementing regulations, thus implementing the governmental coordination included in Hungary's National Cyber Security Strategy. The Council is made up of the state officials delegated by ministers in the fields affected by cyber security, as well as the heads of certain national competent bodies not under the control of the Government.

The Council is assisted by the Cyber Security Forum composed of senior economic, scientific and civil society leaders, which supports the Council in its work as an advisory and proposing body.
The Council's coordination activities and the implementation of its decisions are assisted by sectoral and functional cyber security working groups. Civil servants and non-governmental experts invited by the cyber coordinator, on the basis of proposals from the Council and the Forum, take part in their work.

As a result of the amendment of the Hungarian Cyber Security Act effective from 16 July 2015, the National Cyber Security Center was established from 1 October 2015 under the direction of the Special Service for National Security which covers the GovCERT-Hungary, the National Electronic Information Security Authority and the E-Security Intelligence Center and which enables more efficient task execution and information flow. The qualitative and quantitative development of the available capacities of the National Cyber Security Center is justified by the growing demand for electronic information security supervisory and support tasks.

Regarding state and municipal bodies covered by the Hungarian Cyber Security Act, the general competence in security incident response belongs to the incident response center functioning within the Special Service for National Security, and the official authority competence belongs to the National Electronic Information Security Authority also functioning within the Special Service for National Security.
The Special Service for National Security also performs official authority and incident response tasks for digital service providers under the NIS Directive and – with the exception of the electronic information systems for defence purposes and electronic information systems of the national security service performing civil intelligence activities – incident response tasks related to critical systems designated as European or national critical infrastructures.

Regarding the electronic information systems for defence purposes, the organization performing military national security activities and the national security service performing civil intelligence activities independently perform security incident response, supervision and other information security functions in relation to their own systems.

Regarding the electronic information systems of the infrastructures designated as European or national critical infrastructures based on the Act on the identification, designation and protection of critical systems and facilities, the official authority tasks under the Hungarian Cyber Security Act are performed by the Ministry of Interior National Directorate General for Disaster Management (NDGDM).

Regarding the electronic information systems and communication service providers not covered by the Hungarian Cyber Security Act, the Institute for Computer Science and Control of the Hungarian Academy of Sciences operates an information security incident response organization (HunCERT).

Within the framework of the National Information Infrastructure Development (NIID) Program, the Government Informatics Development Agency operates a computer security incident response organization (NIID CSIRT). The NIID CSIRT is an IT security and incident response group belonging to the NIID Program, to a service provider of the Hungarian public education, higher education, research and public collections. The purpose of the group is to assist in the response and coordination of computer and network security incidents in all cases where at least one NIID member institution is involved. Furthermore, the working group of the

NIID CSIRT also provides important security, prevention and rectification information to the NIID member institutions.
The Faculty of Law Enforcement at the University of Public Administration established the Department against Cybercrime within the Institute of Criminalistics in order to ensure an adequate number of specialists who participated in specialized law enforcement training in the higher education system. The Cyber Security Academy of the University of Public Administration participates in the organization of trainings and further trainings related to cyber security, and in the coordination of educational and research activities related to cyberspace security and related resources.

Objectives of the Strategy

1. Strengthening trust in the digital environment

1.1 Strengthening professional cooperation

Only proper communication, knowledge-sharing and disciplined, coordinated defence, demonstrated in the event of an emergency will provide a solution to the new risks of cyberspace.

The tasks related to security issues and security incident response are of particular importance and represent an activity with appropriate responsibilities not only for information security professionals, but also for organizations operating electronic information systems, citizens and the media. For this reason, in accordance with international practice, it is necessary to establish a set of rules to ensure responsible procedure and communication (rules for responsible information sharing/„responsible disclosure") for the detection of and response to vulnerabilities and security incidents.

Identification of governmental and non-governmental actors performing tasks in the field of cyber security, precise definition of their functions and powers, and assessment of the competencies required to hold such positions. The functions and powers of organizations need to be reviewed and possible overlaps shall be identified.
The rules for cooperation and decision-making procedures shall be laid down for the cooperation between these organizations.
It is a priority to identify the areas where the necessary cooperation has not yet been developed. Establishing cooperation and starting dialogue shall be encouraged in these areas.

