A SECURITY CHECK-UP FOR HEALTHCARE PROVIDERS

CYBER TRENDS, THREATS AND SECURITY BEST PRACTICES

ADVANCED THREAT PROTECTION, SECURITY AND COMPLIANCE

Cyber attacks in the healthcare industry have been on the rise, particularly ransomware attacks targeting hospitals. The Department of Health & Human Services' Office for Civil Rights (OCR) reported more healthcare data breaches in 2016 than in the preceding five years. Ponemon Institute revealed in 2016 that healthcare organizations have experienced approximately one cyber attack every month; 48% of respondents in the study admitted that these attacks had led to loss or exposure of patient information[1].

Given the trove of information healthcare providers have on patients, it is no wonder that cyber attacks in the industry has increased significantly. Patient information, such as social security numbers, credit card information, date of birth and medical insurance information, are quite valuable on the dark web as they facilitate identity theft and medical insurance and financial fraud. Furthermore, several high profile ransomware attacks against hospitals have shut down their electronic health record (EHR) systems and affected hospital equipment. This demonstrates that cybersecurity in healthcare is not just an IT problem but also has ramifications for patient safety. Therefore, it is important for providers to understand the growing threat landscape and invest in solutions that improve their security posture. This paper examines the state of cybersecurity for healthcare providers, and offers guidance on how to address this critical issue.

The push to digitize medical records and have patient information readily accessible to providers increases the attack surface in healthcare. As a result of the HITECH Act of 2009, 96% of hospitals use an EHR system, which, by making it easier to share patient information, has led to improved patient outcomes. However, EHR systems, because of the valuable patient data they contain, are attractive to breaches by malicious external players and insider threats, putting patient safety and privacy at risk.

In 2016, high profile ransomware attacks against hospitals affected EHR systems and prevented patient data access. These ransomware attacks have several ramifications. The first is the impact they have on patient safety. Without access to patient records, physicians might not have the full picture or accurate information to adequately prescribe care. Impaired treatment information, coupled with other operational inefficiencies, could severely impact the quality of care. Secondly, exposing protected personal health information (PHI) data puts patients at risk for identity and medical fraud. Patients need to trust that healthcare providers can provide quality care and protect their information.

Hospital networks often have several thousand medical devices connected to their networks. Network-enabled patient monitors, infusion pumps and imaging devices give providers real-time access to patient information that is needed to swiftly make critical decisions. While patient care has improved as a result, having thousands of medical device endpoints also complicates the task of securing hospital networks from cyber attacks. Many of these devices incorporate older operating systems with vulnerabilities, and hospitals often don't have visibility into all the devices connected to their network. Without the ability to monitor all medical devices, often connected to unsegmented networks, hospitals are extremely susceptible to attacks that exploit those vulnerabilities. Hackers could use vulnerabilities within medical devices to access the hospital network and then exfiltrate patient data. In other instances, malware can spread throughout the network and hide in medical devices, where it lies dormant until it is used as a backdoor to exfiltrate data. Medical devices are critical for patient care, and security precautions commensurate to the grave risks must be taken to ensure the integrity and confidentiality of patient data.

Far from being just an IT problem, cybersecurity in healthcare is also a business problem. Data breaches cost the healthcare industry about $6.2B, yet "the majority of healthcare organizations still don't have sufficient security budget to curtail or minimize data breach incidents," according to Ponemon Institute's Sixth Annual Benchmark Study on Privacy & Security of Healthcare. Because highly publicized data breaches erode customer trust, following a successful cyberattacks healthcare organizations lose customers at a higher rate than other industries[2]. Data breaches can also have severe repercussions on patient health. In the ransomware attack at Hollywood Presbyterian Medical Center, the Locky malware locked down access to computers needed for essential functions, including EMR systems and CT scans[3], for over a week.

"Despite such significant repercussions of a cyber-attack, the healthcare sector lags in terms of its preparedness for cyber threats… in terms of technical capabilities, the healthcare industry is behind other industries in protecting its infrastructure and electronic protected health information (ePHI)—as commonly seen in the use of outdated clinical technology, insecure network-enabled medical devices, and an overall lack of information security management processes" – KPMG, *Healthcare and Cybersecurity: Increasing Threats Require Increased Capabilities,* 2015

Given the serious consequences of healthcare data breaches, healthcare providers need to invest more in cybersecurity. Below are three best practices on how to improve an organization's security posture. Although these recommendations might seem obvious, the spate of cyberattacks indicates that healthcare organizations are not effectively mitigating cyber threats.

DISCOVER & PROTECT ALL ASSETS

The first step in improving the security posture of your hospital is visibility into all the assets connected to your organization's network. Hospitals often have thousands of network-enabled medical devices, workstations—including legacy systems—connected to their network. Organizations cannot monitor and protect undiscovered assets. To ensure that your organization has a thorough inventory of all assets on the network and to increase the efficiency of lean IT security teams, leverage cybersecurity tools that can automatically discover and profile all assets. The 2016 HIMSS Cyber Security Survey showed that only about 50% of acute care providers are using network monitoring tools which provide invaluable information for preventing successful breaches.

