MEDICAL DESIGN BRIEFS

January, 2022

www.medicaldesignbriefs.com

Is Healthcare Ready to Pick Up the Pace in Cybersecurity?

By Shane Keating & Stephanie Van Ness, Integrated Computer Solutions

Cybersecurity in healthcare has never had a higher profile than right now. A string of IT breaches and ransomware attacks on HIPAA-covered entities and their business associates has threatened patient care, led to substantial financial losses, and brought unwanted attention to healthcare organizations. In July 2021 alone there were 70 reported data breaches of 500 or more records, making it the fifth consecutive month where data breaches had been reported at a rate of two or more per day.[1]

Reprinted from Medical Design Briefs, Digital Edition, January 2022 - *https://www.nxtbook.com/smg/techbriefs/22MDB01/index.php?startid=12#/p/12*

If that's not scary enough, there's this: between August 2020 and the end of July 2021, the private health data of 44,369,781 individuals was exposed or compromised in more than 705 reported data breaches (of 500 or more records). For instance, Wisconsin provider Forefront Dermatology reported that hackers gained access to parts of its network that contained the protected health information of 2.4 million individuals.

In a ransomware attack reported by Practicefirst, a New York associate of multiple HIPAA-covered entities, healthcare data of 1.2 million individuals was potentially stolen. Believe it or not, this attack could have been even worse considering that the majority of ransomware gangs today exfiltrate sensitive data before using ransomware to encrypt files, and then force victims to pay twice: once to prevent the publication or sale of the stolen data, and again to obtain the keys to decrypt files.

Swift Change is Needed

In this environment, healthcare organizations face very difficult choices in balancing patient protection with financial demands. Costs for insurance against cyber risks have skyrocketed as attacks have escalated. Organizations' effectiveness in counteracting these threats affect their costs, both in terms of actual incidents and in terms of insurance costs, so new approaches to cybersecurity are warranted.

Historically, cybersecurity for medical devices and medical networks has been weak, and the healthcare industry in general has been conservative in adopting new technologies. But this approach is no longer adequate. For this reason, the Cybersecurity and Infrastructure Security Agency has issued new guidance to help combat this rise in "double extortion" ransomware attacks, offering best practices for preventing cyber threat actors from gaining access to networks, detailing measures to ensure sensitive data are protected, and outlining procedures to follow when responding to a ransomware attack.[2] Additionally, The National Institute of Standards and Technology has updated its cybersecurity guidance on building resilient computer networks.[3]

End-to-End Cybersecurity

With the average cost of a healthcare data breach around $7.1 million, it is essential to protect critical assets.[4] The most effective way to counteract today's threats is by taking an end-to-end view and locking down everything, including PHI (Protected Health Information) and PII (Personally Identifiable Information). How? By securing the entire network and keeping data safe as it traverses from the "edge," where people are interacting with real devices, all the way to the cloud, where data is increasingly being sent for further processing and analysis.

> "The cost of data breaches in fines and damages is directly related to the extent of measures taken to protect data. It is essential that organizations take every possible precaution to safeguard protected data."

Cybersecurity at the Edge

Medical devices are becoming more connected every day, and are definitely here to stay — analysts forecast growth rates of 29 percent in the IoMT (Internet of Medical Things) market.[5,6] Devices that remotely monitor patients, sense glucose levels, measure heart rates, even check hand hygiene — the medical IoT has it all. And users have grown accustomed to the convenience these devices deliver with features like cloud-connectivity, wireless/Bluetooth connectivity, and automatic OTA software updates.

While IoT and Software as a Medical Device (SaMD) devices that patients or practitioners can interact with in a home or institutional setting can conveniently meet patients' needs, they can be irresistible to a cybercriminal. Not only does this huge volume of devices contain valuable data, each individual unit also provides a potential route into an organization's network.