Measures:

1.) the effectiveness of cooperation in the forums set up already for the cooperation between governmental, market, educational and civil society actors shall be reviewed;
2.) a forum shall be ensured where there is an opportunity for social dialogue and wide-ranging information sharing, clarification of the role of ethical hackers and the relationship between society and ethical hackers;
3.) it shall be identified in which areas the existing cooperation shall be improved;
4.) the establishment of coordinated prevention, detection, mitigation and response mechanisms is essential to enable the information sharing and mutual assistance among public authorities, public and civil organizations and incident response centers;
5.) it is necessary to encourage 'Bug Bounty' programs launched by market- and public administration organizations, in which actors wishing to identify vulnerabilities in IT systems can draw the attention of the organizations to security errors within the framework of sound conditions and clear rules;
6.) cyber security exercises shall be conducted at specified intervals to further improve responsiveness and defence capabilities;
7.) there is a need to raise awareness of the shared responsibility of the public and private sectors.

1.2 Raising security awareness

In the digital world, it is becoming an increasingly important task and it is necessary to raise the awareness of citizens and various actors in society, in order to master the safe use of digital devices and services that become part of everyday life.

Hungary takes an active role in the work and organization of domestic and international awareness forums and campaigns related to cyber security in order to make the knowledge needed to use the digital world safely available to the widest possible target audience. (European Cyber Security Month campaign by the European Network and Information Security Agency in October each year, Safer Internet Program, Digital Immune Booster Program).

The specialized agencies – in cooperation with civil, economic and scientific actors – support the awareness-raising activities aimed at the safe use of cyberspace and at the promotion of practical knowledge in order that individual users, companies and organizations can use their digital devices and government and market electronic services in a confident and secure way.

Nowadays, there is a growing interest and attention from the media and also citizens about certain major vulnerabilities, security incidents and campaigns, it is therefore important to inform citizens and economic actors about the contact details of credible information and assistance forums.

It is an extremely important objective of Hungary for the monitoring of the digital world that authentic data is available to the Government on the knowledge, awareness, preparedness and threat situation of the population and economic actors.

Measures:

8.) the population and economic actors shall be aware where they can obtain authentic information and where they can turn for help;
9.) authentic, follow-up data shall be available on the knowledge, awareness, preparedness and threat situation of the population and economic actors;
10.) incentives shall be developed to increase the proportion of organizations with information security policies in the SME sector.

1.3 Law enforcement – development of cyber law enforcement

Crimes committed with the help of computer systems and against computers are now a special category of crime. The high number of offences committed and the extent of the damage caused thereby justify the need for law enforcement agencies to deal with the detection and identification of such cases as effectively as possible, together with preventive measures and the mitigation of damage, including discouraging the future infringing behaviour of the perpetrators.

Measures:

11.) law enforcement and judiciary shall improve the capacity to fight against cybercrime;
12.) competent bodies shall actively cooperate and share information in domestic and international organizations and cooperation against cybercrime.

1.4 Development of a professional management institutional system

The revision of the functions and powers and the rules of cooperation of the organizational system under the government's responsibility and the institutions involved in the performance of tasks (organizations performing tasks related to national security, national defence, law enforcement, disaster management and protection of critical institutions and facilities) shall be considered as a priority goal.

In order to stimulate the digital economy and bridge the digital divide, it is essential to support cyber security in the private sector with an institution which is able to transmit advanced cyber security solutions for the Hungarian corporate sector.

The EU Member States shall ensure to have well-functioning CSIRTs (technical units for averting computer security incidents) and sectoral network security emergency response teams that coordinate them by means possible (hereinafter referred to as 'CSIRT), which possess effective and compatible capabilities to deal with security incidents and risks, as well as meeting the essential requirements to ensure efficient cooperation at EU level. In this way, it is possible to cover the activities of privately owned critical or otherwise critical infrastructure and retail service providers, too (e.g. bank systems, healthcare). These units can be coordinated by a specialized institution in terms of information sharing towards further domestic and international information-sharing bodies.

Measures

13.) the specialized institutions (CSIRTs and authorities) necessary in the sectors covered by the NIS Directive shall be designated or established in accordance with the requirements of the Directive;
14.) an organizational system in line with the objectives set out in the Strategy shall be developed;
15.) the information security authority system for critical systems, facilities and services shall be improved, in order to enforce the requirements of the Directive across sectors;
16.) in addition to the incident response center under the Hungarian Cyber Security Act, a national incident response center shall be set up by examining the extension of existing cyber security regulations, in order to provide cyber security services available to a wider range of users of national cyberspace.

