KOŠICKÁ BEZPEČNOSTNÁ REVUE

KOSICE SECURITY REVUE

Vol. 10, No. 1 (2020), p. 35 – 44

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

Managing Personal Data Security in E-Government Processes

Správa bezpečnosti osobných údajov v procesoch e-governmentu

Hemin Muhammad[1] and Ludek Lukas[2]

[1] Faculty of Applied Informatics, Tomas Bata University in Zlin
2 Faculty of Applied Informatics, Tomas Bata University in Zlin

The manuscript was received on 02. 04. 2020 and was accepted after revision for publication on 21. 05. 2020

Abstract:

The aim of this article is an analysis of managing personal information security within information systems in government organizations. Personal data protection and organization records can be guaranteed as necessary in appropriate legislation, regulations, contractual sections, and technical solutions. Therefore, the research focus on legal and technical approaches that required for securing personal information as well as some specific threaten are shown. General Data Protection Regulation (GDPR) as a powerful regulation for protecting individual's data is discussed with a concentrate on Electronic Identification, Authentication, and Trust Services (eIDAS). eIDAS is controlling electronic signatures, electronic transactions, and other transactions in order to deliver a safe method for users to do online businesses. It makes participants and receivers obtain more security and suitability that provide. In the technical section, most of the necessary information that requires protecting personal data and building a highly secure information system are studied. Besides, the main threatens on an information system and personal data are illustrated by introducing solutions for each of the presented threats.

Keywords: *GDPR, eIDAS, personal information, security, e-government.*

Abstrakt:

Cieľom článku je analýza súčasných trendov v oblasti ochrany osobných údajov v informačných systémoch štátu, zavádzaných v rámci e-governmentu. Požiadavka zabezpečenia ochrany osobných údajov patrí medzi základné predpoklady zaistenia dôveryhodnosti a použitia e-governmentu v štátnej správe. Ochrana osobných údajov by mala byť zabezpečená s pomocou legislatívy, predpisov, zmluvných dohôd a technických riešení. Článok sa zameriava na právne a

technické prístupy, využívané v rámci procesov zabezpečenia ochrany osobných údajov. Medzi hlavné analyzované opatrenia spadá „Všeobecné nariadenie o ochrane osobných údajov“ (GPDR) a „Nariadenie o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie“ (eIDAS). GDPR vytvára právny a organizačný rámec zabezpečenia ochrany osobných údajov. Cieľom eIDAS je špecifikácia technických opatrení z hľadiska elektronickej identifikácie užívateľov a dôveryhodnosti elektronických transakcií. S pomocou týchto opatrení je v rámci e-governmentu zaistená ochrana osobných údajov na garantovanej úrovni nielen v rámci jednotlivých členských štátov, ale celej Európskej únie.

***Kľúčové slová**: GDPR, eIDAS, osobné informácie, bezpečnosť, e-government.*

Introduction

Before inventing information system, which is called paper era, information was more protected because most information was kept only in paper files, and only in certain departments of a business, where many workers would not have access to the information. With the development of computer-based information systems, large amounts of information can be stored electronically rather than in paper formats, therefore the data can be seen by a larger number of users. Thus, many users can reach the information electronically rather than physically and information is more vulnerable to the risk of computer crime and computer misuse. The existing computer issues have threatened information systems in the government and business organizations due to the increased dependability of businesses and individuals on information systems. As well as, with the growing use of the internet in technology systems rate of attacks on information systems increased. Therefore, security and protecting data have to be considered in designing and developing any kind of information system. Attackers can access to a large volume of data easily when there is a simple error in the information system such as hardware failure, software failure, electrical problems, personnel actions, user errors, and communication problems.

Once the network itself is endangered, information systems of an individual or business become even more threatened[1]. Nowadays information systems facing many issues. These issues usually either happened through computer crime or computer misuse. These issues are broadly becoming a common problem as technology can support complete almost any unlawful or unprincipled task. There is a difference between computer crime and computer abuse. Computer crime is when a person uses a computer to commit a prohibited action, whereas computer misuse is when a computer user uses a computer to commit an unethical but not always illegal action. Data is a core element of any information system like e-government. Therefore, the security of data should take into high consideration with designing, planning, and deploying e-government particularly personal data which is a foundation for e-government because E-governments cannot function to their maximum prospective without obtains necessary personal data from citizens. The relations between citizens and e-government services need a legal infrastructure to address privacy protection. Government regulation and organization self-regulation of solution for protecting personal information. Cybersecurity is a procedure of protecting information and data against any violation like loss, misuse, destruction, changing information security should be considered from outside and inside of the organization because loss, misuse, and theft not only come from surroundings but also could become inside the organizations. [2]

