Security issues in healthcare IT systems

Zsolt Szabó

Óbuda University, Doctoral School on Safety and Security Sciences, Népszínház utca 8., H-1081, Budapest, Hungary

Abstract: Nowadays IT systems are essential for the safe, efficient and reliable operation of organizations. Health information technology (e-Health) increasingly becomes an integral part of the services. Doctors, nurses, and other therapists spend more and more time on the computer, using family medicine, specialist care, or integrated hospital systems. Today, it is difficult to imagine health care or the operation of the insurance system without the proper records and computer tools, but modern diagnostic tools can also be considered IT tools with a little exaggeration. The purpose of the article is to highlight the security problems and shortcomings of health IT systems, and medical equipment. We also seek solutions for protection and examine their applicability using international and national regulations (GDPR, Act L of 2013, Act CLXVI. of 2012), recommendations and standards related to the operation of health information systems (CEN, MITS, HL7, IHE, HS).

Keywords: e-Health; data protection and information protection; Advanced Persistent Threat (APT), GDPR

1 Introduction

Health information technology (e-Health) increasingly becomes an integral part of the services (Fig. 1). Today, it is difficult to imagine health care or the operation of the insurance system without the proper records and computer tools, but modern diagnostic tools can also be considered IT tools with a little exaggeration [1]. Doctors, nurses, and other therapists spend more and more time on the computer, using family medicine, specialist care, or integrated hospital systems. Data handled during health care activities mostly belong to the category of special data, whose handling is governed by strict rules [2]. Below, we focus on the problems of health information technology we deem most important. We think that a solution to these problems provides a sound foundation for the creation of a high level of IT background necessary for a high standard of health care. We detail the issues of protecting health care data and Hungarian specialities. It is not easy to find one's way in the maze of laws, regulations and guides. Not knowing them, however, does not absolve anyone of responsibility. This study summarises the most important information in international recommendations, standards, and

laws, and provides useful practical advice for the safe and lawful handling of health care data.

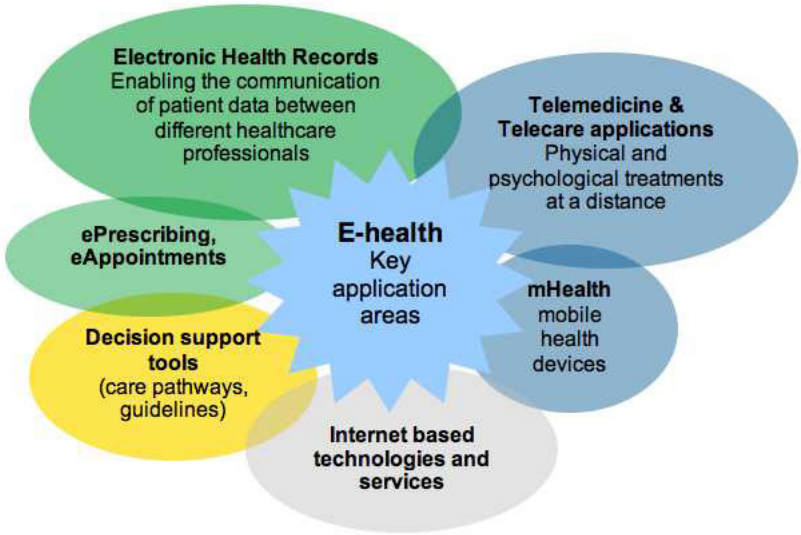

Figure 1
e-Health application areas

2 Attacks against health information services

A cyberattack is an offensive or defensive operation whose expected outcome is personal injury or death, or material loss or destruction [3]. A cyberattack was launched against the British health care system on Friday 12 May, 2017. According to the report of the British National Health Service (NHS Digital), some hospitals in 19 areas, including London, Blackburn, Nottingham, Liverpool and Manchester were attacked, but the media reported similar problems in 40 different areas. In most of the hospitals affected, the telephone service and computer systems faltered. In these hospitals they suspended accepting patients with non-emergency problems [4]. According to NHS Digital, it was a ransomware attack: the writers of the virus demanded money from the hospitals to return access to files the virus encrypted. Some hospitals reported that messages appeared on the infected computers demanding 300 dollars' worth of bitcoin, a cryptocurrency. NHS Digital's investigations revealed that it was probably the Wanna Decryptor virus variant. Many hospitals stopped their own IT systems to protect their databases themselves from attacks. Many GPs reported that they could not access the electronically stored data of their patients, including test