2. Protection of digital infrastructure

2.1 Quality management of IT developments

One of the basic conditions for effective defence against cyberattacks is that the development of quality assurance processes - already at the planning stage - in IT developments, as well as definition and measurement of cyber security criteria shall play a significant role.

In line with international industry standards, the proposed direction of development is that the basic quality requirements, including cyber security requirements for the new IT solution shall be defined at the planning stage in the case of IT development tasks. It is important that a competent responsible person is appointed to monitor compliance with security requirements, furthermore that an easily accessible, understandable methodology – sample documentation and measures and other support tools – are available which help the quality assurance process.

Measures:

17.) creating an easily accessible, understandable and usable information base;
18.) developing modular methodological guidelines for IT projects of different complexity;
19.) developing free aids for internal quality assurance;
20.) it is necessary to develop a Hungarian-English bilingual, free, modular, cyber security quality management knowledge base, accessible to anyone.

2.2 Increasing the security of government electronic services

The operation of the government and the administration shall be supported by such a stable and secure IT background that enables large-scale electronification of the internal public administration processes and administrative services for the population and businesses, as well as the widespread digitalization and public access to information and content of state interest.

It is key to both the reliable and stable operation of public administration and the provision of e-government services and electronic public services that government electronic information systems operate securely, are interoperable and serve all subsystems, institutions and users. This presupposes the systematic construction of a government IT background which is able to provide stable and reliable provision of traditional IT services and cloud-based solutions expected to spread to more and more areas, as well as application lease (ASP) and software services (SaaS) in terms of infrastructure, operation and development.

In case of electronic government services, it is of high importance that the security of networks, systems, processes and user data can be guaranteed at the highest possible level on the part of the public administration. One of the success criteria for e-government services is precisely to ensure that citizens and businesses can be sure that the systems are continuously operational and that services are available, and their data may only be seen for the purpose for which they have been

determined, only by the systems and persons authorized to do so.
The Hungarian Cyber Security Act and the decrees issued on the basis of the authorization of this Act provide an appropriate basis for the cyber defence and information security activities of state- and local government bodies. In parallel with the development of technology, state and municipal bodies shall keep pace with the constantly changing requirements of information security.

Measures:

21.) a stable and secure government IT background shall be established and operated reliably;
22.) maximum protection of critical information infrastructures, internal public administration systems and external applications, as well as user data appearing in them shall be ensured from the point of view of national security and the internal operation of public administration and the availability of electronic public administration services;
23.) maximum protection of networks, IT infrastructure and applications serving the internal systems and external services of the public administration shall be ensured;
24.) security oversight of all the subsystems covering the whole spectrum of public administration shall be ensured taking into account sectoral specificities;
25.) the fulfilment of IT developments receiving government support shall be linked to the implementation of security standards;
26.) a task plan shall be prepared for existing e-public services to achieve the required level of security;
27.) a common set of security requirements for IT developments shall be ensured and made mandatory by tightening up current practices and regulations.

2.3 Strengthening international cooperation

Hungary strives to guarantee the free and secure use of global cyberspace through its international relations system and organizational memberships; therefore, it seeks to establish cooperation based on mutual trust with all state and non-state actors of the global cyberspace with similar values to Hungary. Hungary intends to further strengthen its active role in regional and international cooperation at strategic and operational levels, particularly in cyber security cooperation within the European Union, NATO and the Central and Eastern European region, as well as in formulating international expectations and regulations within these organizations.

It is Hungary's priority interest to maintain its active cooperation in the cyber defence exercises and planning of the international community, thus enabling the continuous development of the international knowledge of our organizations, the establishment of a common operational protocol. It is especially important that the participation of domestic institutions and organizations are coordinated on international cooperation platforms. Also, the establishment of active participation in the cooperation and activities of the communities and centers for sectoral cooperation (ISACs, sectoral CSIRTs) is of high importance through the specialized organizations designated and established to pursue new purposes. Hungary aims to maintain an active role in the Euro-Atlantic and global communities and organizations of security incident response centers and to further deepen its active cooperation with European or international organizations working in certain areas of cyber security.

Measures:

28.) cooperation between the EU institutions as defined in the NIS Directive and the designated domestic institutions shall be initiated and strengthened;
29.) it is necessary to coordinate and enhance the international cooperation of domestic institutions;
30.) participation in international cyber security exercises shall be achieved in order to promote international cooperation and further develop international response and defence capabilities;
31.) Hungary shall emphasize its interests and values in both its bilateral and multilateral relations in the course of its external relations activities related to cyberspace.

