BIZTONSÁGPOLITIKA

HADTUDOMÁNYI SZEMLE

2017. X. évfolyam 4. szám

ANDRAS TOTH[1]

Future Information Security Threats to the Defense Sector [2]

A jövő információbiztonsági fenyegetései a védelmi szférában

Abstract

In the present article the author demonstrates some of the information security challenges facing to the defense sector nowadays. Based on the analysis of the information security forum, the most dangerous security threats have been identified according to the next year, and examining them the author has drawn conclusions on their features, possible defense and repair procedures, solutions. As a summarized conclusion, basic security settings and required tools have been defined that can contribute to the creation of a secure information system inside the defense sector and other environments.

Keywords: information security, cybersecurity, cyber attacks, security threats, malware, ransomware, crime-as-a-service, internet of things

Absztrakt

A szerző a publikációban bemutatja napjaink néhány információbiztonsági kihívását a védelmi szféra vonatkozásában. Az információbiztonsági fórum elemzéseit alapul véve megállapításra kerültek a jövő évben legveszélyesebb biztonsági fenyegetések, melyeket megvizsgálva a szerző következtetéseket vont le azok jellemzőire, esetleges védelmi és javítási eljárásaira, megoldásaira. Összegzett következtetésként meghatározásra kerültek azok az alap biztonsági beállítások és szükséges alkalmazások, melyek hozzájárulhatnak a védelmi szférában és egyéb környezetekben egy biztonságos információs rendszer kialakításához.

Kulcsszavak: információbiztonság, kiberbiztonság, kibertámadások, biztonsági fenyegetések, rosszindulatú programok, zsarolóprogramok, bűnözés-mint-szolgáltatás, dolgok internete

[1] Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, adjunktus - National University of Public Service, Faculty of Military Science and Officer Training, assistant professor, E-mail: toth.hir.andras@uni-nke.hu, ORCID: 0000-0001-6098-3262

[2] „ Supported BY the ÚNKP-17-4-IV-NKE-5 New National Excellence Program of the Ministry of Human Capacities"

INRODUCTION

In the last few years many international and regional organizations and relevant bodies and fora in Europe (the European Parliament, the Council, the ENISA[3], the EU Cybersecurity Agency etc.) provided different significant guidelines, frameworks, directives and legislations to support information security inside the European Union. But these organizations and individual specialists draw attention to the increasing of the number and impact of data breaches, due to the widespread use of smart devices (smartphones, tablets and laptops), smart homes, BYOD[4] concept and IoT[5] services. This is one of the main reasons why the European main bodies have started to develop new strategies and acts. According to these documents Hungary shall have to start to make its own new regulations in the topic of information security.

Information security, that meets the requirements of the above documents, can only be achieved if all actors are aware of the rules and procedures that affect security. When analyzing the security system risks, it can be clearly stated that the human factor is still the weakest link in the chain in most security systems.[6]

From the point of view of my research I emphasized the importance of the information society, the new types of fourth generation warfare, the national and international regulatory background and the expectations of our various alliance memberships, focusing to the defense sector. My research is in sync with NATO's and EU's strategies, tasks and activities, such as the research programs of the NATO Science and Technology Organization (NSTO), the European External Action Service (EEAS) and the European Defense Agency (EDA).[7]

[3] European Network and Information Security Agency – A centre of expertise for cyber security in Europe. The Agency is located in Greece with its seat in Heraklion Crete and an operational office in Athens. ENISA is actively contributing to a high level of network and information security (NIS) within the Union to the development of a culture of NIS in society and in order to raise awareness of NIS, thus contributing to proper functioning of the internal market. Source: https://www.enisa.europa.eu/about-enisa (downloaded: 10.11.2017.)

[4] Bring Your Own Device – It is an increasing trend toward employee-owned devices within a business. Smartphones are the most common example but employees also take their own tablets, laptops and USB drives into the workplace. Source: http://whatis.techtarget.com/definition/BYOD-bring-your-own-device (downloaded: 10.11.2017.)

