IDC
Analyze the Future

IDC TECHNOLOGY SPOTLIGHT

Protect Patient Data from the Inside Out

September 2015

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

Sponsored by Fortinet

Healthcare organizations face thousands of potential cyberthreats on a daily basis. Hundreds of them are potentially dangerous, and at least 10 are so severe that the chief information security officer (CISO) should advise law enforcement of the attack. Advanced attacks are more often than not conducted by foreign cybercriminals, as well as by nation states. That said, healthcare organizations are also at risk of domestic attacks, including on-premise threats. Multiplying points of entry using cloud and mobile technologies make it harder for healthcare organizations to protect the network perimeter. This Technology Spotlight examines the increased threat from cyberattacks on healthcare organizations. It also looks at the role Fortinet's Internal Segmentation Firewall (ISFW) can play in the strategically important healthcare security market to protect patient data from the inside out.

Introduction

Many of the recent high-profile advanced attacks that have compromised millions of consumers' health records were committed by cybercriminals outside the United States. While distance attacks also originate from inside the United States, severe breaches can be launched closer to home as well. For example, breaches can occur if an employee's credentials are compromised via a successful phishing attack and used to access and release data in an unauthorized manner or if a hacker penetrates the network by exploiting a vulnerability in a healthcare organization's guest network via a hotspot in an adjacent coffee shop or restaurant.

A unique concern for healthcare is the proliferation of medical devices, which are vulnerable endpoints as they become more connected to the network and interconnected with healthcare IT systems. Medjacking — the exploitation of vulnerabilities in the embedded systems of medical devices — is becoming more of a concern for healthcare provider CISOs. However, most healthcare organizations have been slow to adequately protect interconnected medical devices. According to an IDC Health Insights survey, only 9.6% of respondents indicated that they had integrated medical devices into their enterprise security architecture and 10.6% had not yet begun this process. A recently issued industry report confirmed that medical devices including insulin pumps, heart monitors, and picture archiving and communication systems (PACS) have been used by cybercriminals as a means of gaining access to healthcare organizations' networks. In three separate cases, medical devices were infected with malware, enabling the cybercriminals to move laterally within the healthcare network to access protected health and other sensitive information. Malware found on the devices included ransomware, Conflicker, Citadel, and Zeus. While the malware could have been used to compromise the operations of the medical devices themselves or to take remote control of the devices, it would appear that the malware was used only to provide backdoor access to the hospitals' networks.

Since most medical devices are closed systems, they are not routinely scanned by the IT security team, and sometimes they are behind a secondary firewall preventing access by the team. The U.S. Food and Drug Administration (FDA) has issued warnings indicating "as medical devices

are increasingly interconnected, via the Internet, hospital networks, other medical devices and smartphones, there is an increased risk of cybersecurity breaches, which could affect how a medical device operates." Specifically, in a 2013 alert, the FDA noted that attacks "could be initiated by the introduction of malware into the medical equipment or unauthorized access to configuration settings in medical devices and hospital networks."

Today's healthcare organization is more complex than ever before with multiple partners exchanging sensitive health information to improve care coordination and collaboration as required by new value-based reimbursement models. Healthcare organizations are relying on cloud and mobile technology to improve access to health information. The proliferating number of access points combined with advanced persistent threats calls into question the reliance on flat network architectures. Once an advanced persistent threat makes it past perimeter defenses in a flat network, it becomes relatively easy for cybercriminals to infiltrate the network because internal traffic is deemed "trusted." Successful attacks could take days to weeks to months to be detected. The vast majority (94.5%) of healthcare respondents to IDC Insights' 2014 *Cross Industry Cyber Threat Survey* claimed that it took a day (41.1%) or one to six days (53.4%) for the attack to be identified.

Internal Segmentation Firewalls: How to Protect the Network from the Inside Out

The first line of defense has always been (and will continue to be) firewalls at the perimeter. These protections include datacenter firewalls and the next-generation firewalls highlighted in the IDC Technology Spotlight *Advanced Network Security to Protect Against Cyberthreats*. If the perimeter defense is successfully breached via spear phishing and duping a user to share his or her credentials, the attacker will essentially have unfettered access to endpoints and devices connected to the network, unless the healthcare organization has deployed an internal segmentation firewall (ISFW). An ISFW further segments the networks and creates virtual fencing around valuable IT assets, providing additional layers of protection to stop threats from spreading quickly once they are inside the network. An apt analogy is locking the front door to protect the house (security at the edge) but also locking up jewelry and other valuables in a home safe to protect them in the event a thief breaks down the door or enters through an open window. An ISFW complements traditional firewall and unified threat management (UTM) technologies, thus providing an additional layer of protection. It is not replacement technology.

