Литература:

1. Бишоп, М. Окинавское каратэ: учителя, стили, тайные традиции и секретная техника школ воинского искусства / Пер. с англ. А. Кратенкова. - М.: ФАИР-ПРЕСС, 1999.
2. Бовин, А. Управление инновациями в организациях. - М., 2008.
3. Кулик В., Полтораков А. Проблемы обеспечения национальной безопасности Украины. – Киев, Центр исследований проблем гражданского общества. – 2010. – 12 с.
4. Korzeniowski L.F. Securitologia – naukowe badania problematyki bezpieczeństwa człowieka i organizacji społecznych., Securitologia. - 2012, № 2 (16)., pp. 11-46 ISSN 1898-4509
5. Peter van Ham and Richard L. Kugler - Western Unity and Transatlantic Security Challenge The M. Center Paper N4, 2004
6. Попов, Пл. Охранителна дейност. С., 2008.
7. Uzunov, D., A. Bakhchevan, «Personal security» - a new method of teaching the officers of law enforcement and security agencies aimed at security ensuring and crime prevention., INNOVATIONS IN SCIENCE AND EDUCATION: CHALLEGES OF OUR TIME. - London, 2016, pp. 96-98.
8. Узунов, Д., Усъвършенстване на методика на обучение по БПТ, гр. Варна, 2011 г.
9. Bedzhev B.Y., Zhekov Zh.St., Prodanova P.K., A Method for Synthesis of Orthogonal Complementary Codes, Proceedings of CERC 2004, Military Technical Academy – Bucharest, Romania, 20.05.-21.05.2004., pp. 184-192.
10. Innovation Policy in Europe 2004, DG Enterprise and Industry. – Brussels., 2004.
11. St.J. Blank, William T. Johnsen, Earl H. Tilford, Jr. – US Policy in the Balkans, 2005.
12. The Army in the Multinational Operations HQ Department of the Army, 2004.
13. Thomas Sluyter. Lexicon: keiko, 2012.
14. NATO in the 21st Century, 2005.

EDUCATION ON CYBER SECURITY ISSUES UNDER EUROPEAN UNION LAW. A STANDARD OF PERSONAL DATA PROTECTION

J. Osiejewicz, PhD, Assistant Professor
Faculty of Law and Administration, Legal Communication Laboratory, University of Zielona Góra, Poland
M. Jóźwik, MSc, Eng., Graduate
Faculty of Electronics and Information Technology, Institute of Computer Science, Warsaw University of Technology, Poland

Conference participants

The computer information systems that are applied in business marketing or in public agencies (e.g. for fiscal or national health insurance purposes) are complex products developed by specialized software engineers and accompanied by lots of documentation, tutorials and user manuals. These systems act in a comparatively complex environment of hardware devices and network infrastructure, often coexisting with other systems. No software product is 100% errorless and user-proof, so education of end users is critical for the security of the whole system in terms of preventing an unauthorized access that could expose data to the risk of loss or theft. The article presents threats connected with the use of complex computer information systems as well the related EU legal framework concerning cyber security. The purpose of the article is to highlight the current EU legal standard for cyber security and to indicate the urgent need for specialized education of the digital society members in this area.

Introduction

The more the computer-assisted systems support the members of digital society in a variety of business areas and their private life, the more knowledge is required for the users in order to properly and responsibly take advantage of these systems. Developing a safe, complex computer information system (hereinafter: CIS) is a tough task. Considering security issues in relation with a CIS would refer, but not be limited, to the following risks: data pollution (a system allows entering of invalid data and thus makes the existing data useless)[1]; data loss (a system allows cancelation of data while not providing a data back up to restore them); data leak (unauthorized access to the system exposes sensitive, secret data, e.g. personal data, to a leak)[2], data theft (creating an additional, unauthorized copy of high-valuedata)[3]; system lock (unauthorized, harmful software running on a hardware, being part of the system disallows access to the system)[4]; system damage (a physical damage to the infrastructure caused by intruder's activity)[5]; disaster causing a great damage (cyber attack directed e.g. on SCADA systems that are used to control automation processes in various areas of infrastructure, such as gas pipelines or nuclear energy plants)[6][7]