[5] Internet of Things – The vast network of devices connected to the Internet, including smart phones and tablets and almost anything with a sensor on it – cars, machines in production plants, jet engines, oil drills, wearable devices, and more. These “things” collect and exchange data. Source: https://www.sap.com/trends/internet-of-things.html (downloaded: 10.11.2017.)

[6] Rajnai Zoltán: Információbiztonság Tudatosság, A XXII. fiatal műszakiak tudományos ülésszak előadásai, Proceedings of the XXII-th international scientific conference of young engineers, 2017, ISSN 2393 – 1280, pp 37-38.

[7] Boda József nb. vezérőrnagy, Boldizsár Gábor ezredes, Kovács László ezredes, Orosz Zoltán altábornagy, Padányi József dandártábornok, Resperger István ezredes, Szenes Zoltán ny. vezérezredes: Fókusz és együttműködés. A hadtudomány kutatási feladatai; Honvédségi Szemle 144. évf. 3. szám (2016/3.), p 4.

SECURITY THREATS IN INFORMATION ENVIRONMENT

2017 was one of the worse years according to data breaches, just think of the most significant ransomware attacks like WannaCry, Petya, Locky etc. According to a report from the Information Security Forum (ISF)[8] we can see, that 2018 will be a much worse year for the attacks. It says that these attacks will be far more expensive for organizations of all sizes. Not just traditional areas, such as network clean-up and customer notification, will account for some of these costs, but additional costs will arise from newer areas, such as litigation involving a growing number of parties. In this point of view, it will affect the defense sector as well, the angry customers, companies, industries will pressure the sector and the government to introduce tighter data protection legislation to strengthen information security regulation at strategic level.

The top five global security threats that businesses will face in 2018, according to the ISF are:

- Crime-as-a-service (CaaS) will expand available tools and services;
- Internet of Things (IoT) will further add unmanaged risks;
- the supply chain will remain the weakest link in risk management;
- regulation will add to the complexity of critical asset management;
- unmet board expectations will be exposed by major incidents.[9]

CRIME-AS-A-SERVICE

When we are reading the articles or forums according to the Deep Web[10] we can meet more and more often with the phrase as Crime as a service or Cybercrime as a service (CaaS). This service puts cybercriminal tools and services in the hands of a wider range of threat actors. Professional criminal or group of criminals develop advanced tools, kits and other packaged services which are then offered up for sale or rent to other criminals who are usually less experienced. It means that even the nontechnical individuals or groups can become a cybercriminal with minimal investment, and inexperienced actors can launch sophisticated cyber-attacks and scams as well. The most popular CaaS kits used by the attackers are:

- Phishing kit: These kits may come with pre-written form letters which imitate the language, format and logos of real organizations; fake web pages to solicit the vic-

[8] The Information Security Forum (ISF) is an independent, not-for-profit organisation. It is dedicated to investigating, clarifying and resolving key issues in information security and risk management, by developing best practice methodologies, processes and solutions that meet the business needs of its Members. Source: https://www.securityforum.org/about/ (downloaded: 10.11.2017.)

[9] Thor Olavsrud: 5 information security threats that will dominate 2018, Source: https://www.cio.com/article/3237784/security/5-information-security-threats-that-will-dominate-2018.html (downloaded: 11.11.2017.)

[10] The part of the World Wide Web that is not discoverable by means of standard search engines, including password-protected or dynamic pages and encrypted networks. Source: https://en.oxforddictionaries.com/definition/deep_web (downloaded: 11.11.2017.)

tim's information; "crimeware" that automates the theft of online credentials; spamming software and more.

