Hadtudományi Szemle
13. évfolyam (2020) 2. szám 35–46. • DOI: 10.32563/hsz.2020.2.4

János Gerevich[1] – Imre Négyesi[2]

Network and Information Security of Cloud Computing Services

A felhő alapú szolgáltatások hálózat- és információbiztonsága

Abstract

The security of network and information systems has become a critical issue for both the public and private sectors in the last decade. This article reviews the current EU directive in this area, looking for safety and reliability requirements. Next, we get an overview of the different models of cloud computing services. Finally, the relationship between the identified security and reliability requirements and the cloud computing service models will be described.

Keywords: *cloud computing, security, reliability, automation, development*

Absztrakt

A hálózati és információs rendszerek biztonsága az elmúlt évtizedben kritikus kérdéssé vált az állami- és a magánszektor számára is. Ebben a cikkben áttekintjük a területet jelenleg szabályozó hatályos EU-irányelvet biztonsági és megbízhatósági követelmények után kutatva. Ezt követően átfogó képet kapunk a felhő alapú informatikai szolgáltatások különböző típusairól. A dolgozat végén a feltárt biztonsági és megbízhatósági követelmények és a felhő alapú szolgáltatástípusok közötti összefüggések kerülnek bemutatásra.

Kulcsszavak: *felhő alapú számítás, biztonság, megbízhatóság, automatizálás, fejlesztés*

[1] Nemzeti Közszolgálati Egyetem, Hadtudományi Doktori Iskola, doktorandusz – University of Public Service, Doctoral School of Military Sciences, PhD student, e-mail: gerevich.janos@agilexpert.hu, ORCID: https://orcid.org/0000-0001-7236-4514

[2] Nemzeti Közszolgálati Egyetem, egyetemi docens – University of Public Service, Associate Professor, e-mail: negyesi.imre@uni-nke.hu, ORCID: https://orcid.org/0000-0003-1144-1912

1. Introduction

Cyberspace is a virtual environment where we can do more and more activities while the number of services available here is continuously growing. Internet-based services are continually expanding, including online shopping, social networking, banking, healthcare, e-government and defence systems. At the same time, we should not forget the various radio- and NFC[3]-based electronic solutions which are also spreading and form part of cyberspace. As a result of technological advancement, the fight against cybercrime and cyber-security is a high priority worldwide as well as in Hungary today. Attacks are aiming at stealing, manipulating, destroying information and creating fake news in the cyberspace. Very often the targets of cyber-attacks are individuals. However, neither the private, nor the public sector including the armed forces can feel secured. The IT systems of defence sector can also be the target of cybercrime, for instance blackmailing. It is also possible that a military organisation which is responsible for the defence activities of a country confronts a hacker group linked to the armed forces of another country. In addition to external risks, the vulnerabilities of hardware and software environments should be highlighted. They might have severe internal risks and require appropriate methods to address them.

If we are looking for a modern approach to addressing the risks outlined, an appropriate start would be to examine the existing regulations of the EU. The last document in this category is the Directive of the European Parliament and the Council concerning measures for a high common level of security of network and information systems across the Union[4] (NIS Directive). We have already seen extensive regulation on the protection of critical infrastructures of the EU in the previous decades. Such measures include rules on the protection of critical infrastructures. The action plan of the European Critical Infrastructure (ECI) protection was already published in a separate document[5] by the European Commission in 2006. Subsequently, the identification and designation of European critical infrastructures were regulated two years later by a European Council directive.[6] The EU has recognised the importance of critical information infrastructures and set further goals in 2011 to achieve global cyber-security. Cybersecurity Strategy of the European Union (Cybersecurity Strategy) with many identified cyber-challenges[7] was published in 2013. One of the difficulties discussed was the question of network and information security. The Cybersecurity Strategy indicated[8] an EU level directive for the protection of the essential services. Finally, in 2016 the EU introduced the NIS Directive, which is the extension of the

[3] NFC – Near-field communication. The term covers a set of standards describing communication between smartphones and similar (usually mobile) devices.