In order to prevent these threats effective users' education is needed. In most cases the cyber security incidents are made possible because of ignorance or recklessness of system users, who consciously violate security procedures for a trivial shortcut in daily work. The everyday life gives several examples of officials failing to comply with basic security rules regarding information systems, e.g.:

1 S. Curtis, Mirror, Bupa suffers massive data breach exposing personal details of over 100,000 health insurance customers, 13 July 2017, http://www.mirror.co.uk/tech/bupa-suffers-massive-data-breach-10793166, accessed 19 July 2017.
2 E. Perez, E. Sciutto, L. Jarrett, CNN, Contractor charged with leaking classified NSA info on Russian hacking, 6 June 2017, http://edition.cnn.com/2017/06/05/politics/federal-contractor-leak-prosecution/index.html, accessed 19 July 2017.
3 D. Talbot, Cyber-Espionage Nightmare, MIT Technology Review, 10 June 2015, https://www.technologyreview.com/s/538201/cyber-espionage-nightmare/, accessed 19 July 2017.
4 Aljazeera, Global hacking attack infects 57,000 computers, 13 May 2017, http://www.aljazeera.com/news/2017/05/global-hack-attack-infects-57000-computers-170513005030798.html, accessed 19 July 2017.
5 K. Zetter, Wired, A cyber attack has caused confirmed physical damage for the second time ever, 8 January 2015, https://www.wired.com/2015/01/german-steel-mill-hack-destruction/, accessed 19 July 2017.
6 J. Swearingen, New York Magazine, New 'Industroyer' Virus Is Designed to Take Down Power Grids, 13 June 2017, http://nymag.com/selectall/2017/06/industroyer-crash-override-virus-power-grid-attack.html, accessed 19 July 2017.
7 K. Poulsen, Daily Beast, U.S. Power Companies Warned 'Nightmare' Cyber Weapon Already Causing Blackouts, 12 June 2017, http://www.thedailybeast.com/newly-discovered-nightmare-cyber-weapon-is-already-causing-blackouts, accessed 19 July 2017.

the CIA director and his hacked email account[8]; the CEO of one of the Swedish biggest security companies who went bankrupt after he lost his identity through a computer hack[9]; emails leaked off the US Democratic National Committee because of e-mail server being hacked, which triggered a catastrophic loss for Clinton's campaign[10]. However, damages caused by cyber attacks may have significant consequences also for averagecitizens. Moreover, those affected have little or even no influence on how well their data is protected. The purpose of the article is therefore to present the current European Union (hereafter: EU) legal standards for cyber security and to indicate the urgent need for specialized education of the digital society members on this subject matter.

Educational assignments of the European Network and Information Security Agency

On 10 March 2004, the European Parliament and the Council issued a Regulation 460/2004 establishing the European Network and Information Security Agency (ENISA)[11]. The Regulation states that in order to ensure confidence in networks and information systems it is necessary to inform, educate and train individuals, businesses and public administrations sufficiently in the field of network and information security. It also provides for that public authorities shall play a role in increasing awareness by serving information to the general public, small and medium-sized enterprises, corporate companies, public administrations, schools and universities. It assigns the obligation to the Agency to provide advice on best practices in awareness raising, training and courses[12]. Furthermore, ENISA should contribute to the availability of timely, objective and comprehensive information on network and security issues for all users. For this purpose, ENISA is expected to promote exchange of up-to-date best practices, including methods of alerting users, and seeking synergy between public and private sector initiatives[13]. The Agency was initially established for the period of five years beginning from 14 March 2004[14]. The continuity of ENISA's mandate was later prolonged for the period of another three years through the Regulation 1007/2008[15], and, subsequently, for another 18 months through the Regulation 580/2011[16]. Finally, the Regulation 526/2013[17] repealed Regulation 460/2004 and established again the ENISA for a period of 7 years agreeing that its headquarter shall be Heraklion(Crete, Greece)[18].