2.4 Protection of essential services and critical infrastructures and their services

The protection of each of the critical infrastructures is a complex task, in the implementation of which, in addition to the various state bodies, economic actors shall also be involved.

A key objective is that the protection of designated critical systems and facilities, including operators of essential services and the operators of digital service providers shall place an increasing emphasis on the risk-proportionate and comprehensive protection of their network and information systems.

A risk assessment methodology shall be developed to enable the correlated collection of data to identify risks as accurately as possible, to make a dynamic estimate of the business impact produced by a possible outage of threatened services and to identify the measures with which the preparation for threats can be started in due time and their potential impact can be minimized as soon as possible.

The methodology shall include metrics that are mandatory for organizations to report annually and can also serve as a basis for the preparation of an annual national cyber security threat report.

Measures:

32.) a methodology of risk assessment and risk analysis at sectoral level shall be developed;
33.) cross-sectoral or sector-specific consensus recommendations and good practices shall be freely available regarding achieving security purposes;
34.) the establishment and maintenance of cooperation between public institutions and private sector actors shall be promoted based on mutual trust;
35.) a single package of services capable of complementing protection shall be made available to the widest possible range of critical infrastructure operators;
36.) targeted tendering opportunities for the development of effective prevention and rapid response capabilities in the field of physical and cyber security of critical systems,

facilities and services are necessary to be provided in order to improve the operation of operators, service providers, relevant authorities and incident response centers;

37.) it is necessary to raise information security awareness activities for operators of critical systems, facilities and services with the participation of relevant authorities and organizations;

38.) critical infrastructure operators shall be involved in national and international protection exercises.

2.5 Development of cyber defence, response and reaction capabilities

Due to the growing threat posed by cyberspace threats, the traditional detection-tracking behaviour is outdated. It is a fundamental national interest to ensure the concentrated availability of adequate cyber defence, response and reaction capabilities.

The aim is to develop and apply a wide range of passive and active tools for cyber defence, response and reaction capabilities on the existing base.

Passive cyber defence and response devices are the system elements built in the IT infrastructure, which perform the function of protection against threats and ensure the timely availability of information on threats. From among the passive tools, the tool or activity suitable for the detection of malicious infrastructures, monitoring and identification of attack activity is worth underlining from the point of view of development activity, which is essential to ensure that countermeasures are targeted.

Active measures are mainly human activities at the current technological level which mean continuous monitoring of threats against IT systems and varying degrees of response to them.

Measures:

39.) it is necessary to develop detection, processing (analysis) and investigation skills, which make it possible to identify, classify threats or attacks and establish the source thereof;

40.) due to the logical connections of these capabilities, governance and management based on uniform coordination at the sectoral level and on cross-sectoral coordination shall be established;

41.) a system for rapid situational awareness, evaluation and risk analysis needs to be developed;

42.) a toolkit for different levels of response to cyber threats needs to be developed;

43.) it shall be made possible for civilians and professionals working in the civil field to take part in national cyber defence in special cases.

3. Support for economic actors

3.1 Cooperation with research centers and strengthening the role of research and development

Cutting-edge capability in information technology security has developed in higher education institutions and other public research centers. In order that these capabilities continue to develop in Hungary and contribute to the nation's security purposes to a greater extent, it is important that there is a close cooperation between these workshops and the market and government actors. In order to strengthen state cyber security research and development, it is essential to establish strategic cooperation with higher education and scientific research workshops that present outstanding and internationally recognized results and to concentrate R&D tasks and resources to those research bases where the appropriate expertise and technical background is already ensured.

Measures:

44.) the training of engineers and researchers and the care of outstanding talents, as well as the conditions of their activities in Hungary shall be ensured;

45.) a research strategy in the field of cyber security needs to be established which aims to enhance the use of cyber security tools, software and products developed in Hungary for strengthening the cyber security of the Hungarian institutional system;

46.) related research and development topics shall be identified, and public incentive opportunities shall be created, including incentives for Hungarian start-up enterprises;

47.) the cyber security research-development-innovation strategy described in point 45 shall prioritize the topics of the European Union's R&D&I calls to be announced between 2021 and 2027, thereby helping innovative Hungarian organizations to participate in international projects as a matter of priority;

48.) the aim of economic diplomacy activities shall be to support the emergence of Hungarian service and development centers dealing with cyber security.

