SPONSORED BY FORTINET

wedi™

TECHNOLOGY TODAY FOR A HEALTHY TOMORROW

Perspectives on Cybersecurity in Healthcare June 2015

Workgroup for Electronic Data Interchange
1984 Isaac Newton Square, Suite 304, Reston, VA. 20190
T: 202-618-8792/F: 202-684-7794

CONTENT

DISCLAIMER

While all information in this document is believed to be correct at the time of writing, this document is for educational purposes only and does not purport to provide legal advice. If you require legal advice, you should consult with an attorney. The information provided here is for reference use only and does not constitute the rendering of legal, financial, or other professional advice or recommendations by the Workgroup for Electronic Data Interchange. The listing of an organization does not imply any sort of endorsement and the Workgroup for Electronic Data Interchange takes no responsibility for the products, tools, or websites listed.

The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by the Workgroup for Electronic Data Inter change (WEDI).

Document is for Education and Awareness Use Only

CYBERSECURITY

Perspectives on Cybersecurity in Healthcare

I. INTRODUCTION

In today's connected health environment, cybersecurity is no longer an option or afterthought – it is a critical strategic asset that must be addressed by every organization. Over the past decade, healthcare stakeholders have implemented a health information technology (health IT) infrastructure to access, send and receive electronic health data. However, unlike other industries such as finance, which have already been transformed by technology, many healthcare organizations have not invested sufficiently in robust IT security measures that can protect and encrypt health data in electronic health record (EHR) systems, interfaces, repositories, databases, connected medical devices and personal devices.

Given that medical records contain a wealth of information that can be used for identity theft and fraud (such as social security number, address or claims data), personal health information carries a higher value on the black market than other industries in which only a credit card number can be compromised. Indeed, while a credit card record might fetch $2 on the black market, a medical record can average more than $20. The data value is greater not only because of the data, but also because identity theft is harder to detect and mitigate in healthcare. Unlike credit cards that can be easily cancelled and replaced within 1-2 days, there is often no straight-forward contingency plan for healthcare records once they have been breached.

As a result, the frequency, scope and sophistication of cyberattacks are growing at a worrisome rate in the healthcare sector. Between 2010 and 2014, approximately 37 million healthcare records were compromised in data breaches, but in the first 4 months of 2015 alone, more than 99 million healthcare records have already been exposed through 93 separate attacks. For the first time, the majority of breach activity in healthcare has been a direct result of criminal behavior. Recent estimates suggest that half of healthcare organizations have experienced cyberattacks in the past 12 months, leading to at least $6 billion in costs and damages. Although healthcare organizations have made great progress in leveraging health IT to drive improvements in quality and efficiency of care, they are also increasing exposure to cybersecurity.