After having established the ENISA, the EU pointed its crucial role in European cyber security in the Directive 2016/1148[19], the so-called Network and Information Systems Directive (hereafter: the NIS Directive). The NIS Directive refers to the ENISA stating that the Agency should assist the Member States and the Commission by providing expertise and advice and by facilitating the exchange of best practice[20]. It also indicates that ENISA should assist and serve guidanceas for adopting legal regulations on cyber security in the EU and provide exercises and trainings, helping to achieve appropriate level of readiness and awareness of interested parties[21].The NIS Directive defines *incident* as "any event having an actual adverse effect on the security of network and information systems"[22], whereas the *incident handling* means "all procedures supporting the detection, analysis and containment of an incident and the response thereto"[23]. In the wording of the NIS Directive, *risk* is to be understood as "any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems"[24]. The content of the definitions indicate that physical, organizational, legal and financial infrastructure is needed to implement a system evaluating and mitigating risks, preventing and handling incidents in network infrastructure of information systems in order to ensure cyber security on a national level. In every aspect, it involves training and education of all user, in particular teams, organizations and cooperating entities, to achieve a predictable and measurable progress in a fight against cybercrime.

The NIS Directive focuses i.a. on training professionals in securing crucial infrastructure of "operators of essential services"[25]. Such an operator would be an entity providing service that is essential for the maintenance of critical societal and/or economic activities, whereas the provision of that service depends on network and information systems and an incident would have significant disruptive effects on the provision of that service. Sectors and subsectors, in which operators of essential services would operate are listed in Appendix II of the NIS Directive: electricity; oil; gas;air transport; rail transport; water transport; road transport; banking; financial market; health;drinking water supply and distribution; and digital infrastructure.The Member States should identify those entities by November 9, 2018[26] and include them in a national strategy on the security of network and information systems. The national strategy on the security of network and information systems shall address, in particular, "an indication of the education, awareness-raising and training programmes relating to the national strategy on the security of network and information systems"[27].

8 K. Zetter K, Wired, TeenWhoHacked CIA Director's Email Tells How He Did It, 19 October, 2015, https://www.wired.com/2015/10/hacker-who-broke-into-cia-director-john-brennan-email-tells-how-he-did-it/, accessed 19 July 2017.

9 N. Rolander, Bloomberg, Swedish Security Company Boss Declared 'Bankrupt' After Identity Stolen https, 12 July 2017, https://www.bloomberg.com/news/articles/2017-07-12/securitas-ceo-declared-bankrupt-after-his-identity-was-stolen, accessed 19 July 2017.

10 L. Harding, The Guardian, Top Democrat's emails hacked by Russia after aide made typo, investigation finds, 14 December 2016, https://www.theguardian.com/us-news/2016/dec/14/dnc-hillary-clinton-emails-hacked-russia-aide-typo-investigation-finds, accessed 19 July 2017.

11 Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance), Official Journal L 077, 13/03/2004 P. 0001 – 0011.

12 Recital 14, ibidem.

13 Article 3 (e), ibidem.

14 Article 27, ibidem.

15 Article 1, Regulation (EC) No 1007/2008 of the European Parliament and of the Council of 24 September 2008 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration (Text with EEA relevance), Official Journal L 293, 31.10.2008.

16 Article 1, Regulation (EU) No 580/2011 of the European Parliament and of the Council of 8 June 2011 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration (Text with EEA relevance) OJ L 165, 24.6.2011, p. 3–4.

17 Article 35, Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 (Text with EEA relevance) OJ L 165, 18.6.2013, p. 41–58.

18 Recital 4, ibidem.

19 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, OJ L 194, 19.7.2016, p. 1–30.

20 Recital 36, ibidem.

21 Recital 38, ibidem.

22 Article 4 p. 7, ibidem.

23 Article 4. p. 8, ibidem.

24 Article 4 p. 9, ibidem.

25 As defined in Article 4 p. 4 and Article 5 p. 2, ibidem.

26 In accordance to the Article 5 p. 1, ibidem.

27 As defined in Article 7, ibidem.

The EU Member States are obliged to implement the NIS Directive by May 10, 2018[28], that is i.a. those aspects regarding: education[29]; risk mitigation[30]; incidents recognition and handling[31]; data and information exchange[32]; strategy building[33]; operators of essential services identification[34].

