HEALTHCARE IOT TAKES US INTO THE FUTURE OF EHEALTH AND DIGITAL THERAPEUTICS, BUT ITS CYBERSECURITY MUST BE RESET BY DESIGN

SERGIO GUIDA

Independent Researcher, Sr.Data/Information Governance Mgr.

Key-words: ehealth

Category: Legal Area

Healthcare providers leveraged technologies to transform care delivery, patient experience, staff /operation management and hospital design. “Patients are now eager to get more insights into their treatment path and how they can speed up that process. Consumer adoption of digital health has reached peak levels; compared to a few years ago, more people use wearable devices, access telemedicine, and go online to search for health-related information”[1].

Smart device manufacturers will double their use cases in healthcare, analysts say[2]. According to the Forrester think tank, 2021 should be the year of the IoT (Internet of Things) in the health sector. As noted, many people stayed home in 2020, leaving chronic illnesses unmanaged and even symptoms undetected. “In 2021, proactive engagement will increase using wearable devices and sensors to track patient health at home. Consumer interest in digital healthcare devices will increase as people appreciate the convenience of home monitoring, an understanding of their health and the reduced cost of connected healthcare devices”, Forrester[3] experts note.

For its part, WHO (World Health Organization) has just established a 'Council on the Economy of Health forAll'[4], with a clear roadmap: to put the principle of "health for all" at the center of how we must imagine creation of value and economic growth.

Upon establishment in November 2020, WHO Director-General Tedros Adhanom Ghebreyesus said: "The time has come to write a new story in which health is not seen as a cost, but as an essential investment for economies at the same time. productive, resilient and stable time".

Meanwhile, the introduction and increase of digital technologies, including 5G and IoT, in healthcare systems is seen as a fundamental way to rationalize healthcare and make it become both more effective and more convenient[5].

The Internet of Things (IoT) consists of a network of physical devices that uses connectivity to enable the exchange of data. In the context of healthcare, the IoT, powered by the now upcoming 5G networks[6], can have big benefits: let's think for example of doctors who use data-intensive augmented reality or virtual reality visualizations to help patients better understand a diagnosis or treatment and technologies that can help a specialist better analyze a patient's condition.

According to experts at Check Point Software Technologies[7], some of the most relevant benefits of using IoT in the healthcare industry include:

- ü the reduction of operating costs (through the use of IoT medical devices),
- ü a better patient experience e
- ü the reduction of errors.

In terms of 'improving patient experience'[8], IoT-connected healthcare applications can offer remote monitoring and make physical spaces smarter and more integrated. Improved efficiency of operations, clinical activities and management of essential resources all contribute to the improvement of the experience.

With real-time data and the ability to analyze a patient's past treatments and diagnosis, smart health systems using IoT can help reduce errors. Treatment outcomes can also be improved as the data collected by IoT healthcare devices is highly accurate and can help healthcare professionals make informed decisions. Likewise, IoT healthcare applications that provide ubiquitous monitoring systems can also be used for disease management, and better data analytics can lead to better insights for better disease management.

However, the use of the IoT in the healthcare sector is far from free of pitfalls: indeed, in general, IoT devices are simple and functional but cannot be managed, patched, updated or protected centrally and this makes them vulnerable to exploitation by cybercriminals.

When it comes to protecting IoT devices from cyber attacks, Dumas[9] added that hospitals face unique challenges and features:

1) There are on average 10 to 15 medical devices per bed, such as infusion pumps and respirators, but many of these devices were designed with no safety in mind.

2) Almost half of the connected medical devices work on unsupported operating system (or legacy operating systems)[10] that no longer receive security updates. These include ultrasound machines, MRIs, and more, making them easy targets for cyber attacks, such as ransomware.

Compromised electronic protected health information (ePHI)[11] records are being smuggled in for hundreds of dollars a record, making them an attractive target. Hospitals spend an average of $ 430 per record to mitigate each stolen medical identity[12]. When hospitals want to update the underlying operating systems of their medical devices, this often proves difficult due to operational considerations and the need to retest and certify the devices for use.

Finally, medical devices are not the only things that are vulnerable: the resources of building management systems and intelligent offices (BMS) are also primary targets, both as a gateway to the hospital network and as a target for manipulation and the acquisition.

The experts from Check Point Software Technologies[13] provide some tips regarding IoT device protection and monitoring, legacy operating systems and medical records for healthcare organizations - it is important to ensure complete visibility of IoT devices and risk analysis, mitigation of vulnerability and zero-day[14] threat prevention even on unidentifiable devices and the intuitive segmentation and management of the Zero Trust network[15].

