KOŠICKÁ BEZPEČNOSTNÁ REVUE

KOSICE SECURITY REVUE

Vol. 9, No. 2 (2019), p. 26 – 33

ISSN 1338-4880 (print ver.), ISSN 1338-6956 (online ver.)

Security of the European Union from the Point of View of Cyber Security Issues

Bezpečnosť Európskej únie z pohľadu riešenia problematiky kybernetickej bezpečnosti

Radoslav IVANČÍK[1]

[1] *Akadémia Policajného zboru v Bratislave, Sklabinská 1, 835 17 Bratislava*

The manuscript was received on 22. 10. 2019 and was accepted after revision for publication on 02. 12. 2019

Abstract:

The number of cyberattacks against public and private companies, as well as the extent of the damage caused by this type of crime, is increasing in recent years. Companies in the European Union, in direct connection with the increase in the number and the severity of cyberattacks, are spending more and more resources to secure their digital assets. Measures against widespread cybercrime activities bring so much cyber security spending that it is almost impossible to keep track of their height. Many companies hesitate to report disruptions, sufferings and damage they have suffered, as well as reporting the amount of money they are spending to increase their cyber security because of fears of losses that could result from damaging their reputation. The main aim of the article is, in the context of cyber security research, using relevant scientific research methods, to highlight the problems faced by organizations due to cyberattacks, while briefly highlighting some cyber security solutions related to European Union policies in this sector.

Keywords: *European Union, companies, cyberattacks, cybercrime, cyber space and cyber security.*

Abstrakt:

Počet kybernetických útokov vedených proti verejným i súkromným spoločnostiam, ako aj rozsah škôd spôsobených týmto druhom kriminality v ostatných rokoch rastie. Spoločnosti v Európskej únii v priamej súvislosti s rastom početnosti, ale aj závažnosti kybernetických útokov vynakladajú stále viac prostriedkov na zabezpečenie svojho digitálneho majetku. Opatrenia voči rozsiahlym aktivitám v oblasti kybernetickej kriminality prinášajú takú sumu výdavkov na zaistenie kybernetickej bezpečnosti, že je takmer nemožné presne sledovať ich výšku. Mnoho spoločností váha oznámiť narušenia, prieniky a škody, ktoré utrpeli, a rovnako tak uvádzať finančné čiastky,

ktoré vynakladajú na zvýšenie kybernetickej bezpečnosti, kvôli obavám zo strát, ktoré by im mohli vzniknúť z poškodenia ich dobrého mena. Cieľom článku je, v rámci výskumu kybernetickej bezpečnosti, s využitím relevantných metód skúmania, poukázať na problémy, ktorým čelia organizácie kvôli kybernetickým útokom, a zároveň stručne upozorniť na niektoré riešenia v oblasti kybernetickej ochrany, ktoré súvisia s politikami Európskej únie v tomto sektore.

Kľúčové slová: *Európska únia, spoločnosti, kybernetické útoky, kybernetická kriminalita, kyber-priestor a kybernetická bezpečnosť.*

Introduction

The sector of communication and information technologies is currently one of the fastest growing areas of society. The development of the Internet and modern computer technologies is not only reflected in the private sphere but is increasingly affecting the state and public administration as well as the security sector. It can be stated that communication and information technologies and devices have reached almost all areas of social life with their wide range of applications.

Intensive internationalization, increasing use of the Internet and liberalization of society, rapid increase in interconnection of individual actors within the ongoing globalization processes and continual acceleration of cooperation and interoperation at transnational level together with weakening of time and space barriers bring along with many positives also many negative effects in the shape of international terrorism, the threats of the use of weapons of mass destruction, cross-border organized crime, mass illegal migration, and more recently in cyberattacks on public or private computer networks. Cyber threats are thus becoming one of the most significant security threats at the end of second decade of the 21st century.

The rapid development of communication and information technologies, coupled with the massive deployment and use of communication and information systems and resources, brings on the one hand higher quality in many spheres of society, but on the other hand it increases the vulnerability of society and the individuals. Possibilities of disruption of this space are increasing and represent potential threats that almost all entities in society must deal with. [1]

Cyberspace as an intangible, virtual space created by modern technology, in which information and communication are exchanged through interconnected computer and telecommunications networks and equipment, [2] given its characteristics, provides free access to information and communications on the one hand, but on the other hand, it is a favourable environment for incidents, vulnerabilities or threats to the security of individuals and public and private organizations (companies). Given the seriousness of the risks and threats, cyber security is considered as a very important component of national and international security. Cyber security is therefore of high importance not only at national level but also at European Union (EU) level.

