STRATEGIES FOR GUARDING AGAINST HEALTHCARE CYBER THREATS

The healthcare industry's digital transformation is enabling increasingly mobile workforces to serve more patients with fewer resources. With more than 50 percent[1] of U.S. doctors receiving meaningful use incentives for electronic health records, 44[2] percent of healthcare organizations already hosting clinical apps in the cloud, and more than 40[3] percent of physicians using mobile devices to access protected health information (PHI), patient data is more portable than it has ever been. But along with this lifesaving flexibility come a variety of new challenges – and protecting the confidentiality, integrity and availability of PHI is now mission-critical.

By implementing strategies that prioritize anti-virus, encryption, file integrity and data management, healthcare organizations can leverage in-depth security solutions that will lock down the workstations and mobile devices holding patient data and enforce compliance with HIPAA privacy, breach notification and security rules.

According to a recent webinar, "Emerging Threats in Healthcare & Strategies for Defense," presented by NaviSite, Inc., a leading provider of enterprise-class, cloud-enabled hosting, managed applications and services, the best way to stay ahead of the advanced persistent threats facing the industry – and to begin the dialogue with IT – is to understand the value of the information at risk, as well as the adversaries and different attack vectors they employ when targeting healthcare environments. Developing this understanding will help ensure healthcare organizations not only have the right in-depth security solutions in place, but the people and processes necessary to support their most efficient use within their environment.

Emerging cyber threats

From 2012-2013, HIPAA data breaches rose 138 percent, with medical-related identity theft accounting for 43 percent[4] of all identity thefts reported in the U.S. in 2013. Medical-device manufacturers are being singled out as the primary target in 2014. The reason for all this unwanted attention is simple: healthcare data is approximately 50 times more valuable on the black market than credit card data because it exposes information such as a person's height, eye color and other physical characteristics, which can be used to create comprehensive fake identities[5]. Healthcare security systems, however, are lagging compared to other industries in addressing this problem.

Healthcare data is approximately 50 times more valuable on the black market than credit card data because it exposes information such as a person's height, eye color and other physical characteristics, which can be used to create comprehensive fake identities.

According to a recent FBI Private Industry notification: "The health care industry is not technically prepared to combat against cyber criminals' basic cyber intrusion

Produced in partnership with
HIMSS Media

tactics, techniques and procedures, much less against more advanced persistent threats. The health care industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore, the possibility of increased cyber intrusions is likely."[6]

As of August 2014, the industry has been hit with approximately 204 incidents this year, losing about 6.6 million names and social security numbers in total.[7] "It shows us that the medical industry is a top priority, and we need to work on securing not only the hospitals and clinics themselves, but also the infrastructure that they use internally," said Stephen Coty, chief security evangelist at Alert Logic, which recently teamed with NaviSite to provide relevant security solutions and strategies for businesses to use in preventing harmful cyber activity affecting the healthcare industry.

> The health care industry is not as resilient to cyber intrustions compared to the financial and retail sectors, therefore, the possibility of increased cyber intrusions is likely.

Although HIPPA compliance has improved over the years, with maximum penalties rising on average from approximately $25,000 to $1.5 million,[8] the healthcare industry has gotten out of the practice of using the IT network as its main source of data. Too often, information is stored locally, which means laptops can be compromised through malware, which increases the risks.

Within the past couple of years, the attack vectors aimed at the healthcare industry have changed a bit. Today, medical-device manufacturers also represent a prime target for overseas hackers as corporate- and state-sponsored cyber-attacks become more prevalent.

Another major threat concerns the nascent Internet of Things (IoT), a growing network of everyday objects that can share information and perform tasks. Europol, the EU's criminal intelligence law enforcement agency, has issued warnings concerning the IoT, and the FDA reports that some 300 medical devices are vulnerable to attack.[9]

What hackers want and how they're getting it

Many trusted reports – from Verizon, the Ponemon Institute, Mandiant and others – provide insight into the adversaries and different types of attack vectors that are hitting the healthcare industry. Some of the commonalities found in recent reports include:

- 92 percent[10] of attacks are coming from external sources, where they are trying to infiltrate through a third-party vendor, a small clinic that might have access to a larger provider's network or through large hospitals. Some even social engineer their way into hospitals by distributing free thumb drives that have been loaded with malware.
- Hackers use 76 percent[11] of the intrusions exploited per week as credentials.
- 78 percent[12] of attacks were not particularly difficult to execute.
- 75 percent[13] of attacks were driven by financial motives.
- 69 percent[14] of attacks were actually discovered by external parties.
- 66 percent[15] of these attacks took months or more to discover.
- The average time an attacker spent on the network was 229 days[16] (much longer for research facilities and/or pharmaceutical companies).

Various groups are behind such attacks, and their motivations vary. Most people are familiar with Anonymous, which has been quick to take credit for its distributed denial of service (DDoS) attacks. However, other hacking groups[17] here in the United States as well as Western Europe and various Chinese hacking groups[18] – represent the primary threat to the industry,[19] stealing the bulk of user names and passwords.

Some of the tools of the trade include software such as Zeus, an easy, point-and-click tool that builds the file containing malicious code that can then be uploaded to a network; Citadel, spyware that resides on a computer and silently collects data until the malicious actor's objective is achieved; and Havij, one of the top two SQL injection tools. Havij works by locating a vulnerability, injecting a piece of code on the site and then collecting information such as user names and passwords.

One of the most sophisticated tools being used is a remote-access Trojan. Built for stealing data and intellectual property, this program's interface resembles a Windows menu and comes with a well-

When it comes to deploying security architecture, healthcare organizations should consider three layers of technology: the network, server applications and the host.

written 42-page user guide. Worse, it includes surveillance tools capable of performing audio-, keystroke-, screenshot- and webcam-captures. It also includes a sniffer, which collects all data going in and out of the infected workstation, and a spreader, which starts a service on the workstation that infects all network shares or USB sticks plugged into it.

