White Paper

Protecting Healthcare Systems and Data From Advanced Attacks

Symantec

Protecting Healthcare Systems and Data From Advanced Attacks

CONTENTS

Brought to you compliments of

Today's healthcare systems are facing a unique set of security, privacy and compliance challenges. The volume of health data is multiplying exponentially day after day, and caregivers, patients and business associates expect to be able to access and share health data securely, from any device. At the same time, federal and state regulatory compliance mandates continue to raise the bar on data protection, and fines for data breaches and compliance violations continue to increase.

TechTarget Custom Media

A TECHTARGET WHITE PAPER

Unique vulnerabilities for health systems

In 2015, the Ponemon Institute reported that health data can sell for as much as $373 per record, making it the most valuable data in any industry.[1] Because health data is worth multiple times more than credit card information on the black market, cyberattacks on health systems have become a lucrative business.

Attacks such as hacking and phishing, as well as malware and viruses spread through email, infected webpages and even social media platforms, are growing more sophisticated by the day, with healthcare companies seeing a 125% rise in cyberattacks in just five years.[2]

Ransomware, or cyberattacks used for corporate extortion, is also on the rise, providing an easy way for attackers to monetize health data–which yields about $33,000 per day.[3] Recent ransomware attacks infected a number of hospital IT systems, resulting in the shutdown of clinical services as hackers broke into core networks, encrypted protected health information (PHI), and demanded payments in return for a key. Several hospitals felt they had no choice but to pay the ransom in order to resume operations quickly, even though security experts agree when organizations pay ransoms, it encourages more attacks.

Hackers have also used medical devices as entry points for attacks. A recent study revealed that researchers found "potentially deadly vulnerabilities in dozens of devices such as insulin pumps and implantable defibrillators."[4] As their numbers increase, networked medical devices are exposed to the same risks as other IT equipment, yet they are typically poorly protected.

Costs and consequences

In recent years, data breaches have cost health systems billions of dollars in regulatory fines, in addition to class-action lawsuits, credit monitoring expenses, brand damage and IT remediation efforts. In some areas of the country, state privacy laws may be even stricter than federal laws and result in additional fines.

Health practices also risk losing customers. Today's consumers have more choices about where to go for healthcare, and the majority of healthcare consumers are concerned

1 *2015 Global Cost of Data Breach Study: Global Analysis*, Ponemon Institute, May 2015
2 "Healthcare cyberattacks see dramatic rise, study finds," Elise Viebeck, *The Hill*, May 7, 2015
3 "Ransomware scare: Will hospitals pay for protection?" Joseph Conn, *Modern Healthcare*, April 9, 2016
4 *2016 Internet Security Threat Report, Symantec*, April 2016

about the security of their medical data.[5] Headlines about data breach incidents at their current providers can drive consumers to other care facilities.

And while cybercrime was once the realm of a select few with advanced skill sets, today anyone can buy attack kits or data, or hire an attack, with hackers for hire dangerously affordable.[6] As recent examples show, modern cybercrime is accessible to anyone, carefully targeted and sophisticated in approach, and it often goes undetected for months or even years.

Why is healthcare security so far behind?

Healthcare as an industry does not fully understand that cyber-risk is really a business risk—not just an IT issue. The emergence of new threats has made it clear that health system security has become a clinical and business problem, as well as an IT challenge.

Part of the challenge is that healthcare is an open culture where the sharing of PHI among clinicians and caregivers is good for the patient. Adding to the problem is healthcare's focus on regulatory compliance, not cybersecurity. After all, it's easier to be prepared for an audit than a cyberattack of unknown form or fury.

As such, investment in data and systems security has not been a priority, resulting in security weaknesses including:

- Medical devices and servers running old software on outdated operating systems.
- Lack of security monitoring and event analysis.
- Clinicians accessing medical data with unsecured personal devices.
- Resistance to security measures, especially if they conflict with or impede efficient care delivery.