- Exploit kit: It incorporates the abundance of software vulnerabilities into a ready-made hacking tool or set of tools that make it easier for a criminal to break into a company's network and/or infect it with malware.
- Malwares: They can be any form of malicious software, viruses, worms, keyloggers, nuisance programs, cryptoware, banking Trojans, remote access Trojans (RATs) and mobile malwares.
- Criminal phone banks: This is a service in which criminals can create their own call center operation to support a phishing email campaign, or to social engineer an office employee or impersonate a company official to fool a bank.
- DDoS-for-hire: The distributed denial-of-service (DDoS) attacks can knock out websites, customer portals, email service and network connectivity. Now it is not needed for the criminals to build up their own "botnet" containing thousands of infected computers in order to launch these attacks, but now all they have to do is rent a botnet service online.[11]

These attacks can affect a company's or organization's bottom line, either directly or indirectly, as manifested in:

- lost sales;
- payment, delivery, or transaction delays;
- unfulfilled orders;
- business process disruption;
- productivity losses;
- legal fines;
- regulatory penalties;
- damage to the company's brand and reputation.[12]

The main change can be according to CaaS in 2018 that because of above mentioned possibility, nontechnical individuals and troops can also buy or rent these services. It means that more and more cryptoware attacks can be executed in the future. The main difference will be that in the past the victims could be sure that when they ransomed their locked computers with money, the criminals unlocked their devices. But in the future, they cannot trust in it, because the attacker can be an inexperienced person without technical knowledge and he or she does not have the key, just rented a kit from the Deep Web. These attacks can result much greater financial damage, because the victims may even have to pay for service after the failed unlock.

[11] Larry Johnson: Crime-as-a-Service Could Be the Next Big Threat to Your Business, Source: https://www.entrepreneur.com/article/298727 (downloaded: 11.11.2017.)

[12] Cybercrime as a Service series: Ransomware as a Service, Source: https://documents.trendmicro.com/assets/resources/ransomware-as-a-service.pdf (downloaded: 11.11.2017.)

To avoid these, participants, staffs, workgroups and organizations at all level in defense sector shall pay attention to use malware detection services with anti-phishing support, website and network vulnerability scanning services and outbound firewalls. They shall have security technologies like: antispam at the Web and messaging gateways, web reputation, application control, content filtering, vulnerability shielding, mobile app reputation, intrusion prevention and host-based firewall protection. It is also necessary to make software updates ordinarily and backups regularly and important to do security awareness training for employees.[13]

INTERNET OF THINGS

The Internet of Things (IoT) refers to the connectivity of billions of network-enabled devices having diverse requirements, and combines tools with sensor capabilities and connectivity to the cloud and allows them to leverage artificial intelligence, machine learning, and big data analytics, sometimes dramatically increasing their capabilities. IoT undoubtedly affects all sectors including the defense sector and the critical infrastructures such as energy, communication or transportation sector.[14] The (IoT) is becoming broader and more encompassing, and almost every piece of electronic equipment with IP address is capturing data – from personal devices storing sensitive personal data (racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health, sexual life, or details of criminal offences) to industrial equipment holding important company information. This information can be compromised and can lead to data theft, loss of system control, catastrophic shutdown and safety issues and/or ransom situations for instance with the solutions mentioned in the former part of this paper. In 2018 this will become even more dangerous, because organizations are increasingly adopting IoT devices, and hackers and criminals look for ways to gain access to networks using unsecure IoT devices. It makes very easy for them that most IoT devices are not secure by design.

We can use more and more different tools at home as smart devices, not just our laptops, smart phones, it can be now a voice control platform, smart lighting, smart bulbs, smart camera, smart thermostat, smart lock, smart doorbell etc. These pieces of hardware use IP addresses and connect to a network which can be reached from external systems. Unfortunately, most of the users choose a cheap solution so they install devices without future support for security and safety patches, which help to turn them zombie bots[15]. It can

[13] Pándi Erik, Paráda István, Jobbágy Szabolcs: A hálózat aktív és passzív eszközeinek, protokolljainak sebezhetőségére épülő támadások, szolgálatok, HÍRVILLÁM = SIGNAL BADGE V:(1), 2014, pp. 171-175.