Security issues regarding CIS should be of interest of system technical designers and architects, end users, system administrators, legislators, as well as system manual creators. The proper legislation is likely to enforce adequate CIS tailoring through the regulation of preliminary design phases and the introduction of obligatory administrator tasks control lists. However, every system would be unprotected, if end users were not act responsibly and with the so-called "cyber hygiene". For this purpose, ENISA introduced a short pamphlet for every CIS user, giving hints on how to stay protected in daily Internet life[35].

Cyber security of Personal Data as a Module Standard

It should be noticed, that by 2017 there has been 13 years since ENISA was founded. Recital 16 of the Regulation 526/2013 stresses, referring to its goals and objectives, that "In order to achieve this, the necessary budgetary funds should be allocated to the Agency". Budget should be "sufficient and autonomous" and "comes primarily from a contribution from the EU and contributions from third countries participating in the Agency's work"[36].The budget of ENISA was set to: 10,06 Million Euro in 2015,11,03 Million Euro in 2016, and 11,24 Million Euro in 2017[37]. Regarding the goals and objectives of ENISA and its special role as an expected shield providing advise and education, aiming at the protection of the EU's private businesses and government agencies from cyber attack,which could have enormous implications[38], the annual budget of ENISAis obviously insufficient. To make it more visible: 11 Million Euro would allow to buy about 500 minutes for commercials in one of the Polish TV networks during high publicity[39]; 11 Million Euro will be paid to a runner-up of football Champions League finals in 2017[40]; 11 Million Euro would allow to break into 10 iPhone locked phones in search for information possibly allowing to prevent a terrorist attack[41]; 8 annual budgets are needed to buy one combat plane Eurofighter Typhoon[42].

Regarding the alleged costs of cyber defence, it should be therefore pointed out that every state needs to introduce and to execute high national legal standards in computer network information systems to ensure that use rare appropriately trained and educated. This requirement is supported by the Regulation 2016/679[43] on personal data protection, according to which a private company can be fined up to 20 Million Euro or 4% of its annual world income for the violation of personal data protection rules[44]. However, in the 119 pages long text of the Regulation 2016/679, a term "education" is mentioned only twice and it only once points to a need to introduce awareness-raising activities addressed to the public, including micro, small and medium-sized enterprises, as well as natural persons in particular in the educational context[45]. The NIS Directive states that personal data are in many cases compromised as a result of incidents[46] and indicates that the processing of personal data shall be carried out in accordance with EU law[47].

However, this is the educational aspect, not the penalization of infringements to the law that should be put in the limelight. The educational approach is more likely to make the data processing more secure, because it is based not on the effect, but on the cause of the infringement. This approach has been applied in the Polish Regulation on the appropriate organizational and technical conditions required for personal data processing in computer systems[48]. The Regulation describes in detail the composition of the security policy that is required to be introduced by any entity processing personal data with the use of IT systems: enumeration of buildings, where data is processed; description of data sets;data flows; procedures of the assignment of credentials; start, pause and end of a working day; creation of backups and storage;handling of electronic data carriers; electronic system security; and systems reviews and maintenance[49]. The Regulation also introduces three levels of required security, depending on the category of the processed data as well as on whether the system is connected to a public information network. The levels of sensitivity, that is basic, intermediate and high, provide for detailed description of precautions needed to be undertaken in order to comply with the required security, such as:the limitation to access to rooms where personal data is stored; the necessity to change password every 30 days; the requirement to

