WHITE PAPER

Healthcare Needs Regular Cybersecurity Checkups

SecureWorks

Introduction

Healthcare providers are big on prescribing wellness for patients through regular checkups but fall short when it comes to following a healthy cybersecurity regimen for their networks. Although healthcare providers would never ignore a gaping wound in a patient, in their infrastructures and in those of their business associates, they allow gaping technological wounds to go untreated at the risk of being exploited.

The global growth of Electronic Healthcare Records (EHR) systems and other medical technologies begets new malware designed to exploit their vulnerabilities. To protect itself from exploits that threat actors have developed for the latest technologies, the healthcare industry needs to change its focus from maintaining HIPAA compliance to securing patient data.

Process

People

Intelligence

Technology

Healthcare organizations must work with the right people, processes, technology and threat intelligence to combat zero-day, evasive and advanced threats.

The inability to identify and resolve advanced threats rapidly can result in publicity-generating breaches, business downtime, financial losses and loss of a competitive advantage.

Who should read this white paper

- CISOs/CSOs
- CIOs
- CFOs
- Directors of Security
- Security Researchers
- Security Architects

Threats

New threats are growing so quickly that antivirus technologies cannot keep up with them. The Counter Threat Unit™ (CTU) research team at SecureWorks sees about 300,000 pieces of new malware every day.

Transcontinental maladies are infecting small, medium and large healthcare systems alike. While hospitals and health insurers are still experiencing many breaches, hackers are also focusing on EHR providers with international customers.[1] According to an April 2014 FBI bulletin, EHR theft takes almost twice as long to detect as normal identity theft. Some threats disrupt operations quickly, making it immediately clear that a system has become infected, but others remain quiet in a network for months and then stealthily begin to wreak havoc on an organization's infrastructure. The SecureWorks Incident Response team finds the latter to be the norm, with an average of 314 days before an organization discovers an adversary in its network. This lag time is used to identify an organization's most critical files, which adversaries may later steal or encrypt for ransom. Ransomware is one of the three most common attack vectors against healthcare organizations,[2] and because they cannot function without their critical files, many of them pay a ransom.

Whether hidden or clearly present, most healthcare organizations either have a threat inside their system now or recently had one. Nearly 90 percent of healthcare organizations surveyed in a recent Ponemon study had at least one data breach that they knew about in the past two years, and nearly half (45 percent) had more than five data breaches in the same time period.[3]

As many as 75 percent of U.S. hospitals responding to a poll could have been hit with ransomware in the last year and not even know it, according to an April 2016 *Healthcare IT News and HIMSS Analytics Quick HIT Survey: Ransomware*.[4]

Healthcare Organization Environment

The healthcare industry and its business associates are under siege from the hacker industry. In war, the best strategy is to attack the opponent's strategy. That's what threat actors do. They know that the defense strategy of most healthcare organizations is solely to comply with HIPAA regulations, leaving many vulnerabilities open for attackers to exploit. Compliance alone does not address old vulnerabilities or new ones that stem from new technologies. Threat actors have modified their techniques to breach clouds, medical devices, mobile devices and Wi-Fi networks, and they will continue to adapt their exploits as new technologies emerge. Hospital medical devices like X-ray systems that are connected to the network can be exploited as can data stored in the cloud from medical devices that reside with patients, such as electrocardiograms built into smartphone cases, glucose and heart monitors, and electronic pill boxes that monitor whether patients are taking their medication. With the rise of the Internet of Things (IoT), there will be more things connected to the Internet and more possibilities for breaches of voicemail systems, customer service call-recording systems, closed-circuit television systems, employee personal computing devices and other devices that will affect hospitals and their business associates.

The HIPAA Omnibus Final Ruling says healthcare organizations are potentially liable for business associates that have been breached and have failed to meet compliance with the HIPAA Security Rule. The No. 2 threat to healthcare organizations is business associates that take inadequate security precautions, according to Healthcare Information Security Today's white paper, *2015 Survey Analysis: Evolving Threats and Health Info Security Efforts*. Healthcare organizations should continually inspect what actions their business associates are taking to secure their own networks and those of their subcontractors. Business associates are held responsible for ensuring that any of their subcontractors who send, receive or maintain personal health information follow HIPAA/HITECH legislation. A business associate is directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule.

Understanding the Value of the Data Being Protected

As organizations work to protect their finances, so too must they protect their data. The richness and uniqueness of the information that health plans, doctors, hospitals and other providers handle – social security numbers, credit card information, insurance information, addresses, phone numbers – is the largest part of the U.S. economy and should be considered a matter of national security according KPMG in its *Health Care & Cyber Security 2015 Report*.