1. E-Government

The simple definition of e-government is using information and communication technology in government organizations to deliver government services to citizens and businesses. It plays a great role in providing facilities for people and fastens daily businesses[3]. In general, the following are the main benefits of e-government:

- Reduced production cost
- Better services
- Avoidance of personal interaction
- Convenience
- Personalization
- Reducing corruption
- Efficiency
- Effectiveness
- Transparency
- Greater democratic participation
- 24/7 accessibility
- Flexibility
- Time saving [4]

Besides of giving e-service to citizens, e-government provides services for all organizations within its authority. The services vary according to the user's requirements. Based on functions, there are four main categories of e-government which are Government to Citizen (G2C), Government to Business (G2B), Government to Government (G2G), and Government to Employee (G2E). G2C makes citizens have direct and appropriate access to government information and services from everywhere anytime, through the use of several channels. Therefore the majority of government services come under G2C. G2B carries important productivities to both governments and businesses. It provides many services exchanged between government and the business sectors such as the delivery of policies, memos, instructions, and rules. G2B also plays an important role in business growth particularly for small and medium enterprises. G2G is an online communication between government organizations, agencies, departments, and units. The main aim of G2G is to centralizing and sharing information among government organizations. The last category is the G2E. It is an online relationship between the government and its employees. G2E offers various online services to employees such as requesting online leave, checking leave balance, checking overtime works, and obtaining salary payment records. [5]

1.1 E-Government Challenges

In developing countries many factors affecting on progressing e-government such as ICT infrastructure, political issues, social issues, and organizational issues. But in some countries, citizen's trust in the internet or government are the main factors of failure in e-government implementation. Government agencies and users have a role in generating challenges. Besides all aforementioned benefits in section 1, some

challenges are deterring the progress of e-government applications. According to many types of research that have been done on e-government barriers reveal that the key challenges e-governments are:

- Privacy issues
- Digital divide
- Availability
- Trust
- Security
- Improper integration between systems and governmental departments
- Infrastructure costs
- Lack of legal frameworks supporting e-government
- Cultural issues
- Lack of Partnership and Collaboration.

Privacy is a serious problem in the employment of e-government because it refers to the assurance of a suitable level of protection information attributed to an individual and the government has a responsibility to guarantee citizens' rights regarding privacy. People worry about information sharing, mishandling of private information, and sometimes about e-government itself because the government can monitor citizens and enter their privacy. For addressing privacy issues, technical and policy responses are required. E-government must achieve citizen's confidence in the privacy and careful handling of any personal information shared with government organizations since most of the information in e-government consisted of personal data. Sometimes people reject e-government services because they are concerned about privacy. Therefore, governments should provide a comprehensive privacy policy in their e-applications to offer insurance to people about their privacy rights and clarify for them that their personal information is collected and processed only for legitimate purposes[4], [6].

2 Threats on Personal Data in E-Government

E-service users are careful in giving their data, they would like to identify who and where they give data to. Hence, security and transparency are the most important factors that must available in e-government. According to works of literature, most of the people are not willing to give their data to e-government when there is not a privacy policy for saving their data. Protect data in e-government information systems require a strong law, regulations, and technical infrastructure. As it is studied, having a problem with privacy leads to losing trust in e-services by citizens and creates an obstacle in implementing e-government. Organizations have to protect all assets within an information system not only sensitive data since having threats on any asset in an information system creates risk on personal data. Threats usually lead to attack information systems via individual computer and it has the main risk on personal data because it can let unauthorized persons access personal information through a small program that able to cross the line between the user's internet and a web site[7],[15] . The following threats are the most common threats affecting information systems in e-government applications.

- Spamming*:* is "the use of messaging systems to send an unsolicited message (spam), especially advertising, as well as sending messages repeatedly on the same website. While the most widely recognized form of spam is email spam, the term is applied to similar abuses in other media. Since spamming is one of the

inexpensive and easiest ways to abuse a computer system, it becomes a risk on an information system and personal data[8].