[4] 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.

[5] Communication from the Commission on a European Programme for Critical Infrastructure Protection 786 final, COM(2006).

[6] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[7] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security,' 163 final, COM(2011).

[8] Ibid. 2.3.

critical infrastructure protection regulations to the operators of essential network and information systems.

2. Network and Information Security Nowadays

Identifying critical systems, analysing risks, creating security plans with disaster recovery capabilities are complex tasks. It is most important to use appropriate methods and technologies during the design and development phase of an information system that provides an essential service or a part of a critical infrastructure. The European Union published the NIS Directive on July 6th, 2016. This document contains 75 points altogether with arguments, insights and steps that need to be taken to address the problem at the appropriate level. The purpose of the following analysis is to identify requirements that can be interpreted from software technology perspective and covered by standard software development methods.

One of the main purposes for the regulation is improving the security and reliability of information systems in the internal market.[9] If we look at security from the perspectives of design, development and operation, security matters are more in the scope of the operation. However, in terms of reliability the design and development scope seems to be more important. A requirement has already been identified as the following: strive for reliability during design and development. Nowadays, the number of security incidents is still increasing regardless of whether a malicious human intention is in the background or a technical error is causing the service outage.[10] These security incidents can be transboundary, so it is crucial to develop methods that have sufficient reliability and security parameters in the era of cloud computing. As we can see, there is a need for new technologies and methods which can increase the security and reliability of network and information systems. Only strategic cooperation between Member States could guarantee[11] the success of the new techniques if they help the development and later apply the standards. The level of preparedness of the Member States regarding cyber-security is unequal and there is a need to uniform minimum requirements at EU level for operators of essential services and digital service providers. The outlined requirements have to be applied to network operators and information system providers.[12] In both cases, detection of security incidents, detection and correction of logical errors requires standard procedures and methods. During the analysis of the basics, we succeeded in identifying four requirements in software technology about the new methods to be developed as follows.

1. *Strive for reliability during design and development.*
2. *In the cloud-based operating environment the services must be developed with the sufficient reliability and security parameters.*
3. *The goal to be achieved is applying high-level security and reliability standards.*
4. *Detection of security incidents, revealing and correction of logical errors has to be done by standard procedures and methods.*

[9] NIS Directive (1).

[10] Ibid. (2)–(3).

[11] Ibid. (4).

[12] Ibid. (5)–(6).

In this section, we meet sectors that are affected by the NIS Directive. There are some sectors where information security has already been properly regulated. Thus, there are also sectors where the security environment is still being formed. The water transport sector must fully apply the NIS Directive.[13] In the sector of banking and financial market the infrastructure regulations in many cases are stricter than what the NIS Directive sets out, which requires at most legal harmonisation for this sector.[14] For online marketplaces and online search engines, the NIS Directive regulates the original providers, not the operator of the mediator services.[15] The document refers to cloud computing providers in a separated point, which is also an area to be regulated.[16] While cloud-based services have both network and information technology risks, Internet exchange points (IXPs) are the riskiest regarding disruption of technically and organisationally separate networks.[17] There is another industry requirement for public administrations in the enforcement considerations: 'The directive applies only to those public administrations which are operators of essential services.'[18] Cloud computing technology has particular importance in all sectors because in all cases where we are talking about just virtual computing capabilities, there is the chance to build private cloud services or contract with third-party cloud providers.