[14] Esmeralda Kadena, Andras Kerti: Security risks of Machine-to-Machine communications, HÍRVILLÁM = SIGNAL BADGE 13, 2017, pp. 105-111.

[15] A zombie (also known as a bot) is a computer that a remote attacker has accessed and set up to forward transmissions (including spam and viruses) to other computers on the Internet. The purpose is usually either financial gain or malice. Attackers typically exploit multiple computers to create a botnet, also known as a zombie army. Source:

cause issues in a relatively new solution what many companies are using today. This technology and policy is the bring your own device (BYOD)[16] which gives some benefits including allowing for more flexible work practices, greater productivity and savings on IT hardware. But it is a huge risk as well, because one unsecured device can compromise a business's entire network, resulting in data or financial theft. The employers have less control over the employees' devices, so they do not know how up-to-date software and apps are used on them, and how they use their devices at home. If they have smart home effected with viruses, malwares it can pose security threats to employers' businesses. Other risk can be that they do know who has still access to the computer at the owner's home. To protect the business and personal devices it is advised to use strong and separate password for the different accounts (users, emails…), always back-up the most important data, install the latest software and app updates and secure the BYOD tools (tablets, smart phones) with screen lock. It is important for companies and individuals to take the time to understand the security measures on their IoT devices to ensure that they are not putting themselves at risk.

According to the defense sector the IoT is a huge challenge in the following areas:

- infrastructure service, energy efficiency;
- building automation services;
- security systems (access, identification, intrusion protection, foreign objects detection, alarm, video monitoring);
- transport (smart cars, smart roads, communicating urban spaces, traffic optimization, traffic monitoring, route planning, p2p transport solutions, sharing economy);
- eHealth (elder people, sensory observation of chronic patients, body-worn and flat-based sensors, central databases, alert to the doctors, predictive medical methodology);
- agro-informatics (micro area sensory measurements, nutrient levels, temperature, humidity monitoring, regulation, automated production);
- environmental protection (large-scale research, observation, sensors on all tree trunks, protection of restricted areas).[17]

In Hungary, the government declared the Digital Success Programme Strategy 2.0 with the Government Decree No. 1456/2017. (VII.19.) in July 2017. In this document, the government laid down the directives to give the access possibility to the Internet for every citizen in Hungary, to develop a comprehensive digital infrastructure and for the digital transfor-

http://searchmidmarketsecurity.techtarget.com/definition/zombie (downloaded: 12.11.2017.)

[16] It is an alternative strategy allowing employees, business partners and other users to utilize a personally selected and purchased client device to execute enterprise applications and access data. Typically, it spans smartphones and tablets, but the strategy may also be used for PCs. Source: https://www.gartner.com/it-glossary/bring-your-own-device-byod (downloaded: 17.11.2017.)

[17] Informatikai, Távközlési és Elektronikai Vállalkozások Szövetsége (IVSZ): Előzetes Megvalósíthatósági Tanulmány „Az Internet of Things koordinált fejlesztése és alkalmazásának elterjesztése Magyarországon", 2015, pp. 16-21

mation of the whole Hungarian educational system. The main tasks in the near future in the strategy are the followings:

- digital infrastructures;
- digital competencies;
- digital economy;
- digital state and
- horizontal themes.[18]

In the horizontal themes, the government laid down the basics of the smart cities in Hungary. With the Digital Success Programme Strategy the citizens have the possibility to continuously develop themselves in the field of information technology. So, they can be smart citizen who could be the fund of a secured smart city which using information technology generally. In this case the citizens are not only able to safely use the advantages of the smart city but also would be able to innovate and improve the city itself.[19] To reach this aim it is necessary to pay attention to the security solutions in IoT environment. According to an IoT security analysis the necessary technologies to protect data on IoT environment are:

- IoT network security: Protecting and securing the network connecting IoT devices to back-end systems on the internet.
- IoT authentication: Providing the ability for users to authenticate an IoT device, including managing multiple users of a single device (such as a connected car), ranging from simple static password/pins to more robust authentication mechanisms such as two-factor authentication, digital certificates and biometrics.
- IoT encryption: Encrypting data at rest and in transit between IoT edge devices and back-end systems using standard cryptographic algorithms, helping maintain data integrity and preventing data sniffing by hackers.
- IoT *Public Key Infrastructure (PKI)*: Providing complete X.509[20] digital certificate and cryptographic key and life-cycle capabilities, including public/private key generation, distribution, management, and revocation.
- IoT security analytics: Collecting, aggregating, monitoring, and normalizing data from IoT devices and providing actionable reporting and alerting on specific activities or when activities fall outside established policies.
- IoT *Application Programming Interface (API)* security: Providing the ability to authenticate and authorize data movement between IoT devices, back-end systems, and applications using documented REST[21]-based APIs.

[18] A Digitális Jólét Program 2.0, 2017, pp. 35-134.

[19] Orbók Ákos: Challenges and risks in the smart cities, New Approaches to the National Security: 11th PhD Conference Proceedings, ISBN: 978-80-7231-455-3, p. 447

[20] The X.509 public key infrastructure (PKI) standard identifies the requirements for robust public key certificates. A certificate is a signed data structure that binds a public key to a person, computer, or organization. Source: https://msdn.microsoft.com/en-us/library/windows/desktop/bb540819(v=vs.85).aspx (downloaded: 17.11.2017.)

[21] Representational State Transfer

SUPPLY CHAIN

The supply chain is presented in every company and organization. We can make differences between cyber supply chains and "non-cyber" supply chains. The cyber suppliers provide the technical background and support such as hardware, software, network solutions, up-dates etc. The "non-cyber" suppliers deal with all the other orders what is coming from the company (furniture, stationery, food…) Every company and organization, in the defense sector as well, needs these suppliers so it is needed for them to share some information with third parties. When that information is shared, direct control is lost. That means an increased risk of compromise of that information's confidentiality, integrity or availability.[22] There can be different issues in the supply chain management, with which we cannot always plan ahead, but we must be calculated with them:

- trouble in production, procurement, warehousing, transportation, scheduling;
- lack or error of control;
- lack of information, unpredictability, unexpected events;
- unreliability, lack of capacity, force majeure;
- economic- or political events, accidents, natural disasters.

To avoid the security issues, it is not enough to focus on the confidentiality, integrity or availability of the shared information and the above-mentioned issues in the supply chain, the companies shall pay attention to organizational culture, to avoid bad standards, to update outdated security strategies, to colleagues and leaders who do not follow the rules. In a business relationship that permits reciprocal, but of course limited use of information systems, it is mandatory to have an agreement between the partners, and according to the ISO/IEC 27001 certification standard it must contain:

- the preparation and acceptance of the confidentiality agreement by both parties;
- regulation of physical access (authorization and withdrawal);
- establishing an appropriate system of eligibility (issuing and invalidating passwords, clarifying the scope of access);
- establishing rules for transmission and transfer of information (e.g. making copies, destroying issues ...);
- the responsibility of the subordinated partner for its employees (e.g. the transfer of the list of authorized persons, without the violate of protection of personal data);
- only providing the necessary and sufficient data / information to the partners;
- regulation of IT outsourcing (some of the organization's information processing tasks are provided by another organization and therefore have access to network elements, databases and software applications ...);
- eliminating the experience of adverse events during the cooperation, quantifying the costs of troubleshooting and clear determination of responsibilities;

[22] Megyeri Lajos, Farkas Tibor: Kockázatkezelés, tudomány vagy kuruzslás? HADMÉRNÖK 12:(3), 2017, pp. 201-207.