- ***Hacking:*** Hacking is "generally refers to unauthorized intrusion into a computer or a network. The person engaged in hacking activities is known as a hacker. This hacker may alter system or security features to accomplish a goal that differs from the original purpose of the system". Hacking usually done by special programs like Trojan horses, logic bombs[2].
- ***Malicious program:*** It is the most common type of electronic crime against information systems. This crime happens when computer viruses are sent through the Internet. These viruses affect the computer and deactivating programs or maybe even causing the computer to crash and become unusable. Malicious software has to turn into the most common harmful software that affecting computers in many aspects because thousands of malicious software are now available such as Monkey, Chernobyl, and code red[9].
- ***Sniffing and Spoofing:*** Sniffing can take one of two procedures: Software which is downloaded onto a computer, or physical in which a sniffing device is located on the computer at the Ethernet port. spoofing also know as "phishing" this threat is very harmful because it is masked with emails and web sites. Spoofers are creating false web sites on the internet to collect personal information then using this information in unethical actions. [10]

3 Discussion

There is no doubt that personal data may not be handled without personal consent or it can be done under a lawful basis by a specific regulation. Individuals need to law or regulation for protecting their private data. In general, protecting personal information within information systems in e-government requires three measures which are Legal Procedures, Organizational Procedures, and Technical Procedures. Law procedures associated with government regulations which are more general and executable in all government organization within the government authority while Organization procedures related to self-regulation that developed by the organizations itself in accordance which supplements government regulations. Besides law procedures, self-regulation sometimes relays on international privacy principles. Implementing self-regulation needs active compliance actions and enforcement mechanisms so the user can believe that the organizations are acting by the rules. Technical procedures are some technical measures for protecting and safeguarding personal information within information systems. It is irrelevant to hardware and software solutions. In Europe, there is a regulation in Europe law which is called the General Data Protection Regulation (GDPR). Individuals in European Union countries and European Economic Area control their data by GDPR inside the EU and during transfer to the outside of the EU. GDPR applies to any organization work in the EEA. As well as, in Europe, there is a regulation on electronic identification and trust services for electronic transactions in the European internal market which called eIDAS (Electronic Identification, Authentication, and Trust Services). It was established in 2014.

3.1 GDPR

The provisions and requirements in GDPR associated with processing personal data. Enterprises and business processes within EEA, that deal with personal data,

must consider principles of protecting personal data. GDPR has many provisions that impose data processors to consider a safeguard of personal data. In case of violating of GDPR provisions, the violator penalizing with money. GDPR contains eleven chapters which are about provisions, principles, rights of the data subjects, transfer of private data to a third party, responsibilities of data controllers or processors, etc. All provisions apply to data subjects, data controllers, or processors founded in the European area but they are not applying on personal or household activities. Article 4 in the GDPR state that "personal data is information that relates to an identified or identifiable individual" this means that any information that processes must take into consideration because it belongs to an individual. GDPR allows personal data to be processed based on some law statements such as if the data owner has consented on processing his/her data. These lawful processes are stated in Article 6 and they have described all saturations in detail. On the other hand, the data owner has the right to withdraw his/her consent on processing data at any time. Article 12 states that the data controller should offer information to the data owners in a transparent and easily accessible method. Data controllers do not have the right to prevent data owners from transferring their data from an electronic system into another[11]. They also have the right to request the deletion of his/her data as stated in Article 17. In case of having risk on personal data, data controllers must inform a supervisory authority without delay as they are available in each state in the European Union. As well as, data owners must be informed if a high risk available on their data as it is required from Article 33. Otherwise, GDPR has many sanctions for those who not obey its provisions. Thus, GDPR has a great effect on increasing trust between e-government and citizens. Even its positive roles encourage countries from outside of Europe to follow its privacy principles in protecting personal information. [12], [13]

3.2 eIDAS

Electronic Identification, Authentication, and Trust Services is an EU regulation that was established in EU Regulation 910/2014 in 2014 on electronic identification and trust services for electronic transactions in the European Single Market. The main mission of eIDAS is controlling electronic signatures, electronic dealings, and other transactions to deliver a safe method for users to do online businesses. It makes participants and receivers obtain more security and suitability. By eIDAS users perform transactions among countries more easily without depending on traditional ways like email or using documents. There are some standards in eIDAS which work the same legal standing as available for a paper transaction. The standards considered electronic signatures, qualified digital certificates, electronic closures. Visions of eIDAS are interoperability and transparency since it requires EU states to have a shared agenda to recognize electronic IDs from other member states and it provides users with an accessible and clear list of trusted electronic services. Article 4 in eIDAS is about data processing and protection which states that personal data can be processed in accord with Directive 95/46/EC and it allows to use of pseudonyms in electronic transactions in a condition of not contradicted with law. Directive 95/46/EC is a Data Protection Directive applies in EU states which regulates how to collect and process personal data in European countries. As the electronic transaction is part of e-government services, providing security for such kind of transaction leads to increase

confidentiality between citizens and e-services that offer be a government. Hence, eIDAS has a crucial character in using e-government services in EU countries. [14]