Security Configuration Management (SCM) tools automatically profile discovered assets on the entire network and provide continuous configuration monitoring to improve the security posture of those assets. Such solutions continuously monitor your assets against their known-good states and alert your team to unauthorized changes. This not only provides confidence that all assets are protected, it saves IT teams' time and effort remediating those changes. Furthermore, because vulnerabilities on hospital networks often stem from legacy systems with configurations that can be exploited, it is important to select SCM solutions that have robust coverage for a wide breath of platforms and platform versions.

In addition, utilizing vulnerability management solutions that scans your network for vulnerabilities helps you achieve and maintain security of your assets. A study by KPMG[4] showed that only 13% of healthcare organizations are tracking cyber attack attempts, and concluded that "mature incident and vulnerability management processes are lacking in most organizations." The right solution, with granular prioritization and alerts, can actually make your IT team more efficient by helping them to focus on the most critical vulnerabilities on the network.

Lastly, insider threat is a growing concern across all industries. In Accenture's "*The State of Cybersecurity and Digital Trust 2016,*" 69% of respondents had experienced attempted or successful data theft by insiders. In healthcare organizations, authorized insiders could access patient data for unauthorized uses. Therefore, a log and event management solution is needed to accurately review system activity and swiftly audit events such as last login, last user and audit logs.

ADOPT AN INFORMATION SECURITY FRAMEWORK

Compliance with the HIPAA Security Rule ensures that healthcare organizations are adequately protecting electronic protected health information (ePHI). However, it is written in broad and technology-neutral language so that it can be implemented alongside other security frameworks such as the NIST Cybersecurity Framework, which provides more detailed guidance to help manage cybersecurity risks. PwC stated that when the NIST framework is implemented, it delivers "regulatory and legal advantages that extend well beyond improved cybersecurity for organizations."[5] However, only 33% of healthcare providers have the NIST cybersecurity framework.[6]

Because these frameworks are highly detailed, manually maintaining compliance can be overwhelming. It is essential your organization selects a robust tool that continuously monitors assets to ensure compliance with security standards, provides alerts to unauthorized changes, and offers recommendations for resolving non-compliance. Solutions that can scan assets for compliance with multiple policies will helping your organization's IT teams increase their efficiency, as your organization can validate its compliance and security posture of various frameworks simultaneously.

USER EDUCATION

While the software tools recommended above will help prevent attacks, educating users cannot be overlooked. Of the top IT Security concerns, 40% of healthcare providers are worried about internal vulnerabilities arising from employee negligence or theft.[7] Locky, which has become a popular ransomware tool for use against healthcare providers, depends on unsuspecting users opening malicious attachments. Other user errors (such as weak or shared passwords, and visiting dubious websites) make end users more likely to make errors that can open doors to attacks. Educating users on best practices, (e.g. secure password management and not enabling macros in word documents—a popular exploit route for Locky) and supporting those practices with security policies should serve to improve your organization's security posture.

The spate of cyber attacks in the healthcare industry and the potential for serious consequences on patient health highlights the need for providers to address cybersecurity as a business issue. Therefore, it is imperative that healthcare providers increase their cybersecurity budget and follow the above recommendations to improve their cybersecurity posture.

REFERENCES

1 Ponemon Institute, *State of Cybersecurity in Healthcare Organization*, 2016

2 Ponemon Institute, *2016 Cost of a Data Breach Study*

3 http://www.csoonline.com/article/3033160/security/ransomware-takes-hollywood-hospital-offline-36m-demanded-by-attackers.html

4 KPMG, *Healthcare and Cybersecurity: Increasing Threats Require Increased Capabilities*, 2015

5 PwC, *Why You Should Adopt The NIST Cybersecurity Framework*, May 2014

6 SANS, *Healthcare Provider Breaches and Risk Management Road Maps: Results of the SANS Survey on Information Security Practices in the Healthcare Industry,* July 2016

7 KPMG, *Healthcare and Cybersecurity: Increasing Threats Require Increased Capabilities,* 2015

tripwire®

◆ Tripwire is a leading provider of security, compliance and IT operations solutions for enterprises, industrial organizations, service providers and government agencies. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business context; together these solutions integrate and automate security and IT operations. Tripwire's portfolio of enterprise-class solutions includes configuration and policy management, file integrity monitoring, vulnerability management, log management, and reporting and analytics. Learn more at tripwire.com. ◆

SECURITY NEWS, TRENDS AND INSIGHTS AT TRIPWIRE.COM/BLOG ◆ FOLLOW US @TRIPWIREINC ON TWITTER

WPHCCU1a 201704