For security and reliability reasons, we should also consider security incidents for organisations that are not operators of essential services but have IT systems. For all sectors, risk management includes the security of stored,[19] transmitted[20] and processed[21] data. In many cases operators of essential services are using other digital services during their activities. Digital service providers are not subject to the NIS Directive but must provide a level of security that is proportionate with the level of service they offer and ensures uninterrupted operation.[22] Hardware manufacturers and software developers play a particularly important role in the improvement of the security of network and information systems because their solutions can enhance the quality of the essential services.[23] 'Technical and organisational measures imposed on operators of essential services and digital service providers should not require a particular commercial information and communications technology product to be designed, developed or manufactured in a particular manner.'[24] So it is not allowed to specify requirements for the production of the hardware, network and software products at the legislative level. Still, recommendations can be made for their production – in our view, we can define the sufficient recommendations for the software development, but we will discuss this later.

[13] Ibid. (10)–(11).
[14] Ibid. (12)–(14).
[15] Ibid. (15)–(16).
[16] Ibid. (17).
[17] Ibid. (18).
[18] Ibid. (45).
[19] Security of stored data is mainly related to hardware (HW) and software (SW) issues.
[20] Security of transmitted data is mainly related to hardware (HW) and network (Net) issues.
[21] Security of processed data is mainly related to software (SW) and network (Net) issues.
[22] NIS Directive (47)–(49).
[23] Ibid. (50).
[24] Ibid. (51).

There are security and reporting obligations for both operators of essential services and digital service providers, but the costs of security measures should be proportionate with the risks. Governmental organisations may request additional security measures by contract.[25] Outsourcing is possible for public-sector bodies. However, in this case, the public-sector body – not the service provider – must comply with the legal requirements for the particular service.[26] It is also possible to make appropriate recommendations for the operating environment of essential services. In the case of software-based services automation is required that can increase operational security and reliability. Table 1 shows the security exposure for some sectors based on software/hardware/network factors from 1 to 5. The values in the table are subjective metrics. They are intended to illustrate the diversity between sectors. Besides the subjective values we can see that different scopes of data security may be critical for different sectors. We can see that the presence of software components (SW) is critical for two territories. The new standards should cover data handling and data storage related processes. In these cases, software technology and software development methods play a significant role. After the previous analysis, we are looking for requirements that can be organically integrated into software development technologies and therefore, they could become requirements of the new standards. In the NIS Directive we can find several goals which can be interpreted in a way concerning software development.

Table 1. *Data operations and some IT-exposed sectors from security perspective*

Sector	SW	HW	Net	Data storage security (HW/SW)	Communication security (HW/Net)	Data handling security (SW/Net)
Water transport	3	5	5		Critical	
Banking	5	5	5	Critical	Critical	Critical
Cloud computing	5	3	5			Critical
IXP	1	5	5		Critical	
Government	5	3	5			Critical

Source: Compiled by the author

The primary purpose of the NIS Directive is to develop appropriate methods from physical protection to information security, taking into account 'physical and environmental security, security of supplies, access control to network and integrity of network and information systems'.[27] This requirement implies the creation of security plans through controlled methods and processes to ensure security in the above listed scopes. For each scope the following capabilities shall be developed on a sector-by-sector basis: 'incident-handling management, incident detection capability, incident reporting and communication'.[28] The cyberspace with the essential services also requires adequate routines to handle, detect and report security incidents with appropriate information. From this perspective the 'service continuity strategy and contingency plans, disaster

[25] Ibid. (52)–(54).
[26] Ibid. (56).
[27] Ibid. (69).
[28] Ibid. (69).

recovery capabilities'[29] are indispensable for the sustenance of network and information systems. Continuous maintenance of essential services requires such plans and capabilities that it can be a realistic goal to maintain the service after a security incident. Reliable design methods to manage security risks are needed to achieve this goal. With these considerations in mind, network and information systems have particular importance in terms of operation, 'monitoring and logging requirements, conducting emergency plans, testing network and information systems, security assessments and compliance monitoring'.[30] To foster the proper reaction capabilities, it is necessary to develop system management solutions that can immediately detect the changes in the essential services – especially the security incidents. During the analysis new requirements have been identified for the design and operation of the essential services to enhance their security and reliability. The newly identified needs are listed below.

