Euro Scientist

European science conversations
by the community, for the community

INNOVATION, SCIENCE IN SOCIETY, SPECIAL ISSUE

CYBERSECURITY: AN EU HEALTH CHALLENGE IN THE POST-COVID ERA

5 MAY, 2022 | EUROSCIENTIST | 1 COMMENT

By Vasiliki Michopoulou

In September 2020, during the pandemic, the German press reported the first death due to a cyber attack on the Hospital of Düsseldorf University, which caused great disturbance such as postponement of surgeries, and scheduled medical examinations or chemotherapies. Cybercriminals by using malicious software, so called ransomware, invaded 30 servers of the hospital, crashed the system and forced the staff to turn away patients treated in emergency. A female patient was sent to Wuppertal 35 km away and eventually died due to treatment delay. Nearly a year earlier, Campbell County Health, a medical group in Wyoming USA, with 20 clinics across the state, had also been target for cybercriminals.

According to a World Economic Forum (WEF) report from January 2022, cyber security threats rank among the top risks facing the world (ttps://www.weforum.org/agenda/2022/01/global-risks-report-davos-agenda-2022-leaders-mobilize/), which is confirmed by the FBI statistics (https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic) showing that since March 2020 in USA there has been an "alarming [400% growth] rate of cyber attacks aimed at major corporations, governments, and critical infrastructures."

Europol's latest security report on Internet Organized Crime Threat Assessment (IOCTA 2021) points out that the degree of sophistication of cybercrime has changed significantly, mainly due to the pandemic caused by COVID-19 (https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021). According to the report the ransomware remains at the center of concern, while advanced forms of malware have been widely used, like mobile malware which evolves with criminals trying to circumvent additional security measures such as two-factor authentication. Ransomware affiliate programs enable a larger group of criminals to attack big corporations and public institutions by threatening them with multi-layered extortion methods such as DDoS attacks. The report explains, that due to the rise of efforts to access reliable information and data during the COVID-19 pandemic, phishing attempts that are exploiting the social vulnerability are constantly rising. Online shopping has led to a steep increase in online fraud. Explicit self-generated material is an increasing concern and is also distributed

for profit. Criminals continue to abuse legitimate services such as VPNs, encrypted communication services and cryptocurrency.

The acceleration of progress marks the rise in cyber attacks

The acceleration of progress in health care shaped by the beginning of the 4th Industrial Revolution, not only fundamentally changed the way we live, work, and connect to each other, but also marked the rise in cyber attacks especially on healthcare organizations. For example, the impact of phishing attacks aiming to collect user credentials as well as ransomware attacks seeking to encrypt the data of hospitals can be huge in critical infrastructures like healthcare, both from a societal (e.g. stolen health records, interruptions of emergency services) and financial (e.g. ransomware payments, production losses due to outages) perspective.

"Due to the fast introduction of technology advancements, vulnerabilities are constantly being identified and new threats are emerging. Cyber-attacks on health facilities are designed to prevent their employees from accessing critical care systems. As a side effect of the recent increased trend in telework and telemedicine due to the pandemic, breaches on operating systems in the cloud are expected to rise" says Mr. Dimitrios G. Katehakis, Head of the Center for eHealth Applications and Services at the Institute of Computer Science, Foundation for Research and Technology-Hellas (FORTH) in Heraklion, Crete (https://www.ics.forth.gr/), adding that in Greece there have been occasional and limited cyber attacks on health care providers, such as the last one in the hospital of Chania, Crete in 2017.

Many cybersecurity challenges in health industry are linked to vulnerabilities existing before the pandemic. According to Mr. Katehakis the health sector is a vulnerable target for cyber attackers because medical devices are usually manufactured without or with weak protection, professionals are not adequately trained in the risks, the sector is highly fragmented, there are many and frequent exchanges of multifaceted data, a large number of technologically outdated IT systems still operate, different technological solutions coexist, while at the same time there is no uniform data protection culture.