results. According to the NHS, there were no signs that the attackers were able to access personal data of patients. The Portuguese National Commission for Data Protection (Comissão Nacional de Proteção de Dados, CNPD) fined the Barreiro hospital in Portugal for allowing illegal access to patient data, reported the Portuguese Publico on 22 October, 2018 [5]. CNPD started the investigation in the middle of July, as a result of which they decided on a fine of 400 ezer Euros. The fine consists of several parts as various sections of the General Data Protection Regulation of the EU (GDPR) [6] were violated. The Portuguese hospital stored the data of the patients in its own system but did not handle access properly according to the CNPD. As a result, at least nine persons gained access to the data, who had no medical qualification whatsoever, such as social workers. Also, a total of 985 users registered as registered medical doctors in the system, when there are only 296 doctors in the hospital. In addition, the hospital did not separate its own patient data properly from the archived data of other hospitals, and authentication during access to the was not adequate. The CNPD stated that the hospital did not do anything to stop unauthorised access, and did not differentiate between groups, who, for example were only allowed access to the data under certain conditions. The further 100 thousand Euro fine was imposed because according to the CNPD, the data handler cannot guarantee integrity and confidentiality within its system in general.

3 Data and information protection solutions

The use of IT in health care (Fig. 2) became a factor of medicine. Medical informatics emerged as a special area and became an essential factor of medical services. A knowledge of the regulation of and ways of implementing information security is important, since the unprofessional handling of medical data can lead to serious problens [2]. The General Data Protection Regulation (GDRP) of the EU came into force in May 2016 [6]. It updated data protection regulation after more than two decades. The regulation started to be enforced after a grace period of two years, on 25 May, 2018. Its purpose is to unite the fragmented data protection regulation existing earlier, therefore it is directly enforced in every member state, including Hungary. The goal is to give people more control over their data and provide stronger protection of data against not only cybercriminals but also companies and intitutions handling the data. Attacks are basically directed to data, which is surrounded by system elements and handled by processes [7]. Cyberthreats threaten data and data handling processes through a chain of system elements. Protection does not only mean implementing a system of tools but the complete system of protection of a system from designing to implementation, including the physical (operation), logic (password generation, cryptography methods, compatibility matrix etc.) administrative (regulation background) and human resources [8]. One of the most important assets of the economy and society

is information. Information is essential for every economic entity, whether it be public or private. There is no development without information; without it nothing can be planned, which results in falling behind [9].

