II. COMMENTARIES

„Ante Portas – Security Studies”
2021, No 2(17)
DOI: 10.33674/220219

Cosmin Florin BIRTA[1]
Romania

CYBER RISKS AND THREATS FOR E-HEALTH PORTALS. A ROMANIAN APPROACH

Abstract:
Cyberspace is a platform for interaction at the level of society, being highlighted by major benefits visible in several sectors of activity, such as: supporting policies and promoting national interests, developing and supporting the business environment and the medical services industry, increasing the quality of life, raising the level of knowledge and predictive capacity in order to prevent risks and threats to national security, developing technical capabilities and skills of human resources in order to achieve national security objectives.

Keywords:
Cyberthreats, e-health, e-health portals, Romania

Types of attacks aimed at stealing data or information, encrypting data, blocking access to services, unauthorized access, manipulation, interruption or destruction of data and information. The risks to which users who ‘enter’ cyberspace are exposed generate ongoing challenges that require a series of actions and responses accompanied by vigilance and long-term investments.

Counteracting cyber aggression by working together can be an effective cyber security system: for the state, companies or public institutions and users. The state can contribute by ensuring an appropriate legislative framework to ensure information security, companies or public institutions must provide

[1] Cosmin Florin Birta, PhD. Mihai Viteazul National Intelligence Academy, Romania.

methodologies, procedures and investments in technical solutions to ensure security, and users must be concerned with information and self-training in the field because they can be both risks as well as a factor of protection of the infrastructure in which it operates.

In this context, the security challenges of e-Health portals also lie in the fact that the data and information stored here are some of the most sensitive, which must be very well protected and at the same time easily accessible. Designing an e-Health portal is a challenge due to specific requirements and functionalities, because the complexity of integrating e-Health services, which are implemented using different technologies, will make it difficult to provide new services at the request of users.

E-Health portals provide healthcare providers with a single point of access to their patients' digital health information. Healthcare providers can thus access laboratory results, images of radiological investigations, diagnostic information, medication data, medical history and other information related to patients' health, thus giving them a complete picture of their health, which brings added value to caring decisions.

The medical services industry is undergoing a major evolution in the information age, as most of the medical records of patients have moved to the online environment, and medical professionals are realizing the benefits of smart medical devices. However, the more the healthcare industry adapts to the digital age, the more often there are concerns about threats to the confidentiality, safety and security of the medical data transmitted.

In the case of e-Health portals, which are at the intersection of medical informatics, public health and business, they are a major target for hackers because they contain very sensitive information, while current cyber security solutions for e-Health portals protect only certain security levels.

The widespread use of security tools and advanced technology provides the infrastructure needed to create modern and reliable security solutions in the field of e-Health portals. The problem that arises is that connecting together the right security tools to ensure overall security without affecting the performance of the portal and user productivity is difficult and requires special configuration. There is little research exploring the relationship between medical data confidentiality and cyber security. Precisely for this reason, this paper explores the risks and vulnerabilities of e-Health web portals, that is, to the security of medical data and information that are shared online.

For this reason, in this paper, an important emphasis will be placed on the challenges represented by the hostilities in cyberspace from an academic, strategic and legal perspective looking for the answers to the following questions:

- Do existing theories provide sufficient answers to the current challenges posed by cybercrime conflicts, and if not, could alternative approaches be developed?

- How do states and non-state actors use cyber weapons when pursuing strategic and political goals?
- How does the emergence of conflicts in cyberspace pose a challenge to the current legal framework?

The conceptual framework will help us to better understand:

- conceptual delimitation of IT portals for citizens' health management, institutional analysis of the place and role of institutions empowered to ensure the security of e-Health IT portals;
- identification of threats and vulnerabilities to the security of e-Health IT portals, - analysis of the impact of attacks on e-Health IT portals, related to the need for the protection and confidentiality of medical data;
- transforming the lessons learned by experts in the field into constituent elements of a strategy to prevent risks and vulnerabilities and counter threats to e-Health IT portals;
- identifying tools and methods to prevent and counter cyber-attacks on e-Health portals, for the next generation of cybersecurity systems, to increase the capacity of e-Health portal specialists and administrators to counteract the actions of malicious actors;
- identifying the current limitations of cyber security solutions for e-Health portals and proposing next-generation cyber security solutions for this type of portals.