"Panacea" a people-centric cybersecurity in healthcare

Numerous cybersecurity studies support the fact that the "Achilles heel" of IT is the users. Healthcare professionals focus on the medical practice *and the patients, not giving the needed attention to issues relevant to health IT* safety and privacy. *"It is common between users to share the same password for accessing medical information systems. Although various information and awareness campaigns have been carried out, it is difficult*

to change the established culture. It needs time and the right approach. Time may be hard to find, but the right approach is possible!", comments Dr. Vangelis Sakkalis, Research Director at the Institute of Computer Science, Foundation for Research and Technology-Hellas (FORTH) in Heraklion, Crete, Greece.

Cybersecurity in healthcare is a complex issue. While there are constant attempts to upgrade old IT legacy systems and to renew connected medical devices and to procure the best new IT technologies, a similar approach in defining risks of the IT systems is not common. *"Cybersecurity starts with the definition of the current risks present in a healthcare system, structural risks and most of all human risks. Humans working in the healthcare sector are not IT oriented and mostly consider the great advantages furnished by digital systems as a waste of time and a drawback on their efficiency in treating patients. This leads to a risk-oriented behavior with very little understanding of security measures. Security must start and rely on the correct behavior of healthcare workers. And this behavior must be proactive and not reactive and neglected. On the other hand cybersecurity must not be agony and an obstacle towards the performance of healthcare procedures"*, adds Prof. Sabina Magalini, at the Rome Catholic University School of Medicine (UCSC) and Senior Surgeon of the Emergency and Trauma Surgery Unit at the Fondazione Policlinico Universitario Gemelli (FPG), who coordinated the European project for cybersecurity in hospitals, named Panacea (https://www.panacearesearch.eu). The project started in 2019 as a part of the European Framework Program for Research and Innovation "Horizon 2020", it has been financed with five million Euros, and it has involved 15 entities between Universities, Institutions and European companies from 7 EU members.

According to Dr. Sakkalis tackling cyber threats (internal and external) requires not just advanced cyber security solutions but also driving a human-centric approach, training and educating medical staff and patients on best-practice behavior, both of which are critical to building resilience in critical infrastructures. *"PANACEA acts on different levels, from healthcare tailored risk assessment, easy and manageable tools for information sharing and identification of secure by design medical devices, to secure and simple measures for healthcare worker identity management. Solutions to cybersecurity in healthcare are many, PANACEA offers a portfolio of possible integrated alternatives"*, concludes Prof. Magalini.

Cybersecurity in EU

In order to help IT professionals in healthcare security to establish and maintain cloud security while selecting and deploying appropriate technical and organizational measures the European Union Agency for Cybersecurity (ENISA) released Guidelines for Cloud Security for Healthcare Services on January 18 2021

(https://www.enisa.europa.eu/publications/cloud-security-for-healthcare-services). In April 21 2021 the EU launched a new body, to be based in Bucharest, Romania, which will in particular channel cybersecurity-related funding from Horizon Europe and the Digital Europe Programme. This 'European Cybersecurity Industrial, Technology and Research Competence Centre' will work together with a network of national coordination centers designated by member states linking the main European stakeholders, including industry, academic and research organizations and other relevant civil society associations, to form a cybersecurity competence community, in order to enhance and spread cybersecurity expertise across the EU.

According to a new regulation (https://ec.europa.eu/info/publications/proposal-cyber-security-regulation_en) proposed by the European Commission and published 22 March 2022, all European Union (EU) institutions, bodies, offices, and agencies will be required to have cyber security frameworks in place for governance, risk management, and control. On 9 March 2022, European governments also drafted a declaration to reinforce the EU's cyber security capacities, which included increasing EU funding to support national efforts and develop a strong cyber security ecosystem (https://www.euractiv.com/section/cybersecurity/news/eu-countries-to-call-for-the-establishment-of-a-cybersecurity-emergency-fund/).

COVID-19 CYBERSECURITY HEALTH

E THOUGHT ON "CYBERSECURITY: AN EU HEALTH CHALLENGE 'HE POST-COVID ERA"

ack: Cybersecurity: an EU health challenge in the post-Covid era - Heal Security Inc