3.2 Supporting Hungarian digital innovation, developing support structures, performing coordination tasks

It is important to support domestic digital innovation with an information security focus which can be a major help in digitalization in Hungary, raising cyber security awareness and achieving data protection capabilities.

The government has already taken major steps (lasting currently, as well) to improve cyber security in businesses, these are the following in short:

1. At the end of 2015, the Economic Development and Innovation Operational Program (EDIOP) 3.2.1 Modern Enterprise Program (MEP) was launched in government-chamber cooperation, which gives a special focus to increasing IT security in companies in its activities of digital attitude and motivation affecting SMEs. Thus, within the project:

- this kind of attitude-forming materials are prepared and available on the program portal https://vallalkozzdigitalisan.hu/ (and will still be prepared),
- free chamber corporate ICT consultants across the country can help SMEs with information security, special emphasis is placed on this,
- IT security-focused events have been (and will be) organized,
- several business cyber security products and services are available at a discount,
- a detailed survey was also conducted on the cyber defence capabilities of businesses.

The program will continue until the spring of 2021.

2. In the EDIOP 3.2.2-8.2.4-16 combined tender, which was closely related to the MEP and has been available since spring 2017, supporting corporate IT developments[2], IT security-related hardware, software, consulting, service costs are eligible costs for applicant SMEs, since May 2018, also GDPR-related consulting and service activities can be integrated into the project (supported) in a targeted way.

In the continuation and expansion of government digital economic development programs, efforts shall be made to further increase IT security in the small and medium-sized enterprise sector. In addition to and related to these, it may also be necessary to launch education and training programs available to employees of enterprises in a subsidized form, beyond hardware and software elements, with security operation and security compliance, audit focus.

In addition to all this, beyond the resource-based support of the Hungarian small and medium-sized enterprise sector engaged in information and communication technologies, the solution is to develop a – direct or indirect (tax credit) – targeted support system which aims to financially strengthen the above-mentioned institutions with proven development and scientific activities and institutions considered to be protected from cyber security aspects.

Measures:

49.) development of state-subsidized cyber security service packages to help companies of the sector for procuring and implementing otherwise difficult-to-access, expensive solutions,

50.) education and training programs available to businesses in a subsidized form, beyond hardware and software elements, in the topic of security operation and security compliance, audit.

[2] *https://www.palyazat.gov.hu/ginop-3.2.2-8.2.4-16-vllalati-komplex-infokommunikcis-s-mobilfejlesztsek-felhalap-online-zleti-szolgltatsok-terjesztsnek-tmogatsa-1*

3.3 Creating a competitive domestic knowledge base

Hungary's goal is to promote cyber security education, training and research and development opportunities to create a competitive domestic knowledge base which meets both international practice and the needs of the domestic labour market.
Hungary's Digital Education Strategy sets out goals and measures - with the same motivation as above - for the development of digital competencies, awareness and information, as well as special fields of education and vocational training that promote information security.

Measures:

51.) the cyber security working group shall review current issues and make suggestions for addressing identified issues;
52.) the relevant educational and vocational qualifications shall provide a reliable basis in the labour market competition;
53.) it is necessary to create a common IT knowledge base accessible to all relevant actors;
54.) the opportunity shall be ensured that the wide range of society has access to information security training and qualifications at each level of competence;
55.) information security qualification requirements and training programs shall be developed regarding the personal staff of the operators of essential services;
56.) local and national cyber security exercises and competitions held with uniform quality standards shall receive support which aim to involve and increase the knowledge of young people in secondary and higher education.

List of actors involved in implementation under the current legislation and their strategic tasks

sector	activity	competent body	applicable law	tasks	contact, division of tasks
state bodies	**authority**	**Special Service for National Security, National Electronic Information Security Authority**	**Act L of 2013, Government Decree 187/2015 (VII.13.)**	a) the tasks of single point of contact is performed by: the National Electronic Information Security Authority [Articles 8 (3) and (4), 10 (3) of the NIS, Section 6 (1) i) of the Government Decree 187/2015] b) cooperates with the network of CSIRTs [Section 6 (1) g) of the Government Decree 187/2015] c) represents Hungary in international organizations responsible for the security of network and information systems [Section 6 (1) h) of the Government Decree 187/2015] d) within its competence, in the case of electronic information systems of operators of essential services or digital service providers identified in accordance with the NIS Directive, the data related to their compliance assessment and the results of the examination is sent to the European Commission, e) cooperates with the GovCERT f) sends the national strategy under the NIS Directive to the Commission g) informs the EEA Member States concerned about the security incident (with significant disruptive effect) h) consults and cooperates with law enforcement agencies and the Hungarian National Authority for Data Protection and Freedom of Information [Section 6 (1) j) to n) of the Government Decree 187/2015]	**Contact: -** with Hungarian bodies: the NDGDM and the authority receiving the notification reports to the National Cyber Security Center; - with the relevant authorities of the other Member States, the cooperation group and the network of CSIRTs