In our case, we aim to validate the following research hypothesis: The more e-Health portals are integrated into the development of the medical act, the greater need to operationalize a culture of security of the personnel with attributions in the use of these portals.

This is necessary because e-Health portals increase efficiency and add value to healthcare by avoiding misdiagnosis and unnecessary therapeutic interventions[2], supporting the continuity of medical practice, improving communication between medical institutions and by expanding access to evidence-based human health knowledge, thus reducing the gap that exists between health professionals and patients.

The question for cybersecurity professionals is: How can I protect the e-Health IT portals of institutions and organizations from appearing on hackers' victim lists? Thus, the better known the possible threats and vulnerabilities to e-Health IT portals, the more effective will be the strategies developed by experts in order to protect them.

[2] M. Hough, *Reducing Misdiagnosis: Healthcare Technology Set To Save Thousands Of Lives And Billions Of Dollars*, <https://www.healthitoutcomes.com/doc/reducing-misdiagnosis-healthcare-technology-set-to-save-thousands-of-lives-and-billions-of-dollars-0001> (30.11.2021).

For my work, I chose a qualitative research method to identify cyber threats to e-Health portals, respectively the solutions to prevent and counter them. Researchers use qualitative methods to explore real situations, understand a phenomenon, identify the meaning of events, answer questions or capture descriptions of human experiences. The respondents were selected among institutions or companies with attributions in the field of cyber security.

In order to establish the most important aspects that should be taken into account in order to streamline the means and methods of preventing and combating cyber risks and threats to e-Health portals, we interviewed a number of twenty cybersecurity experts from institutions or companies with responsibilities in the field, as follows: cybersecurity experts from institutions with responsibilities in the field of defence, public order and national security, researchers from research institutes in the field of cybersecurity, workers in private companies with activity in the field of cyber security, as well as IT experts from institutions/companies with the object of activity in the medical field.

We asked the following twelve questions:

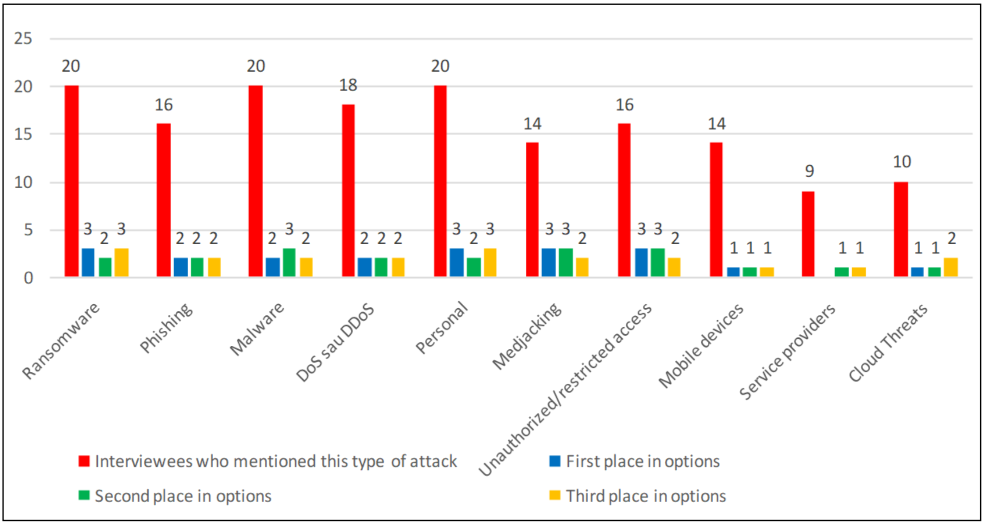
1) What types of actors involved in cyber aggression do you know?
2) What types of cyber-attacks do you know?
3) What do you think are the most used methods for a cyber-attack?
4) What are the most used methods of protection and counteraction in the event of a cyber-attack?
5) What types of cyber-attacks have affected Romania and who was at their origin?
6) What measures did Romania use to prevent and respond to cyber-attacks?
7) What types of IT portals do you know and what are their benefits?
8) What cyber threats to computer portals do you know/can you imagine?
9) What differences can you identify between e-Health portals and other types of IT portals?
10) What cyber threats do you know/imagine about e-Health portals?
11) What cyber-attacks on e-Health portals in Romania do you know / can you imagine?
12) What methods of preventing and counteracting cyber-attacks on e-Health portals in Romania do you know/propose?

