COMMENTARY #29 • JUNE 2021

THESQUARE

MEDITERRANEAN CENTRE FOR REVOLUTIONARY STUDIES

CYBERSECURITY IN HEALTH SECTOR

Jacopo Franceschini

Cyberthreats and Vulnerabilities in Healthcare Sector

Healthcare sector is becoming increasingly more exposed to attacks and threats coming from the cyberspace. Digital technologies are utilized and are specifically developed to serve in a wide range of functions of healthcare industries such as IT networks, medical and surgical equipment, cloud archive systems, privacy of patients and Internet of Things (IoT). Starting from 2015 is witnessed a rampant increase of cyberattacks against healthcare infrastructures. As in the famous case of the ransomware WannaCry in 2017, the attackers were allegedly criminals capable to paralyze 2% of the British National Health System until the ransom was paid in cryptocurrency.[1] Also during the corona virus outbreak and pandemic, cyberattacks targeting healthcare facilities kept raising. One of the major attacks was directed against the Brno University Hospital in Czech Republic brought to a total paralysis of this structure in the midst of the Corona outbreak.

Until now major attacks against healthcare facilities were organize by criminal groups, with no clear political affiliation, which

[1] Andrew Dwyer *"The NHS cyber-attack: A look at the complex environmental conditions of WannaCry"*, RAD Magazine, 44 (January 2018), 5.

exploited the cyber weaknesses of this sector. As all the other major infrastructure, healthcare sector might also be the target of more or less explicit cyberattacks led by other states but despite all this concrete concerns cyber developments in healthcare industries and facilities do not seems to be accompanied hand by hand by an adequate cyber protection by States.

Main Current Threats

Just in the United States (US) the number of breaches documented escalated from 199 in 2010 to 505 in 2019. In the same time lapse cyberattacks against healthcare were limited to the 4.8% data breaches hitting the US healthcare, in 2019 cyber data breaches escalated to 58%.[2] Data breaches do not represent the only type of threat affecting healthcare sector tough.

Disruptive attacks in the form of ransomware are also becoming the main typology witnessed in healthcare. These kinds of attacks give access and encrypt the target's data and ask for a payment to unlock the files. Once this happens, there is no guarantee that the victim will be able to gain access to their data again, even if they negotiate it. Today, the attack vector for ransomware has spread to include applications used on the Internet of Things (IoT) and mobile devices, and viruses include more complex encryption. This is partly due to the availability of ready-to-use ransomware kits, also called ransomware-as-a-service (RaaS), available on the Deep web. Ransomware is now far more adapt at targeting larger organizations such as healthcare institutions than individuals, which means exponentially larger sums of money are at stake. Ransomware has therefore evolved from a small nuisance to a serious threat. Ransomware attacks increased worldwide of 129% in 2020[3] and solely between November 2020 and January 2021

[2] Adil Hussain Seh, Mohammad Zarour, Mamdouh Alenezi, Amal Krishna Sarkar, Alka Agrawal, Rajeev Kumar, and Raees Ahmad Khan, *"Healthcare Data Breaches: Insights and Implications"*, Healthcare Basel, 8, no:2,133-134.

[3] Brian T. Horowitz, *"2020 offered a 'perfect storm' for cybercriminals with ransomware attacks costing the industry $21B"*, FierceHealthcare, accessed 21st April 2021, https://www.fiercehealthcare.com/tech/ransomware-attacks-cost-healthcare-industry-21b-2020-here-s-how-many-attacks-hit-providers

ransomwares in healthcare sector rose to 45%, doubling the number of attacks of the same typology experienced by other industrial sectors[4].

Social engineering cyberattacks are another form of threat which utilizes cognitive vulnerabilities of users to infiltrate systems and access to protected data. Poor procedural and policy knowledge of the cyber realm by professionals with access credentials to a healthcare facility's informatic system, could be exploited by criminals to conduce their attacks. Phishing, still represent the most diffuse email-based method used by criminals to breach into healthcare institutions. In healthcare sector, spear phishing represents the main category of phishing where a certain typology of high rank professionals is the main target[5]. Famous ransomwares such as Petya and NotPetya in 2016-2017 used mainly spear phishing methods to infect healthcare systems[6].

Main vulnerabilities in health sector

- *Electronic Healthcare Record (EHR)*

EHR are a person's digital health information. It contains much more than what's already included in Electronic Medical Record (EMR). Electronic health records include vital signs, past medical history, diagnoses, progress notes, medications, allergies, lab data, immunization dates, imaging reports, insurance and social security information. These information may also travel outside the organization's premises. The EHR system is designed in such a way that it can be shared with all providers involved in patient care. Healthcare workers, laboratories, pharmacies, ministries of health,

[4] *"Attacks targeting healthcare organizations spike globally as COVID-19 cases rise again"*, Checkpoint Software, accessed 21st April 2021, https://blog.checkpoint.com/2021/01/05/attacks-targeting-healthcare-organizations-spike-globally-as-covid-19-cases-rise-again/

[5] Jason Steer, *"Defending against Spear-Phishing"*, Computer Fraud & Security, 2017, No. 8, (August 2017), 19.