Strategies to defend against attacks

When it comes to deploying security architecture, healthcare organizations should consider three layers of technology: the network, server applications and the host.

In the network layer, healthcare organizations must have firewalls and access control lists, as well as intrusion detection. Additionally, the security architecture should include deep packet forensics, netflow analysis, network access controls, DDoS and scanners.

In the server/app layer, the focus should be on identifying vulnerabilities, log management, AV, patch management, mail/web filters, scanners and back-up. Log management platforms, for example, are very important because – beyond compliance – they enable the identification of network anomalies.

In the host layer, the emphasis should be on anti-virus protection, encryption, GPG/PGP (encryption protocols for email), file integrity management (FIM), anti-malware, Lo-Jacking and central storage. A proprietary FIM, for example, will guide users through a malware identification process. Once the threat is identified, FIM performs expert system analysis before forwarding it to a certified analyst, who determines if the threat is legitimate or a false positive. Any legitimate incident is then escalated. Ultimately, data correlation is the key.

Recognizing that humans will always be the weakest link in any healthcare organization's security architecture, the establishment of an enterprise cybersecurity team is crucial. This team should monitor and maintain non-managed hardware deployment uptime and collect and maintain content for all non-managed devices. They should implement cybersecurity awareness programs, maintain an incident response team, be responsible for operational implementation of all security infrastructures, and establish a network and application penetration testing and audit team.

Although many healthcare organizations do not have a 24/7 security operation center – most simply partner with managed security service providers for this type of service – the team should be responsible for detecting zero-day and advanced persistent threat attacks, monitoring for intrusions, responding to incidents and working with the cybersecurity team to mitigate the risks that are introduced into their environments.

Partnerships aiding healthcare organizations

NaviSite's partnership with Alert Logic offers a good example of how such partnerships are benefitting healthcare organizations.

> Recognizing that humans will always be the weakest link in any healthcare organization's security architecture, the establishment of an enterprise cybersecurity team is crucial.

Recently, while working with a large health information exchange that was planning to move to a DNA environment in which patient information would be shared, NaviSite architected a solution in a matter of weeks. But the compliance and the security controls the company put in place took more than three months, leveraging two Alert Logic solutions in the process — Threat Manager IDS with ActiveWatch and Log Manager, which also assists with the HIE's compliance needs.

In another instance, NaviSite was working with a customer that had 50 separate locations. When the provider discovered site traffic from China, where it doesn't do business, NaviSite partnered the provider with Alert Logic. Even though the provider managed their firewalls and all its systems were current, it installed the Alert Logic solution. The day after it was installed, the provider received notification that one of its production servers was infected with a Trojan virus called Ransomware. Fortunately, the Alert Logic solution caught this potentially devastating virus and a crisis was averted.

For organizations lacking the resources to maintain a 24/7 security operation center, partnering with a managed applications and services provider is often the smartest way to stay ahead of the advanced, persistent threats targeting healthcare environments.

For more information, visit www.navisite.com.

SOURCES:

1 HHS. http://www.hhs.gov/news/press/2013pres/05/20130522a.html

2 2014 HIMSS Analytics Cloud Survey. http://www.himss.org/library/healthcare-privacy-security/cloud-security/security-survey

3 Deloitte Center for Health Solutions 2013 Survey of U.S. Physicians. http://www2.deloitte.com/content/dam/Deloitte/us/Documents/life-sciences-health-care/us-lshc-physician-adoption-10012014.pdf

4 Redspin Breach Report 2013: Protected Health Information (PHI). https://www.redspin.com/docs/Redspin-2013-Breach-Report-Protected-Health-Information-PHI.pdf

5 http://www.bitglass.com/company/news/press_releases/healthcare-data-breach-report

6 http://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf

7 http://money.cnn.com/2014/08/20/technology/security/hospitals-data/

8 http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page?

9 https://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01

10 Verizon 2013 Data Breach Investigations Report. http://www.verizonenterprise.com/DBIR/2013

11 Verizon 2013 Data Breach Investigations Report. http://www.verizonenterprise.com/DBIR/2013

12 Verizon 2013 Data Breach Investigations Report. http://www.verizonenterprise.com/DBIR/2013

13 Verizon 2013 Data Breach Investigations Report. http://www.verizonenterprise.com/DBIR/2013

14 Verizon 2013 Data Breach Investigations Report. http://www.verizonenterprise.com/DBIR/2013

15 Verizon 2013 Data Breach Investigations Report. http://www.verizonenterprise.com/DBIR/2013

16 Mandiant Report. M-Trends® 2014: Beyond the Breach https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf

17 http://www.bostonglobe.com/news/nation/2014/09/05/health-care-industry-ill-prepared-for-vicious-cyberthreats/ZdvDGaipJi7VSN0TogezkL/story.html

18 http://www.darkreading.com/attacks-breaches/medical-industry-under-attack-by-chinese-hackers/d/d-id/1139365?

19 http://www.nytimes.com/2014/12/02/technology/hackers-target-biotech-companies.html?_r=0

About NaviSite:

NaviSite, a Time Warner Cable Company, is a leading worldwide provider of enterprise-class, cloud-enabled hosting, managed applications and services. NaviSite provides a full suite of reliable and scalable managed services, including Application Services, industry-leading Enterprise Hosting, and Managed Cloud Services for enterprises looking to outsource IT infrastructure and lower their capital and operational costs. Enterprise customers depend on NaviSite for customized solutions, delivered through a global footprint of state-of-the-art data centers.

TIME WARNER CABLE Business Class® | NaviSite®

Produced by
HiMSS® Media

www.himssmedia.com
© 2015