One of the biggest threats to the cyber security of e-Health portals mentioned by the respondents is the medical staff (users), or rather the lack of adequate education on the cyber security of the medical staff. It all comes down to cybersecurity education - do all employees know how to identify and prevent phishing attacks, ransomware attacks or malware attacks? Well, you should! Managers need to ensure that the organization has a cybersecurity strategy and policy that is not only well understood, but fully followed and implemented.

Another category of threats mentioned by respondents is providers. Healthcare providers often work with other providers without properly assessing the risk. Unauthorized personnel can easily access computers that are not in restricted areas. If these open computers have access to sensitive patient information, unauthorized staff or others in the area can quickly find harmful information. In other cases, successful phishing attempts on general-purpose computers provide a gateway for hackers to more sensitive areas of the network.

When asked what cyber threats to e-health portals do you know/can you imagine? the answers given by the respondents were as per the chart below.

Figure 1. Types of cyber threats to e-Health portals



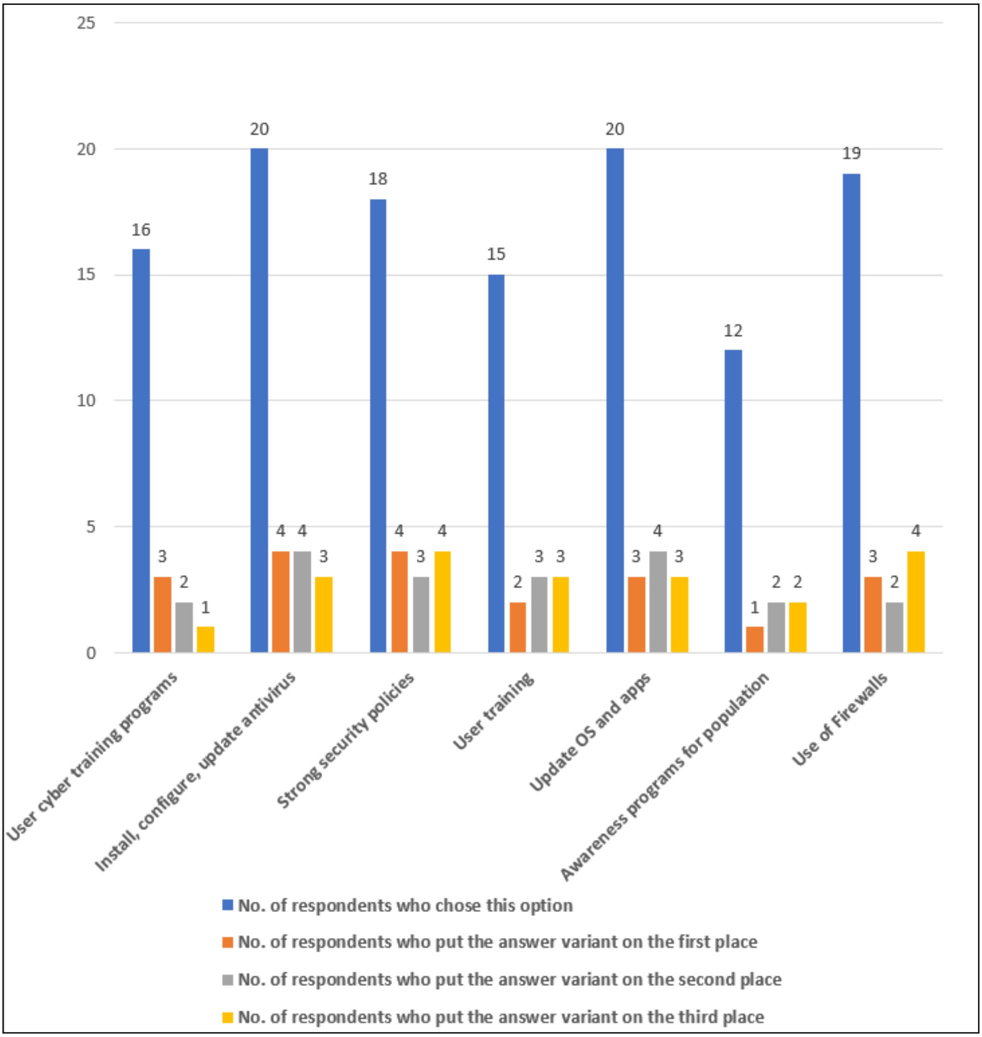
Source: own studies.