---

28 Article 25, ibidem.
29 Art. 7 p. 1(d); Art. 11 p. 3 (e), (f), (k); Art. 12 p. 3 (h); Art.12 p. 3 (j); Art.13 p. (6), p. (7), ibidem.
30 Art. 4 p. 9; Art 6; Art.7 p. 1(f); Art.11 p. 3 (i); Art.12 p. 3 (f); Art.14 p. (1), p. (2), ibidem.
31 Art.1 p. 2(c); Art. 4 p. (7), p. (8); Art. 12 p. 3 (c), (d), (e); Art. 14 p. (4), ibidem.
32 Art.1 p. 2(b); Art. 8; Art.10; Art.11; Art.12, Art.14 p. (3), p. (5), Art. 16 ibidem.
33 Art. 1 p. 2(a); Art. 4, p. (3), Art. 7, ibidem.
34 Art. 5; Art.6; Art.14; Art.15, ibidem.
35 ENISA, https://www.enisa.europa.eu/media/multimedia/posters/cybersecurity-education-posters-2016/enisa-eduposters-el.pdf/, accessed 19 July 2017.
36 Recital 51, Regulation 526/2013, op. cit.
37 Statement of Estimates 2017 (Budget 2017), European Union Agency for Network and Information Security, https://www.enisa.europa.eu/about-enisa/accounting-finance/files/annual-budgets/enisa-2017-annual-budget, accessed 19 July 2017.
38 See: M. Elsberg, Blackout – Morgenist es zuspät, Blanvalet Verlag 2012. The author presents an interesting vision of a total and universal disaster after a cyber attack turning off the electricity in Europe and United States.
39 P. Pallus, Business Insider Polska, Najdroższe reklamy są w Polsacie. Do 97 tys. zł za pół minuty, 22 August 2016, http://businessinsider.com.pl/media/reklama/koszt-reklamy-telewizyjnej/2rjtmpd, accessed 19 July 2017.
40 2016/17 Champions Leaguer evenue distribution, 25 August 2016, http://www.uefa.com/uefachampionsleague/news/newsid=2398575.html, accessed 19 July 2017.
41 J. Edwards, Reuters, FBI paid more than $1.3 million to break into San Bernardino iPhone, http://www.reuters.com/article/us-apple-encryption-fbi-idUSKCN0XI2IB, accessed 19 July 2017.
42 http://www.deagel.com/Combat-Aircraft/Typhoon_a000442001.aspx, accessed 19 July 2017.
43 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88.
44 Article 83 p. 5, ibidem.
45 Recital 132, Regulation 2016/679, op. cit.
46 Recital 63, Directive 2016/1148, op. cit.
47 Article 2, ibidem, indicating the Directive 95/46/EC, that has been repealed by the Regulation (EU) 2016/679, op. cit. Processing of personal data by Union institutions and bodies pursuant to this Directive shall be carried out in accordance with Regulation (EC) No 45/2001, Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, p. 1–22.
48 RozporządzenieMinistraSprawaWewnętrznychiAdministracji z dnia 29 kwietnia 2004 r. w sprawiedokumentacjiprzetwarzaniadanychosobowychorazwarunkówtechnicznychiorganizacyjnych,jakimpowinnyodpowiadaćurządzeniaisystemyinformatycznesłużącedoprzetwarzaniadanychosobowych, Dz. U. z 2004 r. Nr 100, poz. 1024.
49 Article 4, ibidem.

encrypt solid memory units in portable devices; procedures for the utilisation of wasted devices on which the personal data is stored. This Regulation could serve as a model standard of how education on cyber security could be brought into legislation, presenting to readers in-depth precautions indispensable to comply with the law. Interestingly, this Regulation is consistent with the international norms ISO/IEC 27000[50], altogether allowing for relatively easy and predictable processing of personal data in CIS supported by a chain of education, training and certification.

The healthcare system is a representative area of sensitive data that demands great awareness and knowledge in the process of its securing. The Polish Regulation regarding requirements for the System of Medical Information[51] establishes a central national database i.e. of medical occurrences and documents issued by healthcare entities. The Regulation includes a list of Polish norms, which the System of Medical Information shall be compatible with[52]. The norms provide for a model of electronic documentation and security procedures for data transmitted in the healthcare system. It refers to EU regulations regarding data security in international transmission of healthcare data[53] and points out to the ISO/IEC 27002[54] in the context of the management of information security in the healthcare system. References to international norms can be also found i.e. in the Polish Regulation on the system of threads monitoring[55] and in the Polish Regulation regarding minimal requirements for some data communication systems functioning in the healthcare system[56].

