Volume 4, Issue 15 August First Edition 2017

Healthcare Innovation NEWS

Building Secure Medical Devices to Protect Patient Data

by Chandu Ketkar

Despite a number of attempts in the industry to increase security and privacy of patients and their data, the issue is still quite a challenge. Even with the passage of the Health Insurance Portability and Accountability Act (HIPAA) in 1996, whose privacy and security rules went into effect in 2003, problems still exist; however, there has been a significant cultural shift within the industry. Daily operations have been readjusted to focus on the protection of patient information over the convenience of customer service protocols. This shift has resulted in procedural changes involving people, processes and technology that in turn affect patients, doctors, insurance companies and medical device manufacturers.

Fast forward about 10 years. In 2014 and 2015, there was a cluster of security breaches that highlighted some of the still-prevalent information security gaps throughout the healthcare industry, including a data breach of Anthem, Inc. that affected 78.8 million and a breach of Premera Blue Cross, in which 11 million individuals had their information accessed in a hacking incident. UCLA Health System was also the victim of a large-scale cyberattack, reporting a breach in July 2015, which risked the data of approximately 4.5 million patients. The majority of the industry was already moving toward improvements in the security of software and infrastructure, but these major breaches forced their hands.

"In 2014 and 2015, there was a cluster of security breaches that highlighted some of the still-prevalent information security gaps throughout the healthcare industry, including a data breach of Anthem, Inc. that affected 78.8 million and a breach of Premera Blue Cross, in which 11 million individuals had their information accessed in a hacking incident."

In addition to major headlines about the lack of security in the healthcare industry, results of the sixth iteration of the Building Security In Maturity Model (BSIMM), a 2015 study of existing software initiatives,[1] show the healthcare industry still lagging in comparison to other participating BSIMM firms (a total of 78 firms participated in BSIMM6) representing 12 industry verticals.

In an industry already behind others and one that requires securing copious amounts of sensitive customer data, an increasing number of unsecured devices serve as a perfect storm for hackers attempting to steal data. Only 9% percent of manufacturers and 5% of users say they test medical devices at least annually. Instead, 53% of device users do not test or are unsure if testing occurs.[2]

Vulnerable devices can serve as a back door platform for hackers to invade a network that might actually be pretty secure in and of itself. Hackers are aware of the fact that applications on a network that present the most risk to an organization are the most thoroughly tested and, generally speaking, the most secure.

So rather than waste time trying to break into the securely protected parts of a network, hackers will find less protected routes, such as vulnerabilities in medical device software, and pivot to access the sensitive data they are seeking. This is precisely why coding flaws in medical devices pose a serious threat to the healthcare industry and the massive amounts of sensitive data it houses.

"Only 9% percent of manufacturers and 5% of users say they test medical devices at least annually."

Responding to Challenges

The healthcare industry must respond to these challenges by taking a serious approach to security and incorporating a series of best practices to ensure the quality and security of its medical devices and ultimately patient privacy.

Here are some suggestions for healthcare companies to consider:

1. **Establish a secure software development life cycle (SSDLC).** Security works best when treated as a necessary property of a software development process, rather than bolting it on at the end. The overall objective is to perform security functions as early as possible. Many healthcare organizations are performing penetration testing, but successful companies have ensured secure coding guidelines prevent many of the vulnerabilities they have been finding.

   Medical device manufacturers and system developers should move to establish well-defined SSDLCs, which use proactive processes to identify security requirements, design defects and code-level bugs. The key activity in the SSDLC is threat modeling that identifies system assets and methods (called threat vectors or attack vectors), in which attackers can potentially compromise a system. Threat modeling also enables an organization to understand an application's threat landscape and provide actionable guidance for security testing of an application.

(continued on page 2)