- conducting formal procedures where employees of one of the parties breach the agreements;
- in the case of the joint design of an information system, clear separation of IT tools used during development and day-to-day operation;
- transfer of software essential to the maintenance of a business relationship through regulated written agreements (e.g. by keeping in touch with banking systems);
- control of the security of e-commerce and e-mail functions focusing on the authenticity, confidentiality and integrity of business transaction data and messages.

Regulation

On May 25, 2018, the General Data Protection Regulation (GDPR) takes effect as the primary law governing the protection of the personal data of European Union (EU) citizens. Today, one of the key assets of a data handling organization is the personal data. Most of the organizations' data is personal data, which is not only the property of the organization which handling the personal data, but also the person to whom it relates. But the responsibility of the establishment of appropriate data security practices, data protection procedures and ensuring continued compliance with the relevant standards is belonging to the personal data handling organization. Data protection requires awareness of all actors involved in handling and it must be followed every participant involved in product development, technology processes, reporting, etc. To reach this, it is not enough to put in place rules, develop technological controls, logging and testing, it is also necessary that the corporate culture itself should also encourage the development and application of conscious data management practices.

At the defense sector, every member must understand how the personal data is being managed and protected inside his/her staff, organization and informational environment. The members of the sector must measure the currently managed data assets, and must identify which personal information is stored and used and what purpose and legal basis is used to handle it. To build up a well-prepared and well-secured environment it is necessary to take some important steps such as hire a Data Protection Officer (DPO)[23], create a data register, identify data classification, the top priorities and any risks or process that may be vulnerable for them. So, these additional resources likely increase compliance and data management costs, and to pull attention and investment away from other activities, and

[23] A Data Protection Officer (DPO) is an enterprise security leadership role required by the General Data Protection Regulation (GDPR). Data protection officers are responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements. Source: https://digitalguardian.com/blog/what-data-protection-officer-dpo-learn-about-new-role-required-gdpr-compliance (downloaded: 27.11.2017.)

they will bring about the complexity of critical asset management.[24] This complexity and focused attention to the GDPR can cause a possible security threats in organizations including the defense sector. To avoid it, it is necessary for the organizations' Chief Information Officer (CIO)[25], Chief Information Security Officer (CISO)[26] and DPO to share the resources and to pay due attention to all segments of information security.

UNMET BOARD EXPECTATIONS

Cybersecurity is rapidly becoming a standing agenda item in board meetings. Members are asking CISOs for better visibility into their organizations' risk postures, and it is necessary to have engaged conversations around cyber risks and ensure that these are integrated into the enterprise risk management (ERM) program. Boards shall pay special attention to where the CISO is positioned on the organizational chart, who controls the CISO's budget, and the extent to which security projects might have to be cut due to budget or, considering the current skills gap, staffing issues. If it is not organized well it may cause huge controversy between the board and CISO. Usually, at enterprises the board members are not experts in IT and information security so in many cases the board still doesn't perhaps know the right questions to be asking, and the CISO still doesn't perhaps understand how to talk to the board, or the business for that matter.

Nowadays in Hungary almost 2000 information security specialists are missing in the defense sector. It means that the boards in the sector have the same issues regarding the communication with CISOs, which can provide huge security difficulties inside the whole sector. To avoid these, the participants shall reach a common denominator. According to GDPR and other directives it will be mandatory to educate the board members to the basics of the information security, so it will be easier to speak the same language. But it is not enough, the CISOs also must pay attention to help the board to understand the current and finished projects and the spending on the security programs. When they have a good communication a lot of security incidents can be avoided.

[24] Jan Smets: General Data Protection Readiness – hands up if you're GDPR ready or not! Source: https://gdpr.report/news/2017/11/27/general-data-protection-readiness-hands-youre-gdpr-ready-not/ (downloaded: 27.11.2017.)