Benefits of Internal Segmentation Firewalls

When properly deployed, internal segmentation firewalls provide the following benefits:

- **Protect valuable IT data assets with strategically placed ISFWs.** 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, thus increasing the attractiveness of stealing health information. 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. Cordoning off servers that store protected health information mitigates the risk of an expensive breach that violates HIPAA.
- **Ensure continuous operations.** Many healthcare settings are 24 x 7 operations requiring round-the-clock access to mission-critical clinical applications. In extreme situations, lack of access to essential patient health information could mean the difference between life and death. Thus, uptime, network performance, and reliability are critical considerations when downtime is not an option. Segmenting the network into zones helps prevent it from being brought down in the event of an attack that adversely affects network operations.

- **Protect vulnerable access points.** Networked medical devices are often vulnerable endpoints because of poor security practices, such as hardcoded or default passwords, lack of system hardening, out-of-date patch level, and the absence of cybersecurity tools. They present challenging exposure profiles to cyberthreats. The more common threat is collateral damage from malware. Similar to protecting data assets, strategically placed ISFWs can protect vulnerable access points.
- **Mitigate risk of publicly accessible networks.** Most healthcare organizations provide guest networks for patients and their family members, visitors, and clinicians who may have admitting privileges but are not employed directly by the hospital. Other open networks readily available include third-party-provided WiFi offered by a coffee shop or restaurant collocated in the healthcare organization. ISFWs enable the healthcare organization to monitor and segregate these networks without having to have complete control over them.
- **Help achieve meaningful use privacy and security requirements.** Protecting patient health information from unauthorized disclosure along with protecting the confidentiality, integrity, and availability of the health information is a core requirement for qualifying for the Medicare and Medicaid electronic health record (EHR) incentive programs. ISFWs limit the movement of malware that has compromised user credentials by preventing access to protected health information and other sensitive data and help reduce the impact of the malware on the IT infrastructure overall.
- **Provide an additional layer of protection from business associates.** New care delivery and reimbursement models and meaningful use requirements for health information exchange require new levels of care collaboration and data exchange between entities. Some of these entities may be owned, and some may be loosely affiliated business associates whose security controls are not the most rigorous. An organization is only as secure as its weakest link. ISFWs further enhance a healthcare organization's security position.
- **Sequester successful attacks.** Traditional firewalls are designed to protect the perimeter from attack. Should an attack be successful, such as when credentials are compromised as a result of a phishing attack, the internal segmentation firewall restricts the "east-west" movement of the attack along the network, essentially blocking it from doing more damage and accessing its target.

Healthcare Trends with Network Security Implications

Many of the same major trends that promote the widespread deployment of healthcare IT solutions, including those deployed outside the four walls of the institution, such as remote health monitoring, telehealth, and home health, add pressure in securing the healthcare organization's network:

- **Broader, pervasive mobility and wireless usage within healthcare.** The proliferation of mobile devices accessing the network, including those that belong to parties for whom only guest network access is appropriate, is pushing more traffic to wireless networks that should be monitored for potential malware and viruses.
- **Care team collaboration creating more reliance on mobility and wireless communication.** The highly collaborative and (physically) mobile nature of clinical teams makes the strategic investment in clinical mobility essential for success in the new health economy where providers are reimbursed based on outcomes versus fee for service. Health information exchange, and the security challenges it brings, will play an important role in the new healthcare economy.
- **Bring your own device (BYOD) driving demand for guest networks.** The BYOD trend has serious security implications. Primary concerns among IT executives include the loss or theft of mobile devices containing sensitive corporate data or unencrypted protected health information and the challenge of enforcing security policies on devices that are not owned and managed by IT. While guest networks may mitigate the risk of clinician devices introducing malware to the production network or adversely impacting its performance by streaming video for patient education or accessing large files (e.g., images), bandwidth and performance may be limited.

- **Expansion of telehealth and telemedicine.** Improved broadband and network performance, changes in reimbursement for healthcare services (such as virtual care visits with a physician), and staff shortages are all coming together to encourage the provision of care online. While consumers appreciate convenient access to healthcare services from any device, anywhere and anytime, they do express concern for the privacy and security of that interaction with a healthcare provider.
- **Interconnected medical devices.** Medical devices represent a wide range of technology: MRIs and CT scanners, bedside patient monitoring, ultrasound machines, and embedded devices such as pacemakers and insulin pumps. Any vulnerability in the device's software, firmware, or commercial off-the-shelf software (like the operating system) can be exploited by an attacker or is at risk of a malware outbreak — not because the device is being targeted but because of its poor security posture and exploitable vulnerability as a result of poor patching.
- **Real-time location services (RTLS) transform clinical assets and access management.** The adoption rate for RTLS has increased along with the widespread deployment of wireless technologies for mobile access to healthcare IT systems. Consequently, clinical assets such as medical devices, hospital gurneys, and even patients and clinicians themselves can be tracked using wireless nodes in badges, tags, and readers that send and receive signals respectively via WiFi, Bluetooth, ultrawideband, RFID, and GPS.