Stolen EHR is used to acquire prescription drugs, receive medical care, undergo surgery, procure expensive medical equipment like wheelchairs, acquire government benefits like Medicare or Medicaid, falsify insurance claims, file fraudulent tax returns, open credit card accounts and create entirely new medical identities. The healthcare industry must consider the consequences of a breach when evaluating an investment to minimize the vulnerabilities that threaten the integrity, confidentiality and availability of ePHI. In all instances of a breach of the size that requires public notification, an organization may suffer fines, class action lawsuits, reputational loss, lost revenue due to patients finding another provider and loss of support from stakeholders. Although hospitals can usually recover from a breach and continue operations, patients don't fare so well. The Institute for Critical Infrastructure Technology, a cybersecurity think tank, says in the report, *Your Life, Repackaged and Resold: The Deep Web Exploitation of Health Sector Breach Victims*, "Every patient record compromised has the potential to devastate and financially ruin a United States citizen. . . . The entire brutal impact on the incident that resulted from poor cybersecurity and inadequate cyber hygiene on behalf of the healthcare organization is forced onto the shoulders of the victims to deal with for the rest of their life."

Continuous Oversight

As new vulnerabilities constantly are being discovered from existing software and from new changes to the network and to the website, security needs to be top of mind throughout an organization. The executive management team needs to develop a vision for the organization's security posture and to work with its security team to create an action plan containing strategies and tactics to achieve the vision. The plan should continually strive to improve the people, processes, technology and machine capabilities that revolve around security. Of course, the ultimate objective is to secure data; however, to do that, organizations need to know where their critical data is stored. Without policies and controls in place to contain personally identifiable information, it and other critical data could reside in unexpected locations such as in ZIP files, with business associates and on unsanctioned cloud sites like DropBox and public email servers. To determine all possible locations of the critical information that must be protected, organizations need to assess their operational infrastructure. Once the locations of data have been identified, the following questions should be answered: 1) Who is using the data? 2) How is it being used? 3) How is it being shared? 4) Is it encrypted? and 5) How is it being backed up?

Next, organizations should perform vulnerability scans against all infrastructure assets involved in any use, transmission and storage of this information. Then, to discover potential risks within the network, penetration tests should be conducted using the most current threat intelligence and attack tactics. After the risks have been identified, a risk analysis should be conducted using a formal risk framework like NIST 800-30 to determine the probability of a vulnerability being exploited and the approximate cost of that exploitation. The analysis provides information needed to create a Risk Register, which lists risks and prioritizes them based on probability and liability. These prevention measures are standalone programs that should be performed regularly to ensure the organization is prepared to defend against attempted attacks and to rapidly respond to successful infiltrations.

Organizations must continuously monitor events within the infrastructure for indications of unusual behavior on the part of authorized users as well as unauthorized users. Healthcare providers and their business associates must continuously monitor hardware, software and endpoint activity, and review log files for abnormal behaviors. Reviewing logs only once a day gives threat actors an entire day in a network.

The final element of Continuous Oversight is the Computer Security Incident Response Plan (CSIRP). With threats constantly changing, it's important that healthcare organizations treat their CSIRPs as a living document. A CSIRP that is well rehearsed with tabletop exercises and is updated annually can save time and money. Ponemon Institute's *2016 Cost of Data Breach: United States* study found that those breached organizations with a CSIRP in place had fewer costs than those that did not.[5] The CSIRP should include the contact information for a professional IR team that has been designated to help with a breach. Ideally, organizations will have an IR retainer in place with a professional IR team. In addition to ensuring the IR team will be able to respond within 24 hours of breach notification, the IR retainer will save an organization approximately

$100 per hour in remediation costs. Leveraging an incident response team was the single biggest factor associated with reducing the cost of a data breach, saving companies nearly $400,000 on average (or $16 per record). In fact, response activities like incident forensics, communications, legal expenditures and regulatory mandates account for 59 percent of the cost of a data breach.[6] Part of these high costs may be linked to the fact that 70 percent of U.S. security executives report that they don't have incident response plans in place (The Cyber Resilient Organization: Learning to Thrive Against Threats, Ponemon Institute, 2015). At some point, all networks will be breached, so organizations need to be prepared to get their attackers out quickly.

No organization can rely on preventing attackers from entering its network. Determined hackers will persist until they enter a network and find their desired data or until they decide the time and resource investment is too great. Winning the hacker war is not just about preventing threat actors from entering a network but about removing them before they find valuable data and cause harm. The healthcare of a cybersecurity network may not be a matter of life and death, but an ill network that exposes personal information of patients could affect their lives forever.

For more information, call **(877) 838-7947** to speak to a SecureWorks security specialist.

www.secureworks.com

[1] Scott, James and Spaniel, Drew, Institute for Critical Infrastructure Technology, *Your Life, Repackaged and Resold: The Deep Web Exploitation of Health Sector Breach Victims,* September 2016

[2] Ponemon Institute, *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data,* May 2016

[3] Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon, May 2016

[4] HIMSS, *2014 HIMSS Analytics Cloud Survey,* June 16, 2014

[5] Ponemon Institute, *2016 Cost of Data Breach: United States,* June 2016

[6] Ponemon HIMSS, *2014 HIMSS Analytics Cloud Survey,* June 16, 2014