The rapidly evolving nature of cyber threats has necessitated the adoption of several measures to ensure cyber security both at national level and at the level of international organizations. At EU level, ENISA – the European Network and Information Security Agency was established by European Commission Regulation No. 460/2004 of 10 March 2004. Its primary task is to ensure a high level of network and data security in the EU. [3] As part of its activities, the Agency works very closely with the Member States of the Union and the private sector to provide advice and

solutions on cyber security. They are based in Greece with a centre in Heraklion, Crete and an operational office in Athens.

Computer Security Incident Response Teams (CSIRTs) or Computer Emergency Response Teams (CERTs), resp. National Cyber Security Centres (NCSCs) have been set up at national level in EU Member States. The main task of them is to provide the services needed to deal with computer security incidents, mitigate or eliminate their consequences, and subsequently restore the operation of operational information systems and related information and communication means. CSIRT / CERT / NCSC teams differ in their target groups. While the world is dominated by teams created by commercial companies and universities, CSIRT.SK (similarly to the CSIRTs in other EU countries) is a national / governmental cybersecurity team established by the Ministry of Finance of the Slovak Republic in accordance with the National Information Security Strategy in the Slovak Republic to ensure an adequate level of protection and management and its information systems. [4]

1. Cyber Security Policies from the Perspective of the European Union

Cyberspace and its evolution is an integral part of the development not only of each single country but also of a group of countries, for example in the form of a political and economic union such as the European Union.[1] A high level of computerization, information and cybersecurity is crucial for all countries to further progress and develop them in economic, political, social, cultural, technical, technological and other areas. This is directly related to addressing issues of critical infrastructure protection, the fight against cybercrime and the promotion of good governance. Ensuring security is one of the most important roles of each country, but even those that favour their own approach to cyber security recognize the important role played by international organizations and international law in raising the level of cyber security. [5]

Adoption of cybersecurity policies is not easy at all; on the contrary, it is very difficult due to various factors, for example due to the intangible nature of the acts (the impact of cyber security violations is often not visible in the physical sense) socio-technical dependence (people are the weakest link in ensuring cyber security), ambiguous impact if information or data is stolen or altered, or due to the controversial nature of the fight against cybercrime (uncertainty about the measures to be taken to improve security). [6]

However, in recent years, several major pieces of legislation have been adopted in the EU that are used to combat cybercrime, such as the Digital Agenda for Europe, the EU Cyber Security Strategy, the EU Cyber Security Policy, the Digital Single Market Strategy for Europe, the Directive on Network and Information Security and more.

[1] For more details see: [14], [15] a [16].

2. Developing cyberattacks on companies and solutions for protect against them

In today's information society[2], many companies are highly dependent on information and communication technologies and digital processes. In the future, this dependency will increase even further, although the financial losses caused by cyberattacks may climb to enormous levels depending on the size of the company.

Based on the annual Internet Security Threat Report, more than half a billion personal records and more than 4 billion data records are stolen or lost globally annually in recent years. The main targets of cyberattacks are businesses (more than half (55%) reported violations), but hackers also attacked medical institutions and government agencies. There has been an increase in fake emails to track message delivery, as well as the number of sophisticated phishing attempts targeted to specific departments within organizations, notably legal and finance departments.

Several companies have been the target of well-prepared phishing attacks. Half a billion new unique pieces of malware have been identified. Vulnerabilities can occur in almost any type of software, but the most attractive for targeted attackers is software that is widely used. Again, and again, most of these vulnerabilities appear in software such as Internet Explorer and Adobe Flash, which are used by huge numbers of consumers, amateurs and professionals daily. [7]

Organizations' performance in cyber security needs to address several issues such as data collection (in an environment characterized by frequent changes), quality of information (under explicitly indeterminate conditions), performance quantification, quality parameters or intangible results (eg innovation and adaptation capacity), including sensitive data (ethical and legal barriers). The problem is that cyber security is often not given as much attention as it deserves, but it is usually only received when an attack and consequential damage occurs. Another problem is the fact that this is an area that is changing very quickly, with thousands of new viruses and malicious programs being detected every day. Even experts have trouble keeping up with the latest technology.

2.1. Cyber security and IT services spending

In 2004, the global computer security market achieved a turnover of $ 3.5 billion, and in 2017 it was $ 120 billion. The computer security market has thus grown by approximately 35 years in 13 years. Experts predict that global spending on cyber security products and services will cumulatively exceed $ 1 trillion over the next five years. Cybercrime costs include data corruption and / or destruction, stolen money, lost productivity, theft of intellectual property, theft of sensitive personal and financial data, fraud, business disruption or other activity after an attack, forensic investigation, recovery and erasure of infected data and systems, and reputation damage. [8]

[2] For more details see: [17] a [18].