5. *Regulated methods and processes must support security plans creation.*
6. *The security incidents have to be manageable, detectable and reportable with appropriate information.*
7. *Design methods are required that can guarantee the reliability of the essential services and handle security aspects.*
8. *The correspondent reaction capability can be fostered by specialised system management solutions that can immediately detect the changes in essential services and alert potential security incidents.*

The NIS Directive does not contain further methodological and technological considerations, but it is also worth briefly reviewing the related legal context and the implementation process. Operators of essential services and digital service providers are the subject of the NIS Directive. Thus, the providers of public communication networks or publicly available electronic communication services are regulated by Directive 2002/21/EC of the European Parliament and of the Council[31] and not managed by the NIS Directive. Trust service providers have to follow the special security requirements laid down in the Regulation (EU) No 910/2014[32] of the European Parliament and of the Council.[33] The NIS Directive provides the possibility for the Member States to extend the original regulations and introduce new sector-specific rules. In these exceptional cases, the Commission must be informed about the *leges speciales*; besides, Member States could require other additional security standards.[34] In parallel with the possibility of special regulations, Member States should endeavour to create safety standards based on the requirements and the experiences. ENISA[35]

[29] Ibid. (69).

[30] Ibid. (69).

[31] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

[32] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[33] NIS Directive (7).

[34] Ibid. (8)–(9); (57)–(65).

[35] ENISA – European Network and Information Security Agency. From 17 April 2019 European Union Agency for Cybersecurity.

should coordinate this standardisation activity.[36] Organisations not covered by the NIS Directive should also be able to report security incidents voluntarily.[37] In order to implement the NIS Directive, the Commission must be given implementing powers to act to achieve its objectives.[38] After the brief exploration of the legal environment, it can be stated that the document deals with the establishment of safety standards and the encouragement of entities in the public and private sectors both at EU and Member State level.

By analogy with the designation procedure of critical infrastructures, it is up to the Member States to decide about a company if it is an operator of essential service or not. The NIS Directive provides the classification rules sector-by-sector, and the list of sectors is updated periodically due to changes in the entities of the sectors. Sectoral reviews should be carried out regularly in each Member State due to economic and social impacts. The Member State should review the services that are part of the list of essential services. When assessing the result of a security incident, Member States should also take into account cross-sector and sector-specific factors. On the Member State level, the list of essential services should include all the identified essential services. If an operator of essential service provides its service in more than one Member State, the concerned entities should cooperate in the risk management. Member States should also take measures regarding the obligations to regulate the security of the network and information systems and should designate the relevant service providers based on compliance. Subsequently, the size and market share of the identified actors shall be communicated to the European Union anonymously sector-by-sector. In order to manage these tasks, each Member State should publish its national strategy of security of network and information systems.[39] Additionally, each Member State should designate a single national point of contact responsible for coordinating issues related to cross-border cooperation.[40]

The ENISA and CSIRT[41] network within the European Union are responsible for the implementation of the NIS Directive. Anonymous reports shall be prepared by the single point of contact of the Member State concerned and submitted to the Commission. The report shall include the nature, the type, severity and duration of the security incidents. Adequate capabilities are needed at Member State level to prevent, detect, handle and mitigate security incidents.[42] Success requires both cross-sectoral and international cooperation. In the private sector, the operators of essential services should be encouraged for collaboration and dialogue to improve the security of network and information systems. ENISA coordinates this process, the use of existing resources, capacity building and knowledge building are the most important tasks.[43] The information sharing on security incidents should be international, complying with the appropriate rules, through a central website (URL: https://cert.europa.eu)

[36] NIS Directive (66).

[37] Ibid. (67).

[38] Ibid. (68).

[39] Ibid. (19)–(30).

[40] Ibid. (31).

[41] CSIRT – Computer Security Emergency Response Team.

[42] NIS Directive (33).