Considering Fortinet

Fortinet is a major player in the network security space, supplying network and other security appliances 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 the loss of reputation and consumer confidence in the ability of the organization to adequately protect sensitive health information.

In addition to traditional border firewalls, as well as next-generation firewalls, Fortinet also offers ISFWs, a new category of firewalls designed to protect the network from the inside out. ISFWs enable a healthcare organization to segment the network to protect valuable assets while ensuring optimal internal network performance. An ISFW has three key characteristics:

- Performance — Wire speed, multigigabit network performance
- Security — Continuous "inside out" protection against advanced threats through integration with existing security functions
- Platform — One scalable and versatile security platform plus one management console for end-to-end network visibility and control across all segmentation deployment scenarios

The ISFW can then be placed at strategic points along the network in front of servers that contain protected health information or cloud-based Web applications, thus quickly providing visibility to the traffic flowing in and out of the IT asset.

However, it is not enough to simply have visibility and monitor traffic since analyzing logs and alerts can take weeks or months. Fortinet's ISFW applies threat intelligence from FortiGuard Labs to determine whether malicious activity is occurring. FortiGuard is a core component of Fortinet's threat prevention and detection capabilities, which are gleaned from threat intelligence collected from the more than 2.5 million sensors deployed across the Fortinet customer base. Unknown files and executables can be isolated and sent to a sandbox for further analysis. Fortinet's ISFW works with other Fortinet security products, including email and Web gateways, along with cloud and border firewalls and endpoint access management.

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 volumes of patient health information. These data sets are not only valuable assets to healthcare organizations but also lucrative targets for cybercriminals. The black market value of electronic personal health information is greater than that of credit card data.
- **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 for Intelligently Deploying ISFW

Cyberattacks against healthcare will assuredly increase in number and level of sophistication in the next 12–24 months. As other industries become more proficient at thwarting cyberattacks, cybercriminals will continue to cast their nets wider to find vulnerable information assets to exploit. To fully leverage the additional security levels achieved with ISFW, 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 where the most valuable assets are stored.** Critical data assets are most attractive to cybercriminals — both health information and financial information, which are protected by different federal regulations — and where they are maintained should be inventoried. While this may seem like a self-evident recommendation, many healthcare organizations have disparate

healthcare IT systems with hundreds to thousands of applications in a product portfolio that have never been rationalized. The ISFW should be installed in front of these valuable and sensitive data assets to provide an additional level of network protection.

- **Take a multilayered, holistic approach to security.** Healthcare organizations need to think differently about security and move beyond investing in a series of point solutions. They should consider a holistic approach to security and install an integrated suite of security technology, including ISFW, to both thwart and continue to detect the threat actors focused on stealing the data that resides in their network. New security solutions should be integrated with existing security functions and management consoles.
- **Accelerate recognition and remediation of an attack to minimize business disruption.** Cyberattacks are typically not "smash and grab" type attacks. Instead, cybercriminals infiltrate their targets, often using phishing email 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 on the computer 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 that data. By impersonating legitimate users and covering their tracks, they can put off detection for long periods of time. ISFWs provide additional visibility into network traffic and can quarantine suspicious content, applications, and traffic for further analysis until the activity has been deemed safe.
- **Move from reactive to proactive to real-time security.** Automated risk assessment and threat detection will enable predictive analytics and help identify breaches in real time to proactively mitigate cyberthreats before significant loss occurs. A holistic approach to analytics will facilitate detecting "slow and low" threats that emerge over time.
- **Use security products based on extensive security intelligence.** Cybercriminals are notorious for sharing strategies and tools they use to infiltrate computer systems and evade detection. Healthcare organizations similarly need to leverage the threat intelligence gathered by security service providers in real time to detect cyberthreats, most of which are unknown, targeted, and adaptive to risk and security measures. Look for products that have been certified by third-party testing and certification companies for IT security.

Conclusion

Healthcare organizations are more vulnerable to attacks originating from multiple fronts today than ever before. Threats not only are originating from outside the organization in faraway countries but also are happening on-premise via guest networks and WiFi hotspots offered by healthcare providers to improve the patient experience. Mobile and cloud technologies make it possible to improve access to information from anywhere and at any time, but these technologies, along with interconnected medical devices and RTLS, create more access points that need to be secured and managed. Furthermore, a flat network architecture provides little protection once a threat actor makes it past border controls because internal network traffic is deemed "trusted." Thus, healthcare organizations will need to rearchitect networks to protect valuable data and protect against advanced persistent threats and other forms of cyberattack. IDC believes that the market for internal segmentation firewalls will continue to grow in importance as a means of protecting data from the inside out.