Unfortunately, many reports show that employees are the weakest link in an organization's security defence. Organizations must make security a priority and conduct frequent employee training. Often, most security budgets tend to be spent on technology-centric solutions, but institutions and companies need to pay more attention to the human side of security.

When it comes to medical devices, respondents said their security is often lacking, making them easy targets for hackers. As the Internet of Medical Things (IoMT) continues to grow, these devices are designed to export information to external sources and interact with the world outside the medical office. This data could be intercepted or manipulated, creating a number of problems. Furthermore, hackers could gain access to manage most devices connected to the network, including how they operate.

Regarding the question: What methods of preventing and countering cyber-attacks against e-Health portals do you know/propose? the answers resulted somehow normally from those received to the previous question, that is, depending on the possible types of attacks, we implement measures to prevent and counter them.

Figure 2. Measures to prevent and counter-attacks on e-Health portals.



Source: won studies.

Respondents highlighted the fact that although efficient firewalls and other means of defence are used, the human factor remains a weak link that needs to be trained. To minimize human error, system administrators must constantly remind all staff about risky behaviour. This can include anything from downloading unauthorized software and creating weak passwords to visiting malicious websites or using infected devices.

Another option of the interviewees was strong security policies: high complexity passwords to be changed no more than 30 days, creating different groups of users with different privileges, setting custom access ranges where possible, authentication with more many factors, etc.

The greater the number of people using e-Health IT portals (medical, administrative, patient, etc.) who are trained to use them, and complying with the cyber security rules applicable to these portals, the lower the risk of exploiting vulnerabilities.

Academics can help meet the growing need for cybersecurity by training the next generation of cyber defenders, and it is crucial that such training programs be designed to prepare students for this type of fieldwork. Unfortunately, the collection of data on cybersecurity is hampered in some cases where cybersecurity professionals feel uncomfortable with traditional methods of human factor analysis.

Regarding the e-Health portals in Romania, the respondents mentioned that medical institutions allow the mobile connection of both medical staff and patients and do not always require that the devices comply with security standards. This leaves their networks vulnerable to malware and hackers, as not all of the organization's plans and security also cover staff communication devices. This problem is exacerbated once staff remove equipment (in the case of upgrades) – network information or passwords may still be accessible, making it a natural access point for criminals.

Respondents also noted that a large number of connected medical devices, with different specifications and from different manufacturers, makes maintaining security particularly difficult for IT professionals – health. While medical devices do not always store significant amounts of patient data, they can be vulnerable entry points for attackers to access data-rich servers. Keeping these entry points up to date and safe must remain a priority for the medical industry, in order to reduce costs and damage through attacks on this type of device.

Regarding the methods of preventing and counteracting cyber-attacks on e-Health portals in Romania, the respondents pointed out that the human factor remains a weak link, which must be trained. To minimize human error, system administrators should constantly remind all staff about risky behaviour. This can include anything from downloading unauthorized software and creating weak passwords to visiting malicious websites or using infected devices.

Along with the use of outdated systems, some users are not trained on cyber security measures. They may not even have the latest and greatest software installed on their computers at home. Without proper training, users do not know what warning signs to look out for. So they are more likely to click on a link asking them to ‘restore access’ to the email platform or appointments than to ask themselves if this is safe or not.

It is also not enough to install various antivirus applications or software. Continuous updates on time are essential to ensure that healthcare systems receive the best possible protection at all times.