[43] Ibid. (34)–(38).

on security incidents in the Union.[44] CyberEurope exercises can help the Member States to test their preparedness and interoperability and develop an appropriate risk management culture.[45] With this collaboration, the EU can significantly reduce network-based communication risks, while data handling and data storage issues remain open, especially for cloud services.

The legal environment and the identification process of essential services do not contain other technology requirements. However, we can state that the eight requirements identified during the analysis are the goals of the needed standards. The fostered standards in the design, development and operation phases should cover data management and communication issues at the forefront. With this approach, the security and the reliability of future systems can be increased. The more in-depth understanding of security risks requires a closer examination of different cloud computing models.

3. The Security and the Cloud Computing Service Models

The security of critical infrastructures is vital for our society. An excellent example of such a system is the power plants and the physical pieces of the electricity grid together. Nowadays, the physically existing critical systems are mostly using software components, even though they are not information systems at all. Of course, the electronic devices involved in these infrastructures are controlled by software drivers, so physically existing critical infrastructures can have software components. The relationship between software and information systems needs to be clarified from a software technology perspective at this point. There are different uses of software applications. For example, PLC[46] driver programs are commonly used in the industry. However, both the printer driver and the ERP[47] system are special software applications. For the drivers of physical devices, we are usually talking about 'low-level' controllers as a particular type of software.

Previously, a negligible proportion of electronic devices had network connectivity, but in the new millennium a significant portion of the newly manufactured digital 'gadgets' already have network connectivity. This capability and the widespread use of the Internet have made it possible for IoT[48] to become the dominant segment of cyberspace today. The ability to connect to the network has emerged in industrial applications due to central monitoring and control. In everyday life, communication between smart electronics and mobile devices has become widespread. Parallel with the development of these solutions, threats and potential vulnerabilities have emerged from drivers, software updates. The connections between industrial machines, smart devices and their controllers can be already considered as a kind of distributed information system. Cases of traditional information systems are in the following

[44] Ibid. (39)–(41).

[45] Ibid. (42)–(44).

[46] PLC – programmable logical controller.

[47] ERP – enterprise resource planning.

[48] IoT – Internet of Things.

sectors: telecommunication, banking, healthcare, transportation and government. In these cases, the business process is entirely software-based. Therefore, it is possible to create a cloud-based development and operational environment. With the spread of cloud-based technology, different service models have appeared. The difference between service models is the proportion of services provided.[49] The most basic service model is IaaS,[50] in which case the number of components managed and offered by the provider is the smallest. The service provider offers physical devices, servers, storage, network components and the user controls the software. If an essential service is IaaS, security and reliability must be standing on two pillars. On the one hand, the use of safe physical devices can ensure reliability. On the other hand, geo-redundant data storage and backup systems are required to ensure security. Security and reliability for IaaS is mostly not an issue of software technology but an issue of infrastructure design.

The next model of the offered services is the PaaS[51] which is based on the services provided by physical devices. The PaaS model assumes the presence of some basic software in the cloud that enables the production of custom software development. The service provider offers these out-of-the-box software components. Such software components are operating systems, web servers, database servers and programming languages. In this environment, security and reliability issues are related to software development processes. In the case of PaaS model, the reliability of the software components, development tools and programming languages must be verified during the software development workflow. So, the methods and tools used in software development can improve the reliability of the services provided in the PaaS model. The tools for automated testing, code review and continuous integration provide the preconditions of the better software quality.

If the cloud provider offers a software-based service, we are talking about the SaaS[52] model. In this model the user of the service is using the graphical or technical interface of the provided software. The provider is responsible for all technical issues, including the development and operation of the software. Very often the systems in the corporate governance, banking and public sector are available for their customers in this model. Usually, the SaaS model means an outsourced capability where the customer receives a software-based service in addition to a regular fee. Loss of physical networks and hardware damage can have critical consequences for this type of model, but software risks, malfunctions, information theft, system downtime are at least as much of threat.