3.3 Technical Procedures

This section aims to show technical solutions for such kind of threats described in section 2. However, there is a law for punishing for computer crimes but it is hard to enforce therefore security and protection against risks technically should take into consideration. As we understood that spammers could send a huge number of unwelcomed emails to computer users at a very cheap price and it has many types. The most common type of spamming is called Spambot. This type of spam depends on email addresses and hyperlinks on any web page. It scans pages for these two factors, it stores the email addresses to use as a spam target and follow the hyperlinks to find new pages and process again for the email addresses. According to [16] Spam might bait computer users into revealing personal information such as social security numbers and credit cards. Spammers use text messages to ask about the user's password, account details, and personal details while such kind of information is rarely requested by real organizations like a bank. The problem of spamming is currently solved by providing offers against spamming emails from internet service providers. Moreover, there is various technic recently invented to prevent spamming such as Machine Learning-based Spam filtering, Blacklist, Real-Time Blackhole List, List-Based Filters, Whitelist, Greylist. Each of these technics depends on a specific policy and methodology. Besides, as spambots focusing on email addresses, therefore, the email address should be hidden from spammers. There are numerous methods to hide email address form these Spambots, the easiest and best way is a trick that should be done with an email address. The trick is to leave email visible to a human visitor but hidden from the spambots by simply show email address in graphic not in written style. Thus, email addresses are safe from Spammers since Spambots are unable to read graphics.

As stated by [17] hackers could steal personal information by hacking into organizations' sites. This is usually obtained by getting access to the organization's database which may carry much personal information. Hence, the hacker uses this personal information into attack personal accounts. For instance, by knowing the email address of a user, hackers may try to reveal the password of that account by using other personal information that revealed from the database such name of children, date of birthday and other information. Some defensive measures can be taken by managers or end-users. On such a defensive measure, a Firewall is a platform used to carefully monitor exactly what information permits in and out of a computer or information system.

Malicious software can worm computer systems and disable parts or entire systems. For avoiding information systems from malicious software, many programs are developed to deal with them which are called antivirus. Various type of antiviruses nowadays is available. Therefore, computers in information systems should schedule to scan the entire computer systems every day frequently. Since malicious software upgrades, antiviruses should update whenever their new version coming. The most recently developed software for removing Malicious software is Microsoft's program which called Malicious Software Removal Tool. This tool works perfectly on scanning and preventing most of the malicious software such as Viruses, Worms, and Trojan Horses. [18]

On the other hand, for capturing and preventing Sniffing, a sophisticated tool recently designed by the FBI for this purpose Carnivore Software. This software can act strongly on monitoring emails and electronic communications. The simple and easiest way to avoid Spoofing is avoiding yourself from entering personal information on unknows websites since it is very difficult to recognize false websites. [19] As well as, many examples of spoofing can be banned by firewalls and routers.

Conclusion

With the growing use of the internet in technology systems, the rate of attacks on personal data and information systems in e-governments are increased. Therefore, designing and developing any kind of information system security of that system should take into consideration particularly those parts which have critical data like personal information. Usually, electronic systems will not have a long life without security protection that is why security levels should pay attention to organizations. On the other hand, the personal need for a law or regulation for protecting their private data. In Europe, there is a regulation in Europe law which is called the General Data Protection Regulation (GDPR) which obligates all europian governments to protect their people data. This regulation has many advantages for e-governments in Europe since it increased citizen's trust in the government's electronic services. Besides, eIDAS also has a role in safeguard electronic transactions. Although, security technics protect personal data but still threatens are available all the time. Therefore, vulnerable within a system leads to open a gate with the attacker to attack the system and manipulate with personal data. The threatens which are shown in this research are the most common types of virus or electronic crimes that face information systems and individuals. For example, some of these threats embrace spamming, hacking, jamming, malicious software, sniffing, and spoofing. Currently, there is a various solution for these threats. As it is stated in section 3.3, Internet Service Providers can play their role in banning spams. As well as, some particular machines can use against spammers. For hacking issues, computer farewells have an important role in preventing unlawful access to information systems. But malicious programs and sniffing problems can solve by antiviruses and security measures.