Strong security policies should be implemented: high-complexity passwords to be changed no more than 30 days, creating different groups of users with different privileges, setting custom access ranges where possible, multi-factor authentication, etc.

For example, at a hospital, nurses may need to share information with other employees in their unit, but there is no reason for other departments to see this. Visiting physicians can only receive access to information about their patients. Security settings should also monitor unauthorized access or access attempts at each level and send email or phone alerts to network administrators.

It is important to highlight that the methods of protection against cyber-attacks must start from strong password policies, the use of firewalls, the up-to-date updating of the OS and other software used, the use of licensed antivirus and its permanent update, the creation of backups to methods related to each user's level of training or information/awareness: avoiding pirated software and untrustworthy sites, using maximum caution when browsing the Internet, avoiding revealing passwords or personal information through the internet, rigorously questioning anyone who offers you very cheap or free goods or services on the basis of ‘too good to be true’ or ‘nothing is free’.

Given the formulated research hypothesis, I present the following conclusions. The unprecedented development of IoT technology and the connection to the Internet of various types of objects in our daily lives, such as sensors or various devices (medical devices, appliances, electronics, etc.) increase the risk that they are attacked by exploiting their vulnerabilities. IoT is applied in areas such as smart cities, home monitoring and automation, e-Health, production, energy and utilities, smart grids, smart transportation and traffic management.

E-Health portals include a wide range of web-based interventions, for example, test results, electronic records, e-consultations, telemonitoring and web viewing of medical records. However, e-Health is more than a technology;

it is a different way of working and thinking, and it requires a change in attitude that sometimes goes beyond the boundaries of a health care organization.

As technology evolves and attackers become more skilled, there will be more and more vulnerabilities identified. With technological advances, hackers are becoming more adept at finding holes and cracks in the security systems of institutions or companies and can gain access to protected files and data, which poses a significant threat to cybersecurity.

With the exponential upward progress of technology, the presence of malicious actors and other threats to the cyber security of computer networks is also increasing. Increased awareness and knowledge of the risks and vulnerabilities of technology, both by users and hackers, increase the risks of cyber fraud. In order for individuals, institutions or companies to protect their information in the living space, it is important to take security measures against cyber security breaches.

State institutions and companies shall use a strategic combination of robust IT systems to reduce costs, facilitate secure and easy user access to databases, and increase operational efficiency in order to remain competitive in today's globalized ecosystem. IT portals offer a competitive advantage when it comes to users working remotely in the management of databases, documents, information and other critical processes.

Technology in the field of web portals is evolving rapidly, but so are the risks. The ability to ensure the confidentiality, integrity, access and non-rejection (authenticity of identity) of information provides unique opportunities and risks. As the defence dwindles, cyber threats become more sophisticated, persistent, and more impactful.

Data on healthcare, financial profile, patterns of social behaviour and other types of information are becoming increasingly valuable - either for legitimate businesses interested in targeted marketing or for people who want to illegally obtain services at the expense of another or for criminals who take advantage of the sale of this packaged identity or use it to commit fraud worth millions. All this information can be easily accessed from all types of devices, from traditional desktops and laptops to smartphones, through Internet portals.

Therefore, the massive use of computer portals in everyday life increases the risk that users' data (personal, financial, medical data, etc.) are accessed and used without their consent and to the detriment of malicious actors, which confirms the second hypothesis of the research.

Healthcare organizations are increasingly working with e-Health portals that allow patients to play a more active role in managing their health which affects the interactions between the patient and the healthcare professional. E-Health is more than a technology: it is a different way of working and thinking and requires a change in attitude, which sometimes goes beyond the limits of a health care organization[3].

Although there is an undeniable increase in attacks and breaches of the confidentiality of health data, it is possible for IT professionals to defend themselves against apocalyptic scenarios. IT departments in the field of health must act as if a threat to the e-Health portal is imminent and respond as such – both from internal and external sources. A network is more secure when everyone accessing the network can be identified and tracked.