In recent years, myriad devices have been compromised, including baby heart monitors, cardiac devices, and webcams. Security vulnerabilities have impacted hundreds of thousands of devices - a problem that has only grown in light of the pandemic, which has caused large numbers of devices, as well as workers, to migrate to people's homes where networks are even more vulnerable.

Since edge devices typically have less security, are on riskier parts of a network, and have users who are less knowledgeable about good password security (and security measures in general), the manufacturer's efforts to maintain device security should start here.

Securing a Medical Device

Most consumers would expect credit card terminals to incorporate the most advanced cybersecurity measures since they process high volumes of sensitive financial data. To that end, credit card terminals have a hardware root-of-trust, ensuring that all critical assets are protected in a way that attackers cannot see anything by snooping memory while the device is in operation. Additionally, all software updates for these devices must be encrypted and signed. Makes sense.

But when it comes to our health data and the individual medical devices that we rely on to keep us healthy, security is often lacking. Fortunately, that is changing and the latest medical devices are adopting these important security features. And new devices without adequate cybersecurity will face an uphill (if not impossible) battle to win FDA approval.

Cybersecurity features that in the past were considered too weighty for a medical device are no longer a nice-to-have, they are required. Encrypted updates are but one example. It is very difficult to predict the kind of vulnerabilities that may be discovered in OTS (off-the-shelf) software and new problems are found on an ongoing basis. Being able to react to new software issues by securely updating the device is an essential part of a manufacturer's response in today's threat landscape.

Securing Your Device's Data Doesn't End with the Device Itself

Beyond protecting your device, it is likely you will also need cloud connectivity. Moving customer PHI from the device to the cloud (and back) must be secured. Thankfully, cloud

providers like AWS provide out-of-the-box services for supporting IoMT connectivity and associated downstream uses of that data.[7]

After a connection is established between the device and the cloud, data can be routed from an IoT broker to various services like a database, long-term storage for audits, and functions to route data to external systems. Security must be maintained every step of the way, and cloud providers take this responsibility seriously.[8] (For more on protecting cloud data, read our four-part series Securing the Cloud with AWS.)[9]

The Takeaway

AWS's shared responsibility model dictates that the customer is responsible for "security in the cloud" while AWS' is charged with "security of the cloud."[10] Taking an end-to-end view — locking down everything and ensuring data is encrypted while at rest and in transit — is essential for preventing cyber threat actors from accessing your networks and devices to execute costly attacks.

Shane Keating *is cybersecurity engineering and project manager at Integrated Computer Solutions (ICS), especially focused on medical device projects.*

Stephanie Van Ness *is associate director of marketing at ICS and Boston UX. She writes about user experience (UX) design, device cybersecurity and innovations in technology, from gesture-controlled medical devices to self-driving vehicles.*

References

1. S. Adler, “July 2021 Healthcare Data Breach Report,” HIPAA Journal, Aug. 23, 2021.
2. S. Adler, “CISA Publishes Guidance on Protecting Sensitive Data and Responding to Double-Extortion Ransomware Attacks,” HIPAA Journal, Aug. 20, 2021.
3. S. Adler, “NIST Updates Guidance on Developing Cyber Resilient Systems,” HIPAA Journal, Aug. 12, 2021.
4. H. Landi, “Average cost of healthcare data breach rises to $7.1M, according to IBM report,” Fierce Healthcare, July 29, 2020.
5. “Internet of things (IoT) in Healthcare Market to Exhibit Astonishing 25.9% CAGR by 2028; Stoked by Increasing Demand for Medical Wearable Devices Worldwide, says Fortune Business Insights,” GlobeNewswire, June 7, 2021.
6. Internet of Medical Things Market | 2021 Size, Share, Growth Insights, Regional Analysis, Regional Outlook, Key Players, Industry Analysis, Covid-19 Impact, WBOC, May 28, 2021.
7. “AWS IoT Core,” Amazon.
8. “AWS Cloud Security,” Amazon.
9. J. Neto and R. Hampton, “Securing the Cloud with AWS,” ICS, June 30 , 2021.