[25] Chief Information Officer (CIO) is an executive job title commonly given to the person at an enterprise in charge of information technology (IT) strategy and the computer systems required to support an enterprise's objectives and goals. Source: http://searchcio.techtarget.com/definition/CIO (downloaded: 27.11.2017.)

[26] A Chief Information Security Officer (CISO) is the executive-level manager who directs strategy, operations and the budget for the protection of the enterprise information assets and manages that program. Source: http://resources.infosecinstitute.com/job-titles/chief-information-security-officer-ciso/#gref (downloaded: 27.11.2017.)

CONCLUSIONS

More and more businesses are adopting new information technologies and policies what require more and more complicated information security requirements. After analizing the last few years' most common cyber attacks it is possible to indentify that the information security is going to be more complex and diversified. In 2018 there will be five main security threats according to Information Security Forum. They will influence the defense sector as well, so the members of the sector shall focus to avoid them to build up a safe information environment.

To reach this, orhanizations shall focus on security skills for upskilling the security teams and experts such as security tools expertise, security analysis, project management, incident response, automation/devops etc. The other mandatory way is to potect the devices and networks like using firewalls to secure connections, choosing the most secure settings for the devices and software, controlling the access to data and services, keeping them up to date and protecting them from viruses and other malware.

REFERENCES

1. Rajnai Zoltán: Információbiztonság Tudatosság, A XXII. fiatal műszakiak tudományos ülésszak előadásai, Proceedings of the XXII-th international scientific conference of young engineers, 2017, ISSN 2393 – 1280, pp. 37-42.
2. Boda József nb. vezérőrnagy, Boldizsár Gábor ezredes, Kovács László ezredes, Orosz Zoltán altábornagy, Padányi József dandártábornok, Resperger István ezredes, Szenes Zoltán ny. vezérezredes: Fókusz és együttműködés. A hadtudomány kutatási feladatai; Honvédségi Szemle 144. évf. 3. szám (2016/3.), pp. 3-20.
3. Thor Olavsrud: 5 information security threats that will dominate 2018, Source: https://www.cio.com/article/3237784/security/5-information-security-threats-that-will-dominate-2018.html (downloaded: 11.11.2017.)
4. Larry Johnson: Crime-as-a-Service Could Be the Next Big Threat to Your Business, Source: https://www.entrepreneur.com/article/298727 (downloaded: 11.11.2017.)
5. Cybercrime as a Service series: Ransomware as a Service, Source: https://documents.trendmicro.com/assets/resources/ransomware-as-a-service.pdf (downloaded: 11.11.2017.)
6. Pándi Erik, Paráda István, Jobbágy Szabolcs: A hálózat aktív és passzív eszközeinek, protokolljainak sebezhetőségére épülő támadások, szolgálatok, HÍRVILLÁM = SIGNAL BADGE V:(1), 2014, pp. 167-186.
7. Esmeralda Kadena, Andras Kerti: Security risks of Machine-to-Machine communications, HÍRVILLÁM = SIGNAL BADGE 13, 2017, pp. 95-114.
8. Informatikai, Távközlési és Elektronikai Vállalkozások Szövetsége (IVSZ): Előzetes Megvalósíthatósági Tanulmány „Az Internet of Things koordinált fejlesztése és alkalmazásának elterjesztése Magyarországon", 2015.

9. A Digitális Jólét Program 2.0, 2017.
10. Orbók Ákos: Challenges and risks in the smart cities, New Approaches to the National Security: 11th PhD Conference Proceedings, ISBN: 978-80-7231-455-3, pp. 442-448.
11. Megyeri Lajos, Farkas Tibor: Kockázatkezelés, tudomány vagy kuruzslás? HADMÉRNÖK 12:(3), 2017, pp. 198-209.
12. Jan Smets: General Data Protection Readiness – hands up if you're GDPR ready or not! Source: https://gdpr.report/news/2017/11/27/general-data-protection-readiness-hands-youre-gdpr-ready-not/ (downloaded: 27.11.2017.)