	incident response center	**Special Service for National Security, GovCERT**	**Act L of 2013, Government Decree 185/2015 (VII.13.)**	a) The tasks of CSIRT as incident response center are performed by: the Government Incident Response Center (GovCERT) [Articles 9 (1) and 24 (3) of the NIS] b) cooperates with the network of CSIRTs [Section 3 (1) h) of the Government Decree 185/2015] c) cooperates with the National Electronic Information Security Authority [Section 3 (1) j) of the Government Decree 185/2015] d) may request assistance from the EU Network and Information Security Agency for the further development of CSIRTs [paragraph (3) is added to Section 3 of the Government Decree 185/2015] e) participates in the activities of the network of CSIRTs, in relation to the electronic information systems falling within its competence, in which it represents the other incident response centers [Section 5 (4) e) of the Government Decree 185/2015] f) informs the other Member States concerned about the security incidents with a significant disruptive effect on the network and information systems of operators of essential services and digital service providers g) examines, on the basis of information provided by the incident response center concerned, the cross-border impact of security incidents with a significant disruptive effect on the services of operators of essential services and digital service providers [the following Section 5/A of the Government Decree 185/2015]	**Contact:** - with Hungarian bodies: the NDGDM and the authority receiving the notification reports to the National Cyber Security Center; - with the relevant authorities of the other Member States, the cooperation group and the network of CSIRTs

Critical infrastructures (Annex II of the NIS Directive)	**authority**	**NDGDM**	**Act L of 2013, Act CLXVI of 2012, Government Decree 187/2015 (VII.13.)**	a) Maintenance of a list of operators of essential services [Section 2/A (4) and (5) of the Hungarian CIP Act, Article 5 (1) of the NIS] b) Two-year review of the list of operators of essential services [Section 2/A (6) of the Hungarian CIP Act, Article 5 (5) of the NIS] c) Carrying out registry authority tasks related to designated critical systems (Section 5 of the Hungarian CIP Act) d) System of tasks related to the coordination of investigations (Section 8 of the Hungarian CIP Act) e) Carrying out information security authority activities in relation to the network and information systems of service providers designated as critical and, in the future, as an operator of essential services [Section 25 of the Government Decree 187/2015 (VII.13.), Article 8 (1) of the NIS] f) cooperation with the National Electronic Information Security Authority regarding its systems [Section 25 (5) of the Government Decree 187/2015 (VII.13.)]	**Contact:** - with sectoral designating authorities. Annex II of the NIS Directive, namely the registration authority for operators of essential services; - with operators of essential services determined in the sectors 1 to 6 of Annex II of the NIS Directive. Performs official tasks and security supervision in the case of electronic information systems of the infrastructures designated as European or national critical infrastructures with the exception of state and municipal, civilian intelligence, national defence and closed systems and bodies; - with the National Electronic Information Security Authority. Provides information and cooperates to fulfil the notification obligations set out in the NIS Directive.