Mapping the attack surface and marking all entry points and high-risk points can make it easier to continually assess, reassess, and uncover vulnerabilities. Mapping provides an opportunity to take a closer look at how healthcare data is accessed across the network. We may find that many access points (for example, remote access, messaging applications, or VPNs) are not designed for the level of use that their implementation often demands. Our goal is to make the e-Health portal as difficult a target as possible. Most healthcare data breaches are opportunistic in nature. Using rigid security standards and strengthening access portals helps us shut down dangerous opportunities without sacrificing access needed by the business, such as a nurse or professional whose access cannot (and should not) be restricted.

As much as we help employees understand the role they play in cybersecurity and the impact they can have on patients' lives, we will foster an atmosphere in which security is valued and respected. Regular information and communication on the security status of the organization reiterate the organization's emphasis on cyber security. Participating in staff training sessions and turning cybersecurity into a regular topic in meetings could help reduce the risks and threats to e-Health portals.

In this context, I believe that this paper can contribute to the development of cybersecurity in health organizations, in terms of maintaining the balance between identifying risks and vulnerabilities associated with e-Health portals and finding the best and fastest responses to possible attacks on them, without hindering or blocking the access of entitled users to the data and information contained therein.

BIBLIOGRAPHY:

1. Barna C., Birta C.-F., *Revoluția informațională și provocările asigurării securității portalelor e-Health*, “Revista GeoPolitica”, Anul XIX, No. 89-90 (3/2021)

[3] C. Barna, C.-F.Birta, *Revoluția informațională și provocările asigurării securității portalelor e-Health*, „Revista GeoPolitica”, Anul XIX, No. 89-90 (3/2021).

2. Birta C.-F., *Agresiuni Cibernetice ale actorilor statali în era informațională*, “Revista GeoPolitica”, Anul XV, No. 70 (2/2017)
3. Birta C.-F., *Agresiuni Cibernetice ale Chinei împotriva Statelor Unite ale Americii*, “Revista GeoPolitica”, Anul XVI, No. 75 (3/2018)
4. Birta C.-F., *Cum este utilizat internetul de teroriști?*, <https://intelligence.sri.ro/cum-este-utilizat-internetul-de-teroristi/#:~:text=Centrul%20reunit%20pentru%20analiza%20terorismului%20al%20MI5%20a,mare%20dec%C3%A2t%20%C3%AEn%20cazul%20atacurilor%20tradi%C5%A3ionale%20cu%20bomb%C4%83>
5. Briceag V., Bragaru T., Evaluarea riscului securităţii cibernetice, “Economica”, No. 1(115)/2021
6. Hough M., *Reducing Misdiagnosis: Healthcare Technology Set To Save Thousands Of Lives And Billions Of Dollars*, <https://www.healthitoutcomes.com/doc/reducing-misdiagnosis-healthcare-technology-set-to-save -thousands-of-lives-and-billions-of-dollars-0001>
7. Interpol, Cybercrimes cross borders and evolve rapidly, <https://www.interpol.int/Crimes/Cybercrime>
8. *ISO/IEC 27005:2018 Information technology. Security techniques. Information security risk management*, <https://www.iso.org/standard/75281.html>
9. *ISO 31000:2018 Risk management – Guidelines*, <https://www.iso.org/standard/65694.html>
10. New Iranian Espionage Campaign, <https://www.clearskysec.com/wp-content/uploads/2021/08/Siamesekitten.pdf>
11. Passilly T., Tartare M., *The SideWalk may be as dangerous as the CROSSWALK*, <https://www.welivesecurity.com/2021/08/24/sidewalk-may-be-as-dangerous-as-crosswalk/>
12. Threat Intelligence Reports, Cyber Threat Intelligence on Advanced Attack Groups and Technology Vulnerabilities, <https://www.fireeye.com/current-threats/threat-intelligence-reports.html/15GlobalThreatReport.pdf>
13. WannaCry Infecting More Than 300,000 Computers in 150 Countries, <https://www.eyerys.com/articles/timeline/wannacry-infecting-more-230000-computers-99-countries#event-a-href-articles-timeline-namewreck-exposes-hundreds-millions-iot-devices-security-risks039-name-wreck039-exposes-hundreds-of-millions-of-iot-devices-to-security-risks->
14. Vamosi R., *Anonymous hackers take on the Church of Scientology*, <https://www.cnet.com/news/privacy/anonymous-hackers-take-on-the-church-of-scientology/>