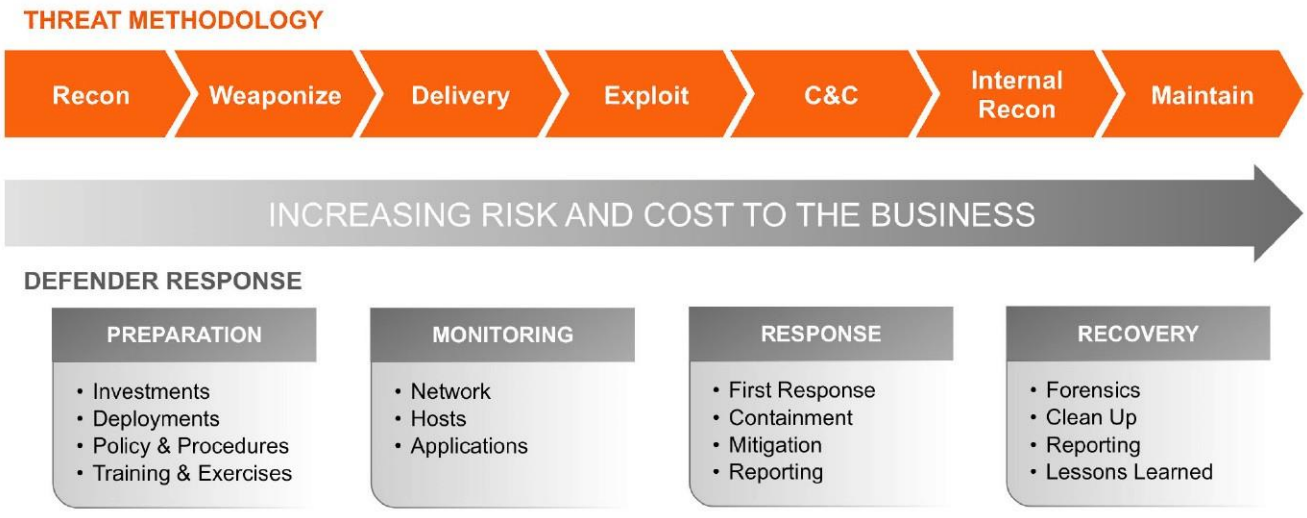
II. PURPOSE OF THIS PRIMER

This primer will briefly illustrate some of the challenges that healthcare organizations face in defending themselves from cyberattacks, and discuss some of the vectors in which they occur.

III. THE LIFECYCLE OF CYBERATTACKS AND DEFENSE

The adoption of new technologies – such as connected medical devices, cloud networks and personal health devices – is transforming the delivery of care as it becomes more decentralized from brick-and-mortar facilities. But in doing so, it has also opened the door to more sophisticated and complex cybercrimes that now occur in the backyard of healthcare consumers where personal health information is regularly accessed, monitored and exchanged. Nonetheless, many healthcare organizations – including hospitals, physician practices and health plans – lack the security, governance or risk management to effectively detect, mitigate and prevent front-line cyber threats. "Cybercrime used to be limited to stolen laptops and USB drives – but today, threat adversaries are exploiting vulnerabilities and human error at a massive scale," observed Tony Giandomenico, Senior Security Strategist at Fortinet. Vulnerabilities can range from administrative (e.g. workforce is not appropriately trained), to physical (e.g. electronic equipment and patient data are easily accessible), to technical (e.g. IT assets are not tracked or audited), to organizational (e.g. no breach notification or response plan). "While organized crime tends to conduct mass attacks driven by profit, government-sponsored attacks can often be more targeted and coordinated in spanning across networks of specific business partners to gather intelligence and account information, " explained Mr. Giandomenico. "Any time that a defense is erected, an attacker will find a way around it - install a lock, they'll break in; build a wall, they'll climb over. A key component of building an effective security program begins with understanding the anatomy of an attack, the methodologies employed by adversaries and lifecycle of appropriate defense responses."

Figure 1: Attacker Defender Lifecycle



IV. THE ANATOMY OF AN ATTACK

Once a potential vulnerability and attack vector are identified, threat adversaries employ a common series of intrusion techniques and methods to gain access to the network of a

healthcare organization. As briefly outlined in the preceding figure, each step of the lifecycle contains specific objectives that are important to consider for defense:

1. Reconnaissance - Adversaries study the network, user behavior and system vulnerabilities to identify weaknesses. Information can be harvested to weaponize a single attack or develop a more advanced multi-tiered campaign.

2. Weaponize – Adversaries build a malicious code that will exploit vulnerabilities and enter a system undetected.

3. Delivery – Adversaries select the best mechanism to deliver the exploit through tactics such as social engineering via phishing, infected websites and malvertising. The more information gained from reconnaissance, the more advanced and layered an attack can be. Phishing schemes are employed to lure recipient targets into supplying confidential information (e.g. username, password) that can serve as entry points to infiltrate an enterprise system or network. Often sent by email with an embedded link to a malicious website for users to click on, phishing can also serve as a vehicle for ransomware attacks, which encrypt data in place and hold information hostage until payment is made before providing a decryption key. Well-designed malware will not trigger any alerts once delivered into a system and because of its polymorphic nature, it can be difficult to effectively detect in real-time. "Once a new piece of malware is detected, there can be as many as 120 different variants within the first hour alone. While variants may differ in look, fee, or digital hash signature, their malicious functionality remains the same," warned Mr. Giandomenico.