2.2. Expenditure on IT services within companies

IT consulting and outsourcing currently represent the categories with the highest spending on cyber security. By the end of 2020, the highest growth is expected to come from security testing, IT outsourcing and data loss prevention (DLP). By 2020, 90 % of organizations are expected to implement at least one form of integrated DLP. Today, it is about 50 %. [9]

Companies (businesses, organizations, companies) are deploying DLPs to address compliance, intellectual property protection and data visibility and monitoring. Newer solutions that include user entity and behaviour analysis, image analysis, machine learning, and data matching techniques are used to extend existing solutions. The unprecedented cybercrime activity brings so much cyber spending that it is almost impossible for an analyst to accurately track it.

2.3. Cyber insurance

Companies are trying to manage cyber risks by adopting a so-called cyber insurance covering specific losses. Insurance solutions have been introduced to the market by innovative insurance companies. Insurance is available from many insurers for various aspects of cyber risk, covering both first-party and third-party losses. Typical third-party coverage includes costs of regulatory investigations, data breaches or loss, media responsibility. The first parties include: crisis management, network disruption, extortion and commercial income and extraordinary expenses. [10]

While the European IT insurance market is still evolving, many companies in the United States already have a resolved liability policy that covers data loss. This is because US companies are obliged to inform their customers about security breaches. The implementation of similar regulations is currently under discussion in EU Member States, including the UK. [11]

3. Cyber security strategies in companies in the European Union

Companies (organizations, businesses, companies) may be reluctant to share information about their computer security spending with the public. Paradoxically, too little spending may indicate poor protection, while too much spending may indicate too much concern that they could be a potential target of attacks. [6] Investments in cyber security are mostly governed by regulatory requirements rather than informing organizations of current and persistent cyber security threats.

According to the results of the EU Security Survey in the Digital World, up to 57% of companies responding to the survey plan to increase the budget for cyber security in the next financial year, while 20% expect to maintain the current level of spending, while 23% still have no clear a picture of the budget for next year. [12]

According to the above survey, 40% of the companies surveyed have no formal cyber security strategy implemented and only 10% have reached a level where such a strategy has been defined, implemented and optimized. The survey also revealed that cyber security is still not fully understood and supported at the level of corporate executives (top managers, directors). Concerning how cyber security challenges are perceived, 87% of respondents are concerned about potential data leaks, 73% fear malware, 70% fear possible business continuity disruption, and another 70% are interested in ensuring protection against targeted cyberattacks.

Regarding potential factors that could have a positive impact on cyber security, most survey respondents believe that raising awareness (including training) of employees about cyberattacks and threats, along with increasing awareness and support for corporate governance, is a decisive factor in improving digital security.

Enforcement of regulatory requirements to improve digital security (77%) is seen as another positive factor. The need to allocate additional security resources (67%) and the exchange of security information with others (57%) was considered by many respondents to be very important for improving digital security. Respondents would also invest in improving the data backup and recovery process (20%), improving access to systems (19%), as well as in data leak prevention solutions (16%) [12].

Conclusion

The fact that companies are increasingly deciding to withhold and not provide critical data on cyberattacks on their networks is a worrying trend. As mentioned above, a low level of cyber security spending may indicate poor protection for companies, while too much funding may indicate too much concern that companies might be a potential target of cyberattacks. However, transparency is very important for security, which is why numerous data sharing initiatives are taking place in the security industry, some of which are increasingly collected and evaluated. Manufacturers must adhere to safety principles and strike the right balance between innovation and constraints. In principle, companies, as well as ordinary consumers, must be assured that suppliers produce and supply safe products and equipment they buy online.

Website security includes more information than just traveling information between the server and website visitors. Companies need to think about their website as part of a system that needs constant care and attention to maintain people's trust. Despite the increasing number of sophisticated cyberattacks, website owners still do not update their websites and servers as often as they should. Companies are encouraged to use technology and expertise to identify risks and keep their computing environment secure. This is particularly important in addressing advanced and targeted cyber threats.

In this context, an increasing number of national cyber security strategies, while addressing mission security [13] are gratifying. However, these documents remain at risk of many problems. Future strategies or their updates must not neglect human resources, especially in raising awareness of cyber security and training staff who act as the first line of defence against potentially destructive cyberattacks.

In conclusion, given that the human community is increasingly dependent on globally interconnected information and communication systems in almost all areas of its activity, the phrase "there is no boundaries in cyberspace" is now much more valid and relevant than ever before. Cyberattacks on public and private networks have confirmed that there is a danger of cyber threats, both at national and international level. Cooperation in the fight against cyber threats and attacks, cyber terrorism and cybercrime; therefore, requires concerted efforts of relevant organizations, institutions, corporations, and companies at national and international level.