	incident response center	**NDGDM, IT Security Incident Response Center**	**Act L of 2013, Act CLXVI of 2012, Government Decree 185/2015 (VII.13.)**	a) Operating an incident response center in relation to the network and information systems of service providers designated as critical and, in the future, as an operator of essential services [Sections 6 (3)-(4), 7 of the Government Decree 185/2015 (VII.13.), Article 9 (1) of the NIS] b) fulfilling the obligation to provide information to the body designated by the Government, i.e. the Center [Sections 5/A (1) of the Government Decree 185/2015 (VII.13.), Article 10 (3) of the NIS] c) is responsible for responding to security incidents, for which purpose it may request information from the bodies within its competence, d) performs dynamic risk and incident analyses and security incident scenarios, e) is responsible for information, early warning and coordination on risks and security incidents, f) participates, through the Center, in the activities of the EU Computer Emergency Response Team in respect of the electronic information systems within its competence g) shares information with the Center about its CSIRT's service, operational and interoperability capabilities h) provides information about the rules of procedure for security incident response, not detailed in law to the single point of contact i) informs the Center about the security incidents with a significant disruptive effect on the services of operators of essential services and digital service providers for the examination of the significance of cross-border effects [Sections 6 (3)-(3a) and 7 of the Government Decree 185/2015 (VII.13.), Article 9 (1) of the NIS]	**Contact:** - with sectoral designating authorities. - with operators of essential services determined in the sectors 1 to 6 of Annex II of the NIS Directive. Operates an incident response center with the exception of state and municipal electronic information systems, closed electronic information systems, critical systems and facilities operated by the National Security Service performing civilian intelligence and national defence - performs network security activities related to the protection of national critical systems and facilities; - with the Center. Informs it about the security incidents and cooperates in the incident response, as well as provides information and cooperates to perform the tasks related to security incidents prescribed by the NIS Directive. - cooperates with the Authority and, if necessary, the bodies concerned regarding the security incident response. The purpose of the contact is to cooperate for the fulfilment of the obligations set out in the NIS Directive.

sector	activity	competent body	applicable law	tasks	contact, division of tasks
Annex III of the NIS Directive (digital services)	**authority**	**NDGDM**		a) performing the information security authority activity of the network and information systems of the digital service providers [Sections 6/A to 6/D of the Hungarian Electronic Commerce Act, Article 16 (1) of the NIS, Article 8 (1) of the NIS]	**Contact** - with digital service providers, - with law enforcement agencies, - with the single point of contact, - with the competent sectoral authorities of other Member States, - with data protection authorities, - with representatives appointed by digital service providers not established in the European Union, offering their services within the European Union;
				b) keeping a record,	
				c) contact with bodies specified by law	
				d) assigning a single point of contact to forward the security incident report to the other Member States concerned,	
				e) monitoring the application of the NIS Directive,	
				f) informing the single point of contact about the notified security incidents,	
				g) informing the public about security incidents,	
				h) an obligation of digital service providers to inform the public,	
				i) participation in awareness and information campaigns,	
				j) carrying out official authority monitoring,	
				k) starting an official authority proceeding for the investigation of security incidents	
				[Section 4 of the Government Decree 410/2017 (XII.15.)]	
	incident response center	**NDGDM**		a) performing the incident response activity regarding the network and information systems of the digital service providers [Sections 615/CA-6/D (2) of the Hungarian Electronic Commerce Act, Article 16 (1) of the NIS, Article 8 (1) of the NIS]	**Contact:** - with digital service providers, - with participants in the government information technology, network security and security incident response system,

				b) keeping a record of security incidents without personal data, c) providing professional support in security incidents response to persons concerned, d) performing alert, information and awareness tasks,	- with the Center. The purpose of communication is to effectively investigate and respond to security incidents, to perform tasks related to security incidents as prescribed by the NIS Directive.
				e) responsible for providing regular information about vulnerabilities and threats and proposed security measures,	
				g) may issue non-binding opinions and recommendations,	
				h) may hold a briefing on the security incident response, and may participate in the awareness program of the institutions responsible for raising awareness to information security,	
				i) cooperates with government information technology, network security, and security incident response system participants,	
				j) performs the tasks specified in Section 6 (3a) to (3e) of the Government Decree 185/2015. (VII.13.)	
				k) performs tasks related to the investigation of security incidents of digital service providers	
				[Section 2 of the Government Decree 410/2017 (XII.15.)]	
national defence sector	**authority**	**Director-General of the Military National Security Service**	**Act L of 2013, Government Decree 187/2015. (VII.13.)**	performing the information security authority activity of the information systems within its competence	**Contact:** - with the bodies within its competence

	incident response center	**Military National Security Service**	**Act L of 2013, Government Decree 185/2015. (VII.13.)**	performing the information security authority activity of the information systems within its competence	**Contact:** - with the bodies within its competence
National security service for civilian intelligence	**authority**	**Director-General of the Intelligence Bureau**	**Act L of 2013, Government Decree 187/2015. (VII.13.)**	performing the information security authority activity of the information systems within its competence	**Contact:**
	incident response center	**IntCERT**	**Act L of 2013, Government Decree 185/2015. (VII.13.)**	performing the information security authority activity of the information systems within its competence	**Contact:**