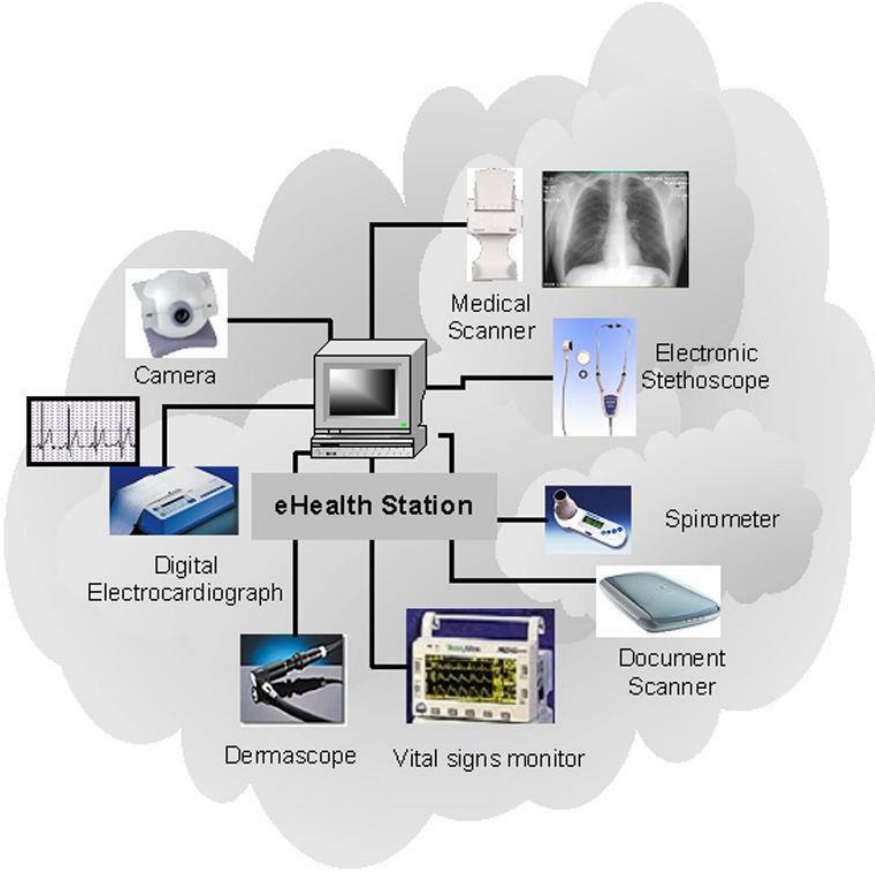

Figure 2
e-Health station

Information security means that the IT components of organisational activities are maintained in an adequate state [10]. Security is an essential element of the operation of an organisation [11], and in the case of health IT systems, it is as important as organisational conditions. Organisational security is a complex concept—the individual subfields are closely related and depend on each other. The following areas need to be taken into account in planning and design: physical security, object protection; data and information security; business security; human security; incident handling and business continuity. Taking into account the above, security has to be closed, comprehensive, proportional to the risks and continuous [12]. The security management of an organisation should be

centralised, uniform, clear, supported by IT tools, and as automated as possible, leaving as little possibility for human error as possible. The information security law [13] requires that the IT systems of state organisations have to be able to detect, log and automatically handle critical security events of hardware and software that is essential for the operation of the organisation. When the security management of a state organisation is designed, it is also important that the security system reflects the security policy of the organisation. The security management should organically include network, user, and firewall management, content filtering and virus protection of the mailing system and other IT systems.

4 Targeted attack of health IT systems

Nowadays the state and its organisations and citizens depend on very complex electronic information systems (Fig. 3) in Hungary's cyberspace, without which the state cannot operate, and services cannot be provided and used. Society is not prepared to operate without this infrastructure, these tools and services therefore they need to be protected. Also, the information and data generated and used during their operation constitute considerable wealth.

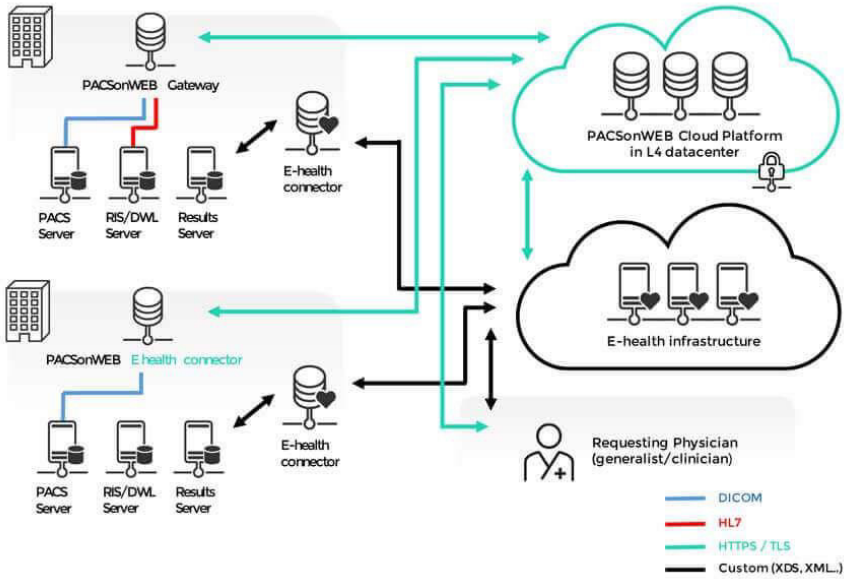

Figure 3
e-Health integration

Based on the above, a possible definition of critical infrastructure is the following: a network of connected and interactive (mutually depending on each other) infrastructure elements, facilities, services, systems and processes, which are essential for the operation of a country and have a fundamental role in providing a minimum level of security, economic operability, public health and environment as expected by society [14]. Targeted Attacks are threats specially directed against a given person or organisation. As opposed to computer viruses, the creator of the malware does not wish to spread the malware as widely as possible, but intends to install it on the devices of the target. Targeted attacks are combinations of simpler attacks (attacks through the web or mail, the attack of a system) but require very deep knowledge of IT systems, since they have to be invisible as well, and also, they are usually directed against systems wich are well-protected.