Having complete visibility of IoT devices and accurate risk analysis helps identify and classify devices on a given network by integrating with leading detection engines to expose risks such as weak passwords, outdated firmware and known vulnerabilities.

IoT devices should be "virtually patched" to correct security flaws, even those with unidentifiable firmware or legacy operating systems. It is critical to identify and block unauthorized access and traffic to and from devices and servers, and to prevent IoT-targeted malware attacks.

Implementing granular security rules across the entire IoT network fabric[16] based on device attributes, risks and protocols will help ensure intuitive segmentation and management of the Zero Trust network.

It is also important to support holistic management of security policies in a single control panel for IT and IoT networks.

“According to recent findings from INTERPOL, the International Criminal Police Organization, those responsible for threats have intensified their attempts to pollute hospital IT networks with ransomware. In the midst of the COVID-19 pandemic, the negative outcome is not limited to data corruption or monetary damage to the organization, but more importantly, it hampers rapid medical response and can impact patients' physical well-being, making the situation literally a matter of life and death" [17].

The following tips are essential to help healthcare institutions be less susceptible to ransomware attacks:

1. Education: Training users on how to identify and avoid potential ransomware attacks is critical. Since many of today's cyber attacks start with a targeted email that doesn't even contain malware, just a 'social engineering' message encouraging the user to click on a malicious link, user education is often considered one of the most important defenses an organization can deploy.
2. Continuous data backups: Maintaining regular backups of your data as a routine process is a very important practice to avoid data loss and to be able to restore it in case of damage or malfunction of the disk hardware. Functional backups can also help healthcare organizations recover from ransomware attacks.
3. Patching: this is a critical component in defending against ransomware attacks as cybercriminals often search for the latest exploit[18] discovered in patches made available and then target systems that have not yet been updated. Hence it is critical that organizations ensure that the latest patches are applied to all systems, as this reduces the number of potential vulnerabilities that an attacker can exploit.
4. Endpoint Protections: Conventional signature-based antivirus is a highly efficient solution for preventing known attacks and should definitely be implemented in any healthcare organization, as it protects against most malware attacks a healthcare organization faces.
5. Network Protections: Advanced protections in the corporate network such as Intrusion Prevention System (IPS), Network Anti-Virus and Anti-Bot are also crucial and efficient in preventing known attacks. Advanced technologies such as sandboxing[19] have the ability to analyze new and unknown malware, execute it in real time, look for signs that it is malicious code and consequently block it and prevent it from infecting endpoints and spreading to other locations in the company. Sandboxing is therefore an important prevention mechanism that can protect against evasive or zero-day malware and allow you to defend against many types of attacks unknown to your business.

Coming back to a more general perspective, I cannot avoid to quote the words of the EDPS [20]: “the pandemic risks being the perfect occasion for some to exploit the most sensitive ‘attributes’ of human beings, health data. We voiced our concerns at the beginning of the year on how corporate entities were appropriating health data for purposes covered by business secrecy. Pandora's box is now open, with digital behemoths conquering the almost unexplored and virgin world of health data markets - until now”.

Indeed, on a 'macro' and official point of view, "the healthcare data analytics market is expected to grow to $47.7 billion by 2024[21].

So possibly it wouldn't be so hard to imagine some kind of correlation on a 'micro' and unofficial point of view, if it's true that "surprisingly, the value of healthcare data can be significantly higher than various types of financial records. According to Experian, a single patient record can sell for upwards of $1000 on the black market, depending on how complete the record is; this is nearly fifty times higher than standard credit card records. Criminals consider healthcare data to be a treasure trove of sensitive information due to the personally identifiable information[22] it contains[23].

That's why, adding a higher level to the measures seen before, let me only make a brief reference to a very useful research, carried up just in 2020[24]: "In this work, we proposed a new IoT layered model, stretched with the privacy and security components and layers identification. The proposed cloud/edge supported IoT system is implemented and evaluated"..."This work will guide regulatory agencies to continue enforcing policies, educating end-users and entities, and stakeholders involved in IoT to develop and apply more appropriate security and privacy measures.

Source: Forrester, EDPS, MDPI.

Link: https://www.healthcareitnews.com/news/asia-pacific/opportunities-pitfalls-healthcare-iot.

[1] Cf. Deloitte, *A journey towards smart health. The impact of digitalization on patient experience*, February 2018 in https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/life-sciences-health-care/lu_journey-smart-health-digitalisation.pdf.

[2] Cf. Aurélien Tardiveau, *Qu'est-ce qui nous attend en matière de santé, en 2021?* Futura Santé, Publié le 19/12/2020 in https://www.futura-sciences.com/sante/actualites/medecine-quest-ce-nous-attend-matiere-sante-2021-84794/#xtor= EPR-57-[ALERTE]-20201219.

