IDC
Analyze the Future

IDC TECHNOLOGY SPOTLIGHT

Advanced Network Security to Protect Against Cyberthreats

August 2015

Adapted from *Business Strategy: Thwarting Cyberthreats and Attacks Against Healthcare Organizations* by Lynne Dunbrack, IDC Health Insights #HI251775

Sponsored by Fortinet

Nearly every week, another healthcare organization reports a serious privacy and security breach that has compromised tens of thousands to millions of consumer health records. In the past, these breaches occurred because a mobile device was accidentally left behind in a coffee shop or stolen from an employee's car. Today's breaches involve cybercriminals representing sophisticated organized crime rings and, in some extreme cases, nation states engaging in cyberespionage. Often, the intrusion starts with a phishing or spear phishing attack that involves social engineering. This paper examines the increased threat from phishing attacks on healthcare organizations. It also looks at the role an advanced threat protection framework and FortiGuard services can play in this strategically important security market.

Introduction

Today's healthcare organizations are at greater risk of a cyberattack than ever before, in part because electronic health information is more widely available today than in the nearly 20 years since the Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996. Cybercriminals view healthcare organizations as a soft target compared with financial services and retailers. Historically, healthcare organizations have invested less in IT, including security technologies and services, than other industries, thus making themselves more vulnerable to successful cyberattacks. The value of health information, which can be used to commit medical fraud, is surpassing the value of social security and credit card numbers on the black market, increasing the attractiveness of stealing health information.

Security breaches take many different forms ranging from physical theft and loss of devices to malicious hacking or IT incidents. Following a breach of unsecured protected health information, HIPAA-covered entities and their business associates are required under the Breach Notification Interim Final Rule (IFR) to notify affected individuals, the media (if 500 or more individuals are affected), and the secretary of Health and Human Services (HHS). Since the Breach Notification Rule became effective in 2009, nearly 1,000 electronic data breaches affecting 500 or more individuals have been posted on the HHS Web site (**ocrportal.hhs.gov/ocr/breach/breach_report.jsf**). Historically, loss or theft was the leading cause of data breaches. In the past several years, malicious hacking events have surpassed other types of breaches. Thus far in 2015, there have been 36 hacking/IT incidents reported that have affected more than 93 million individuals, which is 2.4 times as many individuals as affected from 2009 to 2014.

Phishing and the more targeted spear phishing attacks are increasingly common in the healthcare industry. Cybercriminals are very adept at mimicking email from legitimate sources such as an IT department, customer support site, financial institution, retailer, or other trusted organization. Further, it is common to expect invoices and other attachments from a healthcare or insurance provider.

Combine this skill with the fact that people tend to multitask while reading their email on mobile devices with small screens — such as smartphones — and it's easy for phishing attacks to dupe end users. End users may be tricked into clicking on links that download malware onto the users' device (typically keyloggers that record keystrokes) or that redirect them to another Web site where they enter sensitive information or credentials that are recorded for later use by the cybercriminals to infiltrate critical IT systems. IT professionals are not immune to phishing attacks. In the Anthem breach, several IT staff members had their passwords compromised; their credentials were then used to access the corporate network.

Breaking the "Cyber Kill Chain"

The term "kill chain" originated from the military concept of an attack: target identification, force dispatch to target, decision and order to attack the target, and the destruction of the target. Security professionals use the term to describe a targeted attack on IT resources that consists of reconnaissance, weaponization, delivery, compromise/exploitation, command and control, and exfiltration. Disrupting the kill chain can thwart or at least slow down the attack to enable the security team to respond before too much damage is done. A multilayered security approach is required to ultimately stop the attack from advancing and successfully breaching valuable IT assets.

Consider the following scenario: A phishing email is sent to the target. There are multiple points of opportunity to break the kill chain within each step the exploit takes to get into the network (north-south movement) and then traverse the network (east-west movement). The first opportunity to stop the attack is to use an antispam filter to segregate potentially dangerous email for closer review by the recipient in a spam or junk email folder. If the email gets through the antispam filter and the recipient doesn't recognize that it is a potentially harmful email and clicks on the malicious link, the next line of defense is Web filtering. If the Web filtering fails and a connection is made, the malicious Web site launches exploits back to the target. Intrusion prevention should stop the exploit, but if something gets through and a confirmed connection is made, the malicious site will start to send malware. Antivirus detection then becomes the next opportunity to thwart further exploits that could then infect networks, applications, and other IT systems to find valuable data to steal. App control and IP reputation technologies are the final step in preventing exfiltration of data through a command and control server. In the event a cybercriminal clears all of these security hurdles, the healthcare organization will experience a comprehensive security breach that must be detected and remediated.