4. Exploitation – An exploit is delivered to a user browser or system once a malicious link is clicked or a vulnerability in software or plug-in permits execution of malware. Adversaries will use evasion techniques to avoid detection through a variety of methods, including obfuscation and fragmentation of data into smaller packets, and/or violation of protocols in a way that systems will not understand.

5. Command and Control – Malware will periodically communicate back to command and control servers while adversaries harvest information. Additional malicious tools may be downloaded for further compromises while trying to remain undetected through encrypted communication protocols such as SSL, TOR, ICMP or DNS.

6. Internal Reconnaissance – Because the data that adversaries are looking for is not typically found on the system that is initially compromised, they must move laterally within the network to locate the desired information. After mapping the network and compromising additional systems, adversaries may try to capture administrative rights and access the entire network by installing keystroke loggers and gleaning user credentials.

7. Maintain – Adversaries will seek to maintain a foothold inside the network, exfiltrate data from servers, and install rootkits to hide activity for as long as possible.

V. BUILDING A CULTURE OF PREVENTION

The lack of robust security protocols and standards for data interchange between enterprise systems, medical devices and personal/home health devices can put healthcare organizations at increased risk and exposure. However, by employing a comprehensive threat intelligence strategy, organizations can more effectively, proactively and sustainably defend against threat adversaries. The development of policies, procedures and training can further prevent attacks and raise user awareness to be mindful of clicking links, executing files or sharing account information. "When building cybersecurity capabilities, a Chief Security Officer must be able to identify data in an organizational environment, know the systems, devices and networks on which they are located, and build a security profile around them that addresses potential vulnerabilities," recommended Giandomenico.

A strong cyber defense strategy should address how to prepare and monitor attacks, respond and ultimately recover from breaches. At a minimum, security architecture should be able to stall adversarial efforts, thwart attacks at each phase and facilitate a rapid response. Today, there are several cybersecurity frameworks that organizations may use as guidelines - such as ISO, COBIT and NIST - to develop security architecture. By overlaying these with counter-responses to the tactics, techniques and procedures that a threat adversary may employ, Chief Security Officers can develop a robust defensive infrastructure. Many of these defensive strategies can be broadly characterized into the following three classifications:

1. Mitigate threats before they enter a network by having the basic controls in place -such as ensuring that operating systems and anti-malware, web filtering and antivirus software on servers and endpoints are updated and patched to reduce the risk of vulnerabilities and infections. At a primary level, preventive measures can be employed by implementing layers of firewall technology to stop known attacks. At a secondary level, the potential damage of a breach can be mitigated through automated alerts and notifications that quickly activate appropriate response measures according to security protocols. By training employees and building a culture of cybersecurity from the C-suite down to the trenches, many breaches can be prevented upstream through user awareness of potentially malicious links, emails, websites, advertisements and files.

2. Discover threats that have entered or tried to enter systems. No organization can prevent every cyberattack, but it is important to build a response system that can alert your security staff, rapidly identify a breach and its scope, and notify other enforcement points so that a breach can be contained without extensive collateral damage. Depending on the adversary, an organization may be better served by disrupting and throttling an attack rather than responding with a knee-jerk reaction that tips off an adversary to engage in additional attacks.

3. Respond to any threats that have breached the network. In addition to deploying sandbox appliances which can test and detect novel threats, it may be recommended for some

organizations to deploy internal network firewalls and mitigate an attack once a network has already been breached. Depending on the extent to which data is stored on internal or external servers, organizations may need to develop coordinated responses to a breach with other entities.

The risk of cyberattacks is no longer limited to the IT desk, it is a key business issue that must be addressed by the C-suite. As has been briefly described in this primer, no healthcare organization can be completely immune from cyberattacks and adversaries. However, they can take appropriate measures to erect defenses and integrate cybersecurity into the business environment and culture.

1 jama.jamanetwork.com/article.aspx?articleid=2247135
2 www.idtheftcenter.org/images/breach/ITRCBreachStatsReportSummary2014.pdf
3 www.idtheftcenter.org/images/breach/ITRCBreachStatsReportSummary2015.pdf
4 www.ponemon.org/blog/criminal-attacks-the-new-leading-cause-of-data-breach-in-healthcare
5 Fortinet