The issue of security and reliability is a particularly exciting field in the SaaS model. In addition to the security issues of the IaaS and PaaS models discussed earlier, there are also software technology issues with the software-based services. Such a security question is whether unauthorised penetration or unauthorised data extraction is adequately protected. Does the service provider have sufficient and adequate diagnostic data during operation? Are the operational processes standardised? In case of a security incident, is it possible to create the correct entries into the technical log

[49] András Tóth, 'A felhőinformatika alapjai,' *Hírvillám (Signal Badge)* 2, no 1 (2011), 88–89.

[50] IaaS – Infrastructure as a Service.

[51] PaaS – Platform as a Service.

[52] SaaS – Software as a Service.

files? From the reliability perspective, the following questions may arise. Are sensitive data (e.g. personal data, financial data) modelled correctly? Is it possible to restrict the retrieval of sensitive data in a controlled way? Are anonymous data, encrypted data available to support debugging? Do the upgrades remove previous functionality? Does the system speed slow down after version upgrades? Is the system free of unexpected error messages? Summarising the above questions into a single item, is the software-based service being developed and operated in a standardised way?

The CSIRT network controlled by ENISA protects against malware, spyware and viruses, actively covering the IaaS model and partially covering the PaaS, SaaS layers above it. To specify different platforms, standardised methods and technologies to support software development and operation is a forward-looking task. The challenge of software technology is to increase the security and reliability for PaaS and SaaS cloud computing models available in cyberspace. Beyond quality indicators, the goal should be to develop a rapid response capability in the event of security incidents or threats.

Figure 1 illustrates the required methods to enhance the security and reliability factors for each layer in the service model triangle. From bottom to top, the significance ratio of hardware and network design is decreasing. While in the same direction, the proportion of software technology importance is increasing from the security perspective. In each layer of the triangle the recommended methods are visible for the IaaS, PaaS and SaaS models. As we can see, the methodology strongly coupled with technology can improve reliability and security in the PaaS and the SaaS layers. Nevertheless, the PaaS and the IaaS layers quality factors can be enhanced by trusted devices and software components based on fault-tolerant physical infrastructure.

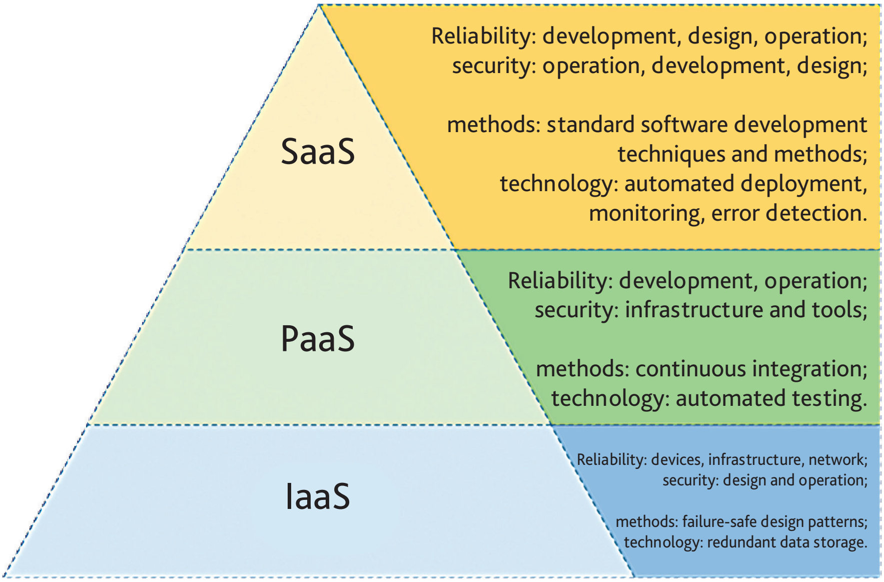
SaaS
Reliability: development, design, operation;
security: operation, development, design;
methods: standard software development techniques and methods;
technology: automated deployment, monitoring, error detection.
PaaS
Reliability: development, operation;
security: infrastructure and tools;
methods: continuous integration;
technology: automated testing.
IaaS
Reliability: devices, infrastructure, network;
security: design and operation;
methods: failure-safe design patterns;
technology: redundant data storage.