Benefits of Advanced Network Security

When properly deployed, advanced networking security, including next-generation firewalls, can provide the following benefits:

- **Protection against known and unknown threats.** Next-generation firewalls contain multiple layers of defense: antispam and Web filtering, intrusion and antivirus detection, and app control and IP reputation technologies that protect against known threats. Sandboxing technologies create an additional layer of protection by helping identify and isolate previously unknown threats rather than allowing them free rein throughout the network.
- **Collection of threat intelligence from millions of sensors and threat information sharing.** The global distribution of millions of sensors found in various products and solution sets enables the collection and dissemination of threat intelligence in near real time to real time across multiple threat vectors — Web, network, file, and message. This enables security insights to be delivered across products and solutions sets, as well as across customers and industries.
- **Share cyberthreat intelligence among healthcare organizations.** Cybercriminals are notorious for sharing strategies and tools they use to infiltrate computer systems and evade detection. Healthcare organizations similarly need to band together to share threat intelligence. And they need trusted vendors as well as their products like sandboxing to share threat intelligence within the organization and the broader security community.

Healthcare Trends with Security Implications

Many of the same major trends that promote the widespread deployment of healthcare IT solutions are also making healthcare organizations more vulnerable to cybersecurity threats:

- **More electronic health information is widely available.** The American Recovery and Reinvestment Act of 2009 (ARRA) provided $20 billion in incentive payments for physicians and hospitals to deploy electronic health records (EHRs). Healthcare organizations are intently focused on meeting meaningful use requirements to avoid Medicare payment penalties. As a result, investment in other technology initiatives, including security, often gets short shrift.
- **Healthcare organizations are consolidating.** In an effort to seek competitive advantage through size and access to resources, or to simply survive, a number of healthcare organizations are looking to acquire other healthcare organizations or be acquired. Portfolios expanded by mergers and acquisition activity tend to be more complex and heterogeneous with data siloed in applications scattered across the enterprise. Security measures for these applications vary widely, leaving IT assets as vulnerable as that of the weakest link's security measures.
- **Consumerization of technology is driving adoption of mobile devices.** Healthcare professionals are a highly mobile workforce and increasingly want to use their personal smartphones and tablets at the point of care. Mobile devices require additional security oversight because of their unique vulnerabilities (e.g., loss, theft, introduction of malware to the corporate network). Bring your own device (BYOD) intensifies the complexity of securing mobile devices because both corporate and personal data are stored on the device and end users often download mobile applications with little regard to the risk of also downloading malware with the application.
- **Cloud technology adoption by healthcare organizations is becoming more common.** Software as a service, platform as a service, and infrastructure as a service are attractive means of deploying IT solutions because they reduce IT costs while accelerating speed to value for the healthcare organization. That said, most healthcare cloud deployments are in a private cloud because healthcare organizations are averse to having PHI commingled with customers' data in a multitenant public cloud. Data concentrated in the cloud creates larger targets for cyberattacks.
- **Meaningful use requires health information exchange.** ARRA and its meaningful use requirements require healthcare organizations to share health information to enable population health management, care collaboration and coordination, and care transitions. Healthcare organizations will have to balance sharing health information to meet these new requirements while maintaining patient privacy, which consumers have come to expect. According to the recent IDC Health Insights' 2014 *Cross-Industry Consumer Experience Survey,* 87.5% of the respondents reported that privacy was important (30.3%) or very important (57.2%). However, only 70.7% of the respondents were confident (43.6%) or very confident (27.1%) that healthcare organizations were protecting the privacy of their data. They are also willing to end a healthcare relationship after a breach, including changing their care providers (21.6%) and changing health plans (5%).
- **The new care delivery and reimbursement models require data aggregation for analytics.** The evolving care delivery and reimbursement models, such as patient-centered medical homes and accountable care organizations, will require a technology platform that correctly identifies patients and provider records managed by multiple healthcare organizations' IT systems, facilitates secure exchange of health information among care team members to improve care coordination and collaboration, and combines clinical and financial data to feed the analytics engine and provide a full picture of clinical, financial, and operational performance. Consequently, healthcare organizations will be investing in more technology that collects, aggregates, analyzes, and shares electronic health information among medical trading partners. These data stores will be attractive targets to cybercriminals because they contain information that can be used for both financial and medical identity theft.