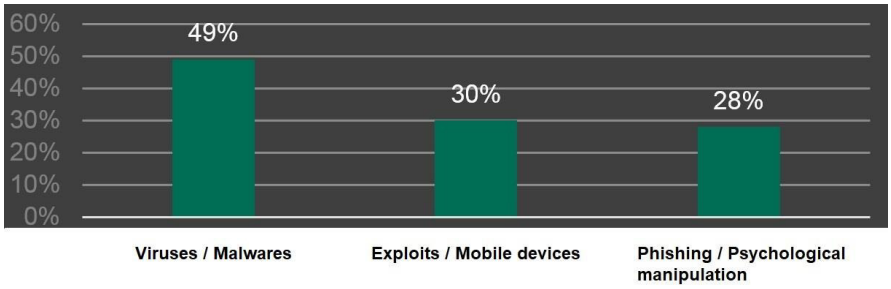

Figure 4
Main methods of Advanced Persistent Threats

Advanced Persistent Threats (APT) require very great expertise. They are usually carried out by professionals, mostly employed by intelligence agencies or criminal organisations. They are also directed to one target, and steal data from it [15]. Advanced Persistent Threats differ from normal cyberattacks in the selection of the target, the duration of the attack and the initial inactivity period These attackes use Social Engineering (psychological) attacks. Advanced Persistent Threats have been growing in number in the past few years and the tendency seems to be continuous. APTNotes, a data bank created and maintained by GitHub (https://github.com/kbandla/APTnotes) has been collecting published reports about APTs since 2008. Fig. 5 shows that the number of these attacks has increased considerable in the past few years. However, these were only the reported incidents - there have probably been a great number of undiscovered attacks as well. In August 2015, they collected a total of 291 APTs against companies, institutions and governments. Of these, 72 were observed in 2015, which is more than twice the amount in the same period in 2014, and similar to the amount experienced in the second half of 2014. Most APTs are directed against financial and business organisations but sometimes political motivations can also be suspected. A worrying trend is the increasing number of attacks against medical data. Nowadays most IT attacks are experienced at the application level.

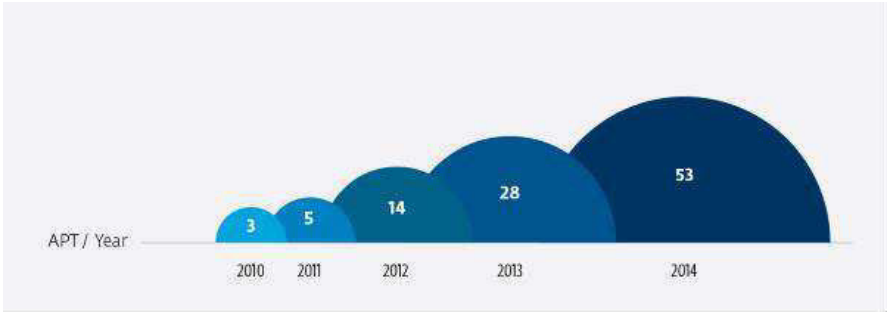

Figure 5
Reports of APTs

At the lower levels of Fig. 3, sophisticated defence solutions are available which protect against attacks effectively but not necessarily fully. Among applications, services accessible through the web are most popular. Nowadays this affects certain portal engines but some tools are already available which detect vulnerabilities of web services. The above-mentioned international incidents indicate that such attacks may also be directed against Hungary's health information systems in the future, and therefore they need to be prepared for with the help of national and international standards (CEN, MITS, HL7, IHE, HS), recommendations and good practices, and reinforce IT systems [16].