[3] Cf. Michele Pelino, *Predictions 2021: Technology Diversity Drives IoT Growth*, October 28, 2020 in https://go.forrester.com/blogs/predictions-2021-technology-diversity-drives-iot-growth/.

[4] Cf. WHO *establishes Council on the Economics of Health for All - The Council, comprising top economists and health experts, will focus on investments in health, and achieving sustainable, inclusive and innovation-led economic growth*. News release 13 November 2020, Geneva in https://www.who.int/news/item/13-11-2020-who-establishes-council-on-the-economics-of-health-for-all.

[5] Cf. Sophie Porter, *Vodafone releases report on how 5G and IoT technology can transform healthcare*, November 11, 2020 in https://www.healthcareitnews.com/news/emea/vodafone-releases-report-how-5g-and-iot-technology-can-transform-healthcare.

[6] We can find a detailed analysis in the Report "*Better Health, Connected Health: How 5G and IoT Technology can Transform Health and Social Care, A WPI Strategy report for Vodafone UK*" November 2020 in https://newscentre.vodafone.co.uk/app/uploads/2020/11/Vodafone-5G-Health-Report.pdf. For example, at page 2 we read "Technology has already helped to transform the NHS at short notice at a critical time. But it promises even more in the future – particularly with the roll-out of 5G and Internet of Things (IoT) technology. The possibilities unleashed by 5G and IoT touch almost every part of the healthcare system, from the visible (remote surgery, or drones carrying transplant organs and drugs between hospitals) to the unseen but vital (IoT-enabled hospital equipment management systems that use sensors to automatically monitor stock levels). Both NHS patients and staff stand to benefit from these technological innovations".

[7] Cf. Evan Dumas - Check Point Software Technologies , Opportunities & pitfalls in healthcare IoT , December 18, 2020 in https://www.healthcareitnews.com/news/asia-pacific/opportunities-pitfalls-healthcare-iot.

[8] For instance, we can read "today, the patient journey is still in its infancy. But patients increasingly choose healthcare providers who can respond to their needs. Improving patient experience is about improving the sum of all interactions that influence patient perceptions across the continuum of care. This starts with engaging people before they become patients and it continues with the diagnostic and therapeutic experience in a care setting. Ultimately what matters to patients are treatment outcomes that lead to higher-quality of life. Patients stay loyal to health systems that create excellent experiences" in https://www.siemens-healthineers.com/insights/improving-patient-experience.

[9] Cf. Evan Dumas - Check Point Software Technologies , Opportunities & pitfalls in healthcare IoT , December 18, 2020 in https://www.healthcareitnews.com/news/asia-pacific/opportunities-pitfalls-healthcare-iot, cited above.

[10] A legacy platform, also called a legacy operating system, is an operating system (OS) no longer in widespread use, or that has been supplanted by an updated version of earlier technology. Many enterprises have legacy platforms, as well as legacy applications, that serve critical business needs.

[11] Cf. "What is Protected Health Information? Anything related to health, treatment or billing that could identify a patient is PHI. This includes:

- Name
- Dates (e.g. birthdate, date of treatment)
- Location (street address, zip code, etc.)
- Contact numbers (phone number, fax, etc.)
- Web contact information (email, URL or IP)

- Identifying numbers (Social security, license, medical account, VIN, etc.)
- Physical identity information (photo, fingerprints, etc.)

Under the HIPAA (Health Insurance Portability and Accountability Act , a US federal law) Privacy Rule, PHI can generally only be used to furnish medical services and process payments. There are also a few special cases when PHI must be disclosed, such as under a court-ordered warrant. Medical information that has been de-identified (stripped of all identifying information) is no longer subject to the HIPAA Privacy Rule, and can be used for other purposes, such as case studies" in https://www.virtru.com/blog/what-is-ephi/.

[12] Cf. Evan Dumas - Check Point Software Technologies , Opportunities & pitfalls in healthcare IoT , December 18, 2020 in https://www.healthcareitnews.com/news/asia-pacific/opportunities-pitfalls-healthcare-iot, cited above.

[13] Ibidem.

[14] Software vendors continuously check for new vulnerabilities in their products and upon discovery, issue a patch to protect their users. 'White hat' researchers are also constantly on the lookout for new vulnerabilities, and when they find one, report them to the vendor so they can issue a patch. "A zero-day (or 0-day) vulnerability is a software vulnerability that is discovered by attackers before the vendor has become aware of it. By definition, no patch exists for zero-day vulnerabilities and user systems have no defenses in place, making attacks highly likely to succeed. A zero-day exploit is a method or technique threat actors can use to attack systems that have the unknown vulnerability. One method is zero-day malware – a malicious program created by attackers to target a zero-day vulnerability. A zero-day attack is the actual use of a zero day exploit to penetrate, cause damage to or steal data from a system affected by a vulnerability", as we can read at https://www.cynet.com/advanced-threat-protection/zero-day-attack-prevention/.