Considering Fortinet

Fortinet is a major player in the network security space, supplying network and other security appliances powered by top-rated security subscription services for a wide range of customers including enterprises, datacenters, carriers, and managed security service providers (MSSPs). The company's Advanced Threat Protection Framework encompasses Fortinet solutions that are designed to:

- **Prevent** intrusion by acting on known threats or information
- **Detect** previously unknown threats
- **Mitigate** damage by responding quickly to potential incidents

Using this three-pronged approach, healthcare organizations can thwart cyberattacks and mitigate the potential risk of serious damage to the infrastructure, expensive privacy and security breaches, and loss of reputation and consumer confidence in the ability of the organization to adequately protect their sensitive health information.

Key Fortinet technologies that are instrumental in providing advanced threat protection include:

- **FortiGate**, the company's flagship network security platform, provides entry-level, midrange, and high-end next-generation firewalls.
- **FortiMail** offers an all-in-one solution for inbound and outbound protection for one of the most exploited vectors — email. Antispam, antiphishing, antimalware, and sandboxing capabilities reduce the chance of malware getting in. Outbound inspection technology and identity-based encryption reduces the risk of sensitive data, such as protected health information, from getting out and being compromised by cybercriminals.
- **FortiWeb** shields Web servers, especially public-facing ones, from the exploitation of vulnerabilities and insertion of malicious code. Behavior-based protection learns about your applications to baseline normal activity in order to identify deviations associated with an attack.
- **FortiClient** protects vulnerable endpoints, including mobile devices and medical devices, from malware seeking network access, credentials, or protected health information. Medical devices are particularly vulnerable because their embedded software is often not reliably patched and in some cases (e.g., Microsoft XP) no longer supported. It also enables encrypted and strong (two-factor) authentication to networks.
- **FortiSandbox** provides protection against advanced persistent threats by scanning files and URLs within a secure virtual runtime environment ("sandbox") to determine if they are a threat or not. Customers can opt to share threat intelligence with FortiGuard Labs.

FortiGuard Labs: Identifying Unknown Threats and Thwarting Zero-Day Exploits

FortiGuard is a core component of Fortinet's threat prevention and detection capabilities gleaned from threat intelligence collected from the more than 2.5 million sensors deployed across the Fortinet customer base. Customers can opt in or out of sharing threat information with FortiGuard Labs, the research unit of Fortinet. FortiGuard analyzes 35 million events detected by its sensors and devices every minute across the world, scanning for known and unknown threats to be researched further. Fortinet has strong partnerships with many computer emergency response teams (CERTs) and more than 200 threat intelligence collaborations.

Zero-day vulnerabilities and attacks can wreak havoc when it comes to network security and protecting valuable data assets. They are called zero day because the vendor has only one day (or less) to develop, test, and deploy a patch for a security hole that was unknown until cybercriminals exploit the

vulnerability and launch a zero-day attack. Often zero-day vulnerabilities escape detection by signature-based filters. Multiple layers of network security, particularly sandboxing technologies, can mitigate the risk of zero-day attacks. Suspicious objects are sent to FortiGuard Labs, Fortinet's global threat research unit, to be further analyzed by the company's 175 security researchers and analysts.

Unified threat management requires big data and analytics capabilities to analyze the billions of HTTP and HTTPS queries per day from 35 million devices. FortiGuard Labs has discovered 200 zero-day vulnerabilities since 2006. The company has discovered 51 zero-day threats so far in 2015 and is on track to identify more than 100 by the end of the year. Once a threat has been detected, FortiGuard Labs discloses the security hole to the vendor. While the vendor develops the patch, FortiGuard Labs develops an advanced zero-day IPS signature that is pushed out to all Fortinet customers in advance of the patch release, which helps trap the threat before it infiltrates the healthcare organization's IT systems. This step is an important component of providing advanced persistent threat protection. FortiGuard does not publicly disclose the identified zero-day vulnerability until after the patch has been released, in keeping with its responsible disclosure protocols.

Challenges and Market Opportunities

The market challenges that Fortinet and its customers face can also present opportunities for a company with strong healthcare experience and a broad product portfolio:

- **Data volumes are growing exponentially, creating larger, more attractive targets.** Big data and analytics are driving the aggregation of large PHI datasets. These data sets are not only valuable assets to healthcare organizations but they are lucrative targets for cybercriminals. The black market value for electronic personal health information is greater than credit card data. According to a 2012 report issued by the Healthcare Information and Management Systems Society (HIMSS), a patient health record is valued at $50 compared with $3 for a social security number and $1.50 for a credit card number.

- **Shift from wired to wireless networks.** The proliferation of mobile devices accessing the network, including those devices that belong to patients, their family members, and other parties to whom only guest network access is appropriate, is pushing more traffic to wireless networks. The wide range of endpoint devices, many of which are not under the direct control of the IT organization, creates additional vulnerable points.