[6] *"Cybersecurity in Healthcare: Responding to Petya/NotPetya Attack"*, Global HIT Blog, accessed 14th April 2021, https://blog.thehcigroup.com/responding-to-the-notpetya-cyber-attack

private IT contractors, medical IT devices industry, all these actors might be in possession of these sensible data concerning all medical records of the person. These records can be easily accessed and used by the same patient to make treatment, book appointment and take medical decisions through apps delivered by health institutions. Eventually, EHR includes various tools that providers can use to make important decisions about patient treatment, giving a more comprehensive and data crossed understanding of the information of one patient not limiting it to a single patient diagnosis. EHR represent for cybercriminals an extremely valuable target to obtain ransom by healthcare industry or to resell the data.

- *Internet of Things/Internet of Medical Things*

The Internet of Things (IoT) is the network of commonly used objects that are connected to the internet. These objects, of the most varied types and uses, range from microscopic devices to large, complex equipment. It is an ever-expanding network of objects, which is changing the world in all sectors, including medical and healthcare, and is entering the field of telemedicine. The medical sector has generated its own acronym for this: IoMT - Internet of Medical Things. IoMT is a component of the emerging field of "digital health", which includes sectors such as healthcare companies based on clinical support systems, patient health data analysis, telemedicine and large-scale IT systems that manage electronic health records. Repetitive tasks, which otherwise would have to be done manually, are thus delegated to technology, allowing administrators and healthcare professionals to focus their time on skilled work.

The factors that allow the industry to expand are: availability of a global internet network, or the ubiquity of internet connectivity via cellular, satellite and Wi-Fi, miniaturization of technology, which allows devices to obtain greater power in ever smaller dimensions. Three important applications of IoMT concern the interest in materials engineering which, by developing new materials, has facilitated progress in the sector of sensors, actuators, enclosures and other components used in IoMT technology. Secondly, Cloud computing where the cloud stores and makes available the data generated by the IoT. Eventually, the Big Data which gives the ability to analyze large amounts of unstructured or semi-structured data deriving from IoMT, by data scientists, to improve the quality of healthcare operations. By remotely acquiring medical data, facilitating drug delivery and enabling digital healthcare applications, IoMT offers results of improved convenience and functionality for patients and their doctors. From a cybersecurity perspective IoMT are one of the most vulnerable spots of e-healthcare. IoMT, in practice, mainly relies on legacy systems, limited security enhancements with few aftermarket securities updates.[7]

Beside the "traditional" threats represented by stolen data/privacy records, paralysis of e- system of healthcare institutions when dealing with IoMT there is a possible and alarming direct threat toward human security. Some IoMT devices consist in wearable tools dosing therapies to patients or monitoring health signs. Despite not have been recorded any significant attempt to undermine these kinds of devices through cyber alteration or sabotaging, it is which have to be taken into consideration given the high vulnerabilities of IoMT.

At the moment, one of the most witnessed incidents involving IoMT happened due to a human awareness on vulnerabilities coming from cyberspace. Staff members of healthcare industries and institutions might be the vectors of cyber threats because of unconscious risky behaviour such as not downloading updates, use of inefficient/not adjourned passwords, poor patch management during their job routine while using IoMT devices. The phenomenon of bring your own devices (BYOD) among healthcare professionals also expand the spectrum of vulnerabilities while personal device are connected to IoMT. [8]

[7] *"Baseline Security Recommendations for IoT in the context of Critical Information Infrastructure"*, ENISA (November 2017),22.

[8]Rashad J. McFarland, Samuel BO Olatunbosun, "*Exploratory Study on the use of Internet_of_Medical_Things (IoMT) In the Healthcare Industry and their Associated*

Conclusions

The recent ransomware attack to Ireland's National Health System in May 2021 witnesses the current trend which sees health sector increasingly more under threat in the cyber domain.[9] Avoiding completely these kinds of attacks coming from the cyber domain is realistically impossible for States, health institutions, private contractors and all the subjects composing the cyber network of health sector.

In order to strengthen the cybersecurity of health sector a more comprehensive and human-oriented understanding of cybersecurity should be promoted. Trainings on cyber threat have to become a central part of the education of medical and management staff. At the same time, the awareness of patients and users of medical services, interfacing themselves through e-health networks and devices, should be raised since the cybersecurity in healthcare represents a first line of defense for health and human rights[10] of each citizen.

Cybersecurity Risks", International Conference Internet Computing and Internet of Things, (2019), 119.

[9] "*Cyber-attack on Irish health service 'catastrophic'*", BBC, 20 May 2021. https://www.bbc.com/news/world-europe-57184977

[10] *"Playing with Lives: Cyberattacks on Healthcare are Attacks on People",* The CyberPeace Institute, (9 March 2021).