[15] Zero trust security is an IT security model that requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network perimeter. The philosophy behind a zero trust network assumes that there are attackers both within and outside of the network, so no users or machines should be automatically trusted. Another principle of zero trust security is least-privilege access. This means giving users only as much access as they need, minimizing each user's exposure to sensitive parts of the network. Zero trust networks also utilize microsegmentation, i.e. the practice of breaking up security perimeters into small zones to maintain separate access for separate parts of the network. For example, a network with files living in a single data center that utilizes microsegmentation may contain dozens of separate, secure zones. A person or program with access to one of those zones will not be able to access any of the other zones without separate authorization. Multi-factor authentication (MFA) is also a core value of zero trust security: it simply means requiring more than one piece of evidence to authenticate a user, so just entering a password is not enough to gain access. In addition to controls on user access, zero trust also requires strict controls on device access, by monitoring how many different devices are trying to access their network and ensure that every device is

authorized. This further minimizes the attack surface of the network. More details available at https://www.cloudflare.com/it-it/learning/security/glossary/what-is-zero-trust/.

[16] Network fabric is the term used to describe the structure of a computer network: as in the textile industry it describes the interweaving of various types of cloth to make a useable material, fabric in the computer industry describes the weaving of various IT components that communicate through interconnected switches. In the IoT world, where everyday devices like smart locks, thermostats, and fitness bracelets are internet-connected, the network fabric a) facilitates the movement of data from the hardware-defined product, essentially sensors that collect information, to the software-defined product, or brain, of the IoT device. b) As a distributed computing system, it brings together software pieces from multiple systems to function as a single unit. It also incorporates storage capabilities. c) Enables networking through various protocols or layers: media/networking/application/meta. These layers help organize and transport information that will be used by the IoT device.

[17] Cf. Evan Dumas - Check Point Software Technologies , Opportunities & pitfalls in healthcare IoT , December 18, 2020 in https://www.healthcareitnews.com/news/asia-pacific/opportunities-pitfalls-healthcare-iot, cited above.

[18] "An exploit is a piece of software, data or sequence of commands that takes advantage of a vulnerability to cause unintended behavior or to gain unauthorized access to sensitive data. Once vulnerabilities are identified, they are posted on Common Vulnerabilities and Exposures (CVE). CVE is a free vulnerability dictionary designed to improve global cyber security and cyber resilience by creating a standardized identifier for a given vulnerability or exposure.

Exploits take advantage of a security flaw in an operating system, piece of software, computer system, Internet of Things (IoT) device or other security vulnerability. Once an exploit has been used, it often becomes known to the software developers of the vulnerable system or software, and is often fixed through a patch and becomes unusable.

This is why many cybercriminals, as well as military or government agencies do not publish exploits to CVE but choose to keep them private. When this happens, the vulnerability is known as a zero-day vulnerability or zero-day exploit", as we can read at https://www.upguard.com/blog/exploit.

[19] "In cybersecurity, a sandbox is an isolated environment on a network that mimics end-user operating environments. Sandboxes are used to safely execute suspicious code without risking harm to the host device or network.

Using a sandbox for advanced malware detection provides another layer of protection against new security threats, zero-day (previously unseen) malware and stealthy attacks, in particular. And what happens in the sandbox, stays in the sandbox,avoiding system failures and keeping software vulnerabilities from spreading", as reported, for instance, in https://www.forcepoint.com/cyber-edu/sandbox-security.

[20] Cf. Wojciech Wiewiórowski, *Projecting our future: A privacy carol*, Friday, 18 December, 2020 in https://edps.europa.eu/press-publications/press-news/blog/projecting-our-future-privacy-carol_en.

[21] Cf. Amalio Telenti , *Medical Data Goes To The Market* , Forbes Technology Council, Dec 30, 2019 in https://www.forbes.com/sites/forbestechcouncil/2019/12/30/medical-data-goes-to-the-market/.

[22] See note 11 above.

[23] Cf. TBConsulting , *Why Healthcare Data is so Valuable on the Black Market,* Published on June 24, 2020 in https://blog.tbconsulting.com/why-healthcare-data-is-so-valuable-on-the-black-market.

[24] Cf. Lo'ai Tawalbeh, Fadi Muheidat, Mais Tawalbeh, Muhannad Quwaider, *IoT Privacy and Security: Challenges and Solutions*, Published: 15 June 2020 in https://www.mdpi.com/2076-3417/10/12/4102/pdf.