- **More advanced, persistent cyberattacks.** The increasing volume of phishing attacks and high-profile security breaches inside and outside the healthcare industry is creating a heightened demand for security products and services. This is both an opportunity and a challenge for Fortinet to keep up with the demand for its services and to stay ahead of the cybercriminals whose attacks are becoming more sophisticated and pernicious.

- **More stringent HIPAA requirements and increased penalties for noncompliance.** As more patient information is moved into EHRs, and made accessible both inside and outside the organization via a range of devices, including mobile devices, the risk of a privacy and security breach rises. The HIPAA Omnibus Rule, which went into effect September 23, 2013, implements the new privacy and security provisions proposed under ARRA's HITECH Act. As a result, privacy breach notification, minimum use, and disclosure reporting requirements become more stringent. The risks and liabilities associated with privacy breaches increase, and annual penalties for violations can total up to $1.5 million per provision, up from $25,000 per provision.

Best Practices

Healthcare organizations should not confuse HIPAA privacy compliance with having adequate security to prevent cyberattacks. The threat landscape is rapidly changing, and healthcare organizations must change their approaches to cybersecurity to keep pace and adequately protect themselves against cyberattacks and the resulting financial, operational, technical, and reputational damages. Healthcare organizations are encouraged to adopt the following best practices, which were identified in the IDC Health Insights report *Business Strategy: Thwarting Cyberthreats and Attacks Against Healthcare Organizations*:

- **Identify assets that would be attractive to cybercriminals.** One of the first steps to protecting the healthcare organization against cyberattacks is to identify the assets that would be attractive to cybercriminals so that internal segmentation firewalls can be strategically placed to provide an extra layer of security should a threat get past perimeter controls. In addition, these firewalls can include deep packet inspection for better visibility into traffic and attacks, thus helping minimize damage and reduce remediation costs by enabling security teams to respond to breaches faster.
- **Take a multilayered approach to security.** Cyberattacks are typically not "smash and grab" type attacks. Instead, cybercriminals and nation-state actors infiltrate their targets often using phishing emails to lure users to open a link or attachment that has embedded malware that then installs itself on the computer and multiplies itself by installing additional malware and creating backdoors to ensure continued access in the event that the first malware is noticed and removed. Once inside the network, the criminals have access to other systems, can steal user credentials and certificates, can explore the systems for sensitive information, and then can exfiltrate or steal that data. By impersonating legitimate users and covering their tracks, they can put off detection for long periods of time. Healthcare organizations need to take a holistic approach to security and install an integrated suite of security technology to both thwart and continue to detect the threat actors focused on stealing the data that resides in your network.
- **Include all devices and device types in the risk assessment.** Any device that is connected to the network or can be accessed remotely should be evaluated for its potential to be exploited by cybercriminals. Devices include medical devices, photocopiers, HVAC, and other operational systems connected to the Internet. Cybercriminals infiltrated Target by stealing log-in credentials from the retailer's HVAC vendor.
- **Be hypervigilant about installing patches.** While it can be a daunting task to keep up with security patches, it is imperative that these known vulnerabilities be addressed, ideally through physical patching but also through IPS shielding whenever a patch is not yet applied.
- **Utilize strong access controls**. There are two steps to increasing the strength of access controls. First, establish multiple checkpoints between locations — with different information types and authorized members who can access them — and then second, ensure that access is controlled with more than a username/password, which is often stolen. Adding a second "factor" such as a physical token or even sending a confirmation message via SMS or email greatly reduces the risk of a compromise from stolen credentials.

Conclusion

Healthcare organizations simply cannot keep up with the level of attacks levied against them by cybercriminals whose arsenal is evolving rapidly with greater levels of sophistication and insidiousness. The proliferation of electronic health information and Internet-enabled devices connecting to the network to access that information is placing additional demands on the network security and exacerbating healthcare business risks. Healthcare organizations should think about security and compliance not just in terms of the technical risk but also in terms of the business risk of

a system failure. What happens to patient care and other services in the event of a systems outage as a result of a cyberattack? What happens if access to mission-critical applications, such as EHRs or CPOEs, is disrupted? What about the damage to the healthcare organization's reputation if there is a privacy and security breach?

Forward-thinking healthcare organizations have elevated compliance from a tactical initiative to a strategic one led by IT and business executives to address these pressing security concerns. To be successful, CISOs must have a combination of IT and business acumen. To dispel the perception of being "Dr. No," CISOs must embrace the role of change agent to enable innovation. Network security and privacy controls should be built into the architecture of new systems rather than retrofitted. Success lies in striking the right balance of security and usability that enables clinicians to have the immediate access to healthcare information that they need to care for their patients.