Conclusions

We presented two important data and information security issues of health information systems, focusing on international comparison and tasks in Hungary. We could not strive for comprehensiveness in the framework of this article as each subfield would require independent analysis and strategic planning. In our opinion, the most important tasks are:

– Grading the systems used in the management of institutions and in providing health care.

– Applying the standards for the storage and transmission of medical data.

– Ensuring that the central databases are authentic and up-to-date.

– Electronic identification of patients and doctors/medical staff.

– Publishing a collection of medical data and information protection regulatons, and providing information security awareness training for users.

References

[1] P. Racskó, Health Informatics abroad and in Hungary. Health Economics Review 6/2008. pp. 26-31

[2] J. Ködmön, E. Z. Csajbók, Information Security in Healthcare, Medical Weekly, 2015, 156(27), pp. 1075–1080

[3] Tallinn Manual on the International Law Applicable to Cyber Operations, General editor Michael N. Schmitt, US Naval War College, Cambridge University Press 2013, rule 30, pp. 1-255

[4] The Guardian Massive ransomware cyber-attack hits nearly 100 countries around the world, Last accessed September 2018. [Online]. Available: https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs

[5] Publico Hospital do Barreiro contesta judicialmente coima de 400 mil euros de Comissão de Dados, Last accessed October 2018. [Online]. Available: https://www.publico.pt/2018/10/22/sociedade/noticia/hospital-barreiro-contesta-judicialmente-coima-400-mil-euros-comissao-dados-1848479

[6] 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). Brussels, Official Journal of the European Union 119/1 05/04/2016. (EN) pp. 1-88

[7] Z. Nyikes, Z. Németh, A. Kerti, "The electronic information security aspects of the administration system," 2016 IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI), Timisoara, DOI:10.1109/SACI.2016.7507395, 2016, pp. 327-332

[8] Zs. Szabó, Cybersecurity issues of pension payments, Anikó Szakál (ed.) IEEE 15th International Symposium on Intelligent Systems and Informatics: SISY 2017. Szabadka, Szerbia, 14-16/09/2017, New York: IEEE, 2017. pp. 289-292

[9] Á. Csiszárik - Kocsir, J. Varga, Crisis - Project - Risk: According to the Opinions of Hungarian SMES', Project Management Development - Practice and Perspectives: Sixth International Scientific Conference on Project Management in the Baltic Countries.2017. pp. 60-70

[10] P. Michelberger, Cs. Lábodi, After Information Security – Before a Paradigm Change: A complex Enterprise Security Model, Acta Polytechnica Hungarica 9:(4), 2012, pp. 101-116

[11] D. Csubák, K. Szücs, P. Vörös, A. Kiss, Big Data Testbed for Network Attack Detection, Acta Polytechnica Hungarica Volume 13 Issue Number 2 2016. DOI: 10.12700/APH.13.2.2016.2.3. pp. 47-57

[12] Zs. Szabó, Options of micro-simulation in the modelling of the pension system and the intelligent IT security system, Computational Intelligence and Informatics (CINTI), 2016 IEEE 17th International Symposium on

Óbudai University 17-19. Nov. 2016, Conference book, DOI: 10.1109/CINTI.2016.7846421. 2017, pp. 295 -298

[13] Act LX of 2013 on the Safety of Electronic Information Systems of Public and Local Government Offices (Ibtv.). Hungarian Bulletin No 68 of 2013, pp. 50241-50255

[14] Z. Rajnai, B. Puskas, Requirements of the Installation of the Critical Informational Infrastructure and its Management, Interdisciplinary Description of Complex Systems 13: (1) pp. 48-56

[15] Zs. Szabó, Cybersecurity issues in industrial control systems, Anikó Szakál (ed.) IEEE 16th International Symposium on Intelligent Systems and Informatics: SISY 2018. Szabadka, Szerbia, 13-15/09/2018, Budapest: IEEE Hungary Section, 2018. pp. 231-234

[16] P. Simon, Information management theory and practice in health care, Semmelweis University 2014, Last accessed November 2018. [Online]. Available: https://www.tankonyvtar.hu/hu/tartalom/tamop412A/2011_0015_informaciokezeles_elmelet/html/block-11714-page-2.html