References

[1] NEČAS, P. – UŠIAK, J. 2010. *Nový prístup k bezpečnosti štátu na začiatku 21. storočia*. Liptovský Mikuláš : Akadémia ozbrojených síl generála Milana Rastislava Štefánika v Liptovskom Mikuláši. 2010. 167 p. ISBN 978-80-8040-401-7.

[2] KOEPSELL, D. R. 2003. *The Ontology of Cyberspace*. Chicago : Open Court Publishing, 2003, 160 p. ISBN 978-0-8126-9537-3.

[3] ENISA. 2019. *European Network and Information Security Agency*. [on line] [cit 10-10-2019] available from: <https://www.enisa.europa.eu>

[4] CSIRT.SK. 2019. *Computer Security Incident Response Team*. [on line] [cit 10-10-2019] available from: <https://www.csirt.gov.sk>

[5] SHACKELFORD, S. J. – KASTELIC, A. 2016. *Toward a state-centric cyber peace? Analyzing the role of national cybersecurity strategies in enhancing global cybersecurity*. [on line] [cit 11-10-2019] available from: <http://www.nyujlpp.org/wp-content/uploads/2016/01/Shackelford-Kastelic-State-Centric-Cyber-Peace-18nyujlpp895.pdf>

[6] BRUIJN, H. – JANSSEN, M. 2017. Building cybersecurity awareness: The need for evidence-based framing strategies. In *Government Information Quarterly*, Vol. 34, No. 1/2017, pp. 1-7. ISSN 0740-624X.

[7] SYMANTEC. 2018. *Internet Security Threat Report*. [on line] [cit 10-10-2019] available from: < https://www.symantec.com/security-center/threat-report>

[8] CYBERSECURITY VENTURES. 2018. *2018 Cybersecurity Market Report.* [on line] [cit 10-10-2019] available from: <https://cybersecurityventures.com/cybersecurity-market-report/>

[9] GARTNER. 2016. *Gartner Says Worldwide Information Security Spending Will Grow*. [on line] [cit 10-10-2019] available from: <https://www.gartner.com/newsroom/id/3404817>

[10] PROPERTYCASUALTY360. 2017. *The cyber liability insurance market rises.* [on line] [cit 10-10-2019] available from: <https://www.propertycasualty360.com/2017/09/19/the-cyber-liability-insurance-market-rises/?slreturn=20180918101428>

[11] WITTE, CH. 2017. *Attacks from cyberspace.* [on line] [cit 10-10-2019] available from: <https://www.agcs.allianz.com/assets/PDFs/GRD/GRD%20individual%20articles/It_failures_cybercrime.pdf>

[12] TODAY. 2018. *More than half of companies plan cybersecurity budget increase.* [on line] [cit 10-10-2019] available from: <http://www.outsourcing-today/ article.php?id=7084>

[13] NEČAS, P. – ANDRASSY, V. 2018. Diplomatic missions order versus security and sustainability. In *Journal of Security and Sustainability Issues*, Vol. 8, No. 2 (2018), pp. 267-276. ISSN 2029-7017.

[14] BRHLÍKOVÁ, R. 2013. *Politiky Európskej únie po Lisabone*. Nitra : Univerzita Konštantína Filozofa v Nitre, 2013. 326 p. ISBN 978-80-558-0478-1.

[15] ROŽŇÁK, P. 2015. *Politologie pro všechny*. Ostrava: Key Publishing, 2015. 343 p. ISBN 978-80-7418-214-3.

[16] ROŽŇÁK, P. 2015. *Mechanizmy fungování Evropské unie*. Ostrava: Key Publishing, 2015. 331 p. ISBN 978-80-7418-237-2.

[17] BARIČIČOVÁ, Ľ. 2018. Informačná kompetentnosť v kontexte aktuálnych potrieb informačnej spoločnosti. In *Aktuálne výzvy prevencie počítačovej kriminality – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia policajného zboru v Bratislave, 2019, pp. 8-17. ISBN 978-80-8054-773-8.

[18] KUCHTOVÁ, J. 2018. Aktuálne trendy súvisiace s využívaním moderných technológií. In *Aktuálne výzvy prevencie počítačovej kriminality – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia policajného zboru v Bratislave, 2019, pp. 90-98. ISBN 978-80-8054-773-8.

Author:

[1]**Radoslav Ivančík –** Akadémia Policajného zboru v Bratislave, Sklabinská 1, 835 17 Bratislava 35, Slovenská republika, email: radoslav.ivancik@minv.sk