Figure 1. *Cloud computing service triangle and recommended security methods*

Source: Compiled by the author

In the SaaS model reliability and security are related to the design, development and operation of the software. For reliability, the software development related activities are more critical, while in the field of security the operating environment is more important. The improvement of quality indicators can be achieved by automated methods, where the cooperation of the design–development–operation areas is combined. Automated installation processes, monitoring and error detection can provide the technical background for security and reliability. In the case of methods, standard software development methods can be used to produce systems of appropriate quality for the operating environment.

Such software development-related activities are usually done in the PaaS model. The continuous integration method can help the developers to integrate the new features into the software continually with appropriate feedback. This method is supported by automated testing tools. If the requirements are specified correctly, automated tests can hold and cover them as a shell of the production system. This way, the top two layers of the cloud triangle can be managed together to produce better quality software.

The requirement analysis techniques, software development methods and operation environment must be involved during the preparation of new software technology standards. If the new standards are developed and widely used, our information systems will not only be more secure on the hardware and network side, but also the software technology side. Both the physical and the virtual aspects must be managed to achieve a higher level of security of network and information systems.

4. Conclusion

Over the last fifteen years the European Union has set out its objectives for the protection of European Critical Infrastructures and developed related regulatory mechanisms. Measures to protect essential services are vital to enhancing the security of our digital society. During our analysis, we learned about the NIS Directive, which defines the protection of critical infrastructures in cyberspace, with other words, the protection of essential services as a part of the Cybersecurity Strategy.

The process of identification, designation and management of essential services is well regulated, similar to measures for critical infrastructures. The CSIRT network adequately supports vulnerability detection for widely used softwares in the Member States and prevention of security incidents on computer networks. Sufficient alarm and response procedures are available for security incident mitigation. We have seen that software technology needs to address security issues of data transmission and data storage need to develop new standards. In the analysis we have identified the security risks of cloud-based service models bearing in mind the security and reliability issues mentioned above.

The framework for the EU has adequately supported the mitigation of threats to computer networks and physical IT infrastructure. With the terminology of cloud services, the NIS Directive adequately supports the IaaS model. For the PaaS and SaaS models, the process of software development and operation is only partially covered by the document. Both service models have the potential to improve the security and reliability indicators defined in the NIS Directive. The following eight requirements identified during the analysis may serve as a basis for the standards to be developed. The new rules as an integrated software technology approach must allow automation from the identification of requirements through software development to operation.

1. *Strive for reliability during design and development.*
2. *In the cloud-based operating environment the services must be developed with the sufficient reliability and security parameters.*
3. *The goal to be achieved is applying high-level security and reliability standards.*
4. *Detection of security incidents, revealing and correction of logical errors has to be done by standard procedures and methods.*
5. *Regulated methods and processes must support the creation of security plans.*
6. *The security incidents have to be manageable, detectable and reportable with appropriate information.*
7. *Design methods are required that can guarantee the reliability of the essential services and handle security aspects.*
8. *The correspondent reaction capability can be fostered by specialised system management solutions that can immediately detect the changes in essential services and alert potential security incidents.*

Bibliography

Communication from the Commission on a European Programme for Critical Infrastructure Protection 786 final, COM(2006), Brussels, 2006. 12. 12.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security' 163 final, COM(2011).

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

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.

Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Tóth, András: 'A felhőinformatika alapjai.' *Hírvillám (Signal Badge)* 2, no 1 (2011). 85–90. Available: www.comconf.hu/kiadvany/hirvillam_2evfolyam_1szam.pdf (02. 10. 2020.)