Conclusions

The legal approach to cyber security and cyber defence needs to be developed on a educational level in order to ensure that the assumptions of the EU regulations are possible to be achieved with the allocated means, that is: budget, infrastructure and authority's support. Too much expectation for required results in cyber defence relying on ENISA could undermine the awareness for the need of education on cyberspace security. It is obvious that ENISA is not able to cover this subject efficiently, since the annual budget allocated for its activities is not sufficient in any case.

In order to protect the cyberspace, the legislator should include in adopted legal acts the information on not only "what" should be done and "what" is allowed or disallowed, but also on "how" to do it and "how" to avoid the risks. To improve the law quality and to comply with the intentions of the legislator it is therefore recommended to provide for more specific information on how to achieve the desired result by giving reference to widely accepted norms, standards or literature published by or on behalf of legal authorities. It is also advisable to introduce educational programs intending to train not only entrepreneurs and entities, who are responsible for cyber security, but also "ordinary citizen" on what level of security they may expect from those responsible for their security and how they could safeguard themselves.

EUROPEAN STANDARDS OF YOUTH WORK SECURITY

M. Dei, Candidate of Jurisprudence, Associate Professor of Academic dpt
of University Education and Law of SHEI
University of Educational management NASU, Ukraine
H. Karieva, Postgraduate Student
Kyiv University of Law of NASU, Ukraine

Conference participants

In this article we consider the peculiar properties of regulation of minor's workers security within the Law of the European Union. To reveal such peculiar properties of legal regulation of a work security of youth within the Instruction of EU 89/391/EEC, as well as Instructions of 94/33/EC. Proper analysis of regulation of rules and rules of guarantees of the workers` rights under the age of 18 years which work on the basis of the labour contract or rules which are determined by the current legislation of the state-member and/or conformed to the current legislation of the state-member was fulfilled. Thus, we may confirm, that except for some details, within EU territory the complex of the minimal labour standards for stable working environment which now are applied in all states-participants is created.

Keywords: *work security, youth work, European Union, EU legislation.*

The important direction of Ukrainian integration is cooperation with the European Union which final strategic aim - fully entry of Ukraine into the European Union. A key element of successful integration is an achievement of the certain level of a coordination of the legislation of our country with European Union law.

One of directions of harmonization process is coordination of Ukrainian legislation which settles labour safety issue in conformity with rules of the European Union. It has to be noticed, that labour safety, especially an issue of work of youth safety is related to the area of the labour law.

Some radical political, economic changes in state and society, have pointed the problems connected with use of hired labour, creation of the effective mechanism of regulation of labour relations, providing of guarantees of human's right to work. Their resolving, especially concerning work of youth, has the important social value, requires radical changing of traditional approaches

50 ISO/IEC 27000 family - Information security management systems, https://www.iso.org/isoiec-27001-information-security.html, accessed 19 July 2017.
51 Rozporządzenie Ministra Zdrowia z dnia 28 marca 2013 r. w sprawie wymagań dla Systemu Informacji Medycznej, Dz.U. 2013 poz. 463.
52 Article 9, ibidem.
53 Article 12, p. 2, ibidem.
54 ISO/IEC 27002:2013, https://www.iso.org/obp/ui/ Information technology -- Security techniques -- Code of practice for information security controls, available at: https://www.iso.org/standard/54533.html, accessed 19 July 2017.
55 Article 4, Rozporządzenie Ministra Zdrowia z dnia 9 lipca 2013 r. w sprawie Systemu Monitorowania Zagrożeń, Dz.U. 2013 poz. 853.
56 Article 9, Rozporządzenie Ministra Zdrowia z dnia 14 sierpnia 2013 r. w sprawie minimalnych wymagań dla niektórych systemów teleinformatycznych funkcjonujących w ramach systemu informacji w ochronie zdrowia, Dz.U. 2013 poz. 999.