References

[1] Shareef, M., Enhancing Security of Information in E-Government. In: *Journal of Emerging Trends in Computing and Information Sciences*,2016, vol. 7, no. 3, pp. 139–146.

[2] Athina, L., *Virtual communities, social networks and collaboration*. Sparti:Springer, 2012.

[3] Costas, L., Stefanos, G., Fredj, D., Gunther, P. Pernul. Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy. In: *Computer communications*, 2003,vol. 26, no. 16, pp. 1873–1883.

[4] Abdulrahman, A. Privacy and eGovernment in Saudi Arabia. In: *World Congress on Engineering and Computer Science*, 2015, vol. 2, pp. 21–24.

[5] Mohammed, A., Seifedine, K. E-Government: Latest Trend and Future Perspective The Iraq Case. In: *Editors-in-Chief*, 2013, p. 307.

[6] Silverio, H., Jesus, D. Indicators of urban sustainability in Mexico. In: *Theoretical and Empirical Researches in Urban Management*, 2010, vol. 5, no. 7, pp. 46–60.

[7] Shi-Cho, C., Kuo-Hui, Y. A data-driven security risk assessment scheme for personal data protection. In: *IEEE Access*, 2018, vol. 6, pp. 50510–50517.

[8] Yinglian, X., Fang, Y., Knnan, A., Rina, P., Geoff, H., Ivan, O. Spamming botnets: signatures and characteristics. In: *ACM SIGCOMM Computer Communication Review*,2008, vol. 38, no. 4, pp. 171–182.

[9] Said, K., Roman, J. *Security of information systems*. Zlin: Tomas Bata University, 2015.

[10] Marc, L., Roger, J., Mina, L., Raghunandan, R., Vuk, M., Jeffrey, R. LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation. In: *IEEE Communications Magazine*, 2016, vol. 54, no. 4, pp. 54–61.

[11] Jona, B, Ine, Z., Jo, P., Rob, H. The Social Construction of Personal Data Protection in Smart Cities. In: *CTTE-FITCE: Smart Cities \& Information and Communication Technology (CTTE-FITCE)*, 2019, pp. 1–6.

[12] Paul, V., Axel, B. The eu general data protection regulation (gdpr). In: *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, 2017.

[13] Daniel, S., Jos, H. Evaluation of the usability of a new ITG instrument to measure hard and soft governance maturity. In: *Governance, governmentality and project performance: the role of sovereignty*, 2019, vol. 7, no. 2, pp. 37–58.

[14] Colette, C., Jessica, S. eIDAS as guideline for the development of a pan European eID framework in FutureID. 2014.

[15] Ludek, L., Martin, H. Resilience as main part of protection of critical infrastructure. In: *INTERNATIONAL JOURNAL OF MATHEMATICAL MODELS AND METHODS IN APPLIED SCIENCES*, 2011, vol5, issue 6, p1135-1142.

[16] NortonLifeLock, 2020. *Dealing with spam text messages and unwanted calls.* [on line] [cit 5-1-2020] available from: https://us.norton.com/internetsecurity-how-to-deal-with- spam-textmessages.html.

[17] Cohen, M., 2020. How to Protect Your Personal Information from Hackers. [on line] [cit 20-12-2019] avaible from:: https://eccitsolutions.com/protectpersonal-inormation-hackers.

[18] Liu, R. Fingerprint-Based Detection and Diagnosis of Malicious Programs in Hardware. In: *IEEE Transactions on Reliability*, 2015.

[19] Marc, L., Roger, J., Mina, L., Raghunandan, R., Vuk, M., Jeffrey, R. 5G NR Jamming, Spoofing, and Sniffing:Threat Assessment and Mitigation. In: *IEEE International Conference on Communications Workshops*, 2018

Autors:

[1]**Hemin Muhammad –** Faculty of Applied Informatics, Tomas Bata University in Zlin, Nad Stráněmi 4511, 760 05, Zlin, Czech Repulic, email: muhammad@utb.cz

[2]**Ludek Lukas –** Faculty of Applied Informatics, Tomas Bata University, Nad Stráněmi 4511, 760 05, Zlin, Czech Repulic, email: lukas@utb.cz