What's more, health systems have to defend themselves continuously and do it right all the time, whereas an attacker has to be right only once. And because they are typically understaffed and underskilled, IT and security teams can have a hard time prioritizing and sorting out events to determine what needs immediate attention.

Best practices for health system security

To combat increasingly sophisticated cyberattacks, health systems must take a comprehensive approach to health data security. A best-practice strategy includes:

5 "80 Percent of Patients Worry About Health Data Security," Bruce Jaspin, *Forbes*, Dec. 4, 2014
6 "Hacker-for-Hire Market is Booming, Says New Report," Nicole Hong, *The Wall Street Journal*, April 5, 2016

- Finding, prioritizing and fixing threats across endpoints, networks and email.
- Blocking known and unknown threats at endpoints and virtual desktops.
- Protecting against spam, spear phishing and malware that enter via email.

To achieve this, it's critical that healthcare IT follow these key practices:

- Secure the entire stack, not just parts and pieces of infrastructure.
- Gain a complete understanding of the infrastructure and network, and what needs protecting—a task that's difficult in a bring your own device (BYOD) culture.
- Automate security with a system that is reliable and fast at high volumes.
- Inventory hardware and software, and automate updates.
- Explore what needs funding and where to invest regarding security, and engage executives across all stakeholder groups.
- Engage professionals with experience in security and healthcare who can help you correlate events across multiple control points.

Symantec Advanced Threat Protection: Preventing data breaches before they happen

Symantec has a broad range of threat protection solutions that can help health systems prevent data breaches before they happen.

Symantec Advanced Threat Protection

Symantec Advanced Threat Protection allows you to expose, prioritize and remediate advanced threats across endpoints, networks and email, all from a single console. You can scan for attack artifacts across the infrastructure, drill into the details of an attack, prioritize compromised systems and quickly remediate—all with the single click of a button. Advanced attacks can be contained in minutes, rather than weeks or months.

Symantec Endpoint Protection

Symantec Endpoint Protection provides unrivaled protection for endpoints and virtual desktops to block all known and unknown threats. Endpoint Protection combines global telemetry from one of the world's largest cyberthreat intelligence networks with local customer context across endpoints to uncover attacks that would otherwise evade detection.

Symantec Hosted Email Security.cloud and Messaging Gateway

Symantec Hosted Email Security.cloud and the on-premises Messaging Gateway protect against email-based attacks including spam and spear phishing. This technology leverages one of the world's largest cyberintelligence networks and Skeptic scanning technology to block unwanted email and safeguard cloud-based email, Office 365, Google Apps, and more.

Email Security.cloud and the on-premises Messaging Gateway analyze the email body, subject and headers, as well as text within document attachments, to identify and prevent loss of confidential data. Policy-Based Encryption seamlessly encrypts email to protect confidential communications, while Image Control scans emails and attachments to identify and block inappropriate images from entering or leaving the organization.

Web Security.cloud

Web Security.cloud helps protect your organization from compromised websites and malicious downloads, and allows you to control, monitor and enforce acceptable use policies for users, whether on-premises or away from the office. Automatically updated antimalware layers block threats safely away from your network, while URL filtering policies and traffic limits prevent Web misuse and help protect your bandwidth.

Conclusion

Healthcare systems face an increasing and unique set of security, privacy and compliance challenges: New threats and attacks are growing in frequency and complexity, IT is often underskilled and understaffed, and healthcare leadership has yet to realize the realities of the costs and consequences of data breaches. To meet the challenges of modern healthcare IT security, health systems need holistic solutions that don't disrupt workflows. Symantec Advanced Threat Protection solutions allow you to expose, prioritize and remediate threats quickly and easily from a single console, and provides full visibility of threats across your entire network.

More Information

Visit our website

www.symantec.com/healthcare

Contact Us

1-855-487-1449

About Symantec

Symantec Corporation (NASDAQ: SYMC) is the global leader in cybersecurity. Operating one of the world's largest cyberintelligence networks, we see more threats and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives.

Symantec World Headquarters

350 Ellis Street
Mountain View, CA 94043 USA
1-866-893-6565
www.symantec.com