WHITEPAPER

HEALTHCARE SECURITY STRATEGY: A DEFENSE-IN-DEPTH APPROACH

> The cost of a security breach is higher in healthcare than in other industries. Healthcare organizations need a comprehensive approach to security.

888-435-7986 | www.getgds.com

GLOBAL DATA SYSTEMS

INTRODUCTION

Healthcare cyberattacks and data breaches have become an all-too-frequent occurrence.

An Industry Under Siege

According to the 2019 Healthcare Data Breach Report from HIPAA Journal, there were 510 healthcare data breaches exposing 500 or more records in 2019. That's a 37.4 percent increase over the preceding year. In a recent HIMSS survey of hospital IT security leaders, 82 percent reported that their organization had suffered a "significant security incident" in the preceding 12 months.

The Healthcare Sector Has Inadequate Security Measures

Cybercriminals target the healthcare sector to get hold of highly valuable information. Experts say a Social Security number nets less than a dollar on the black market, while a payment card number is worth about $5. A complete healthcare record, on the other hand, can be valued at up to $250 because it includes multiple elements of an individual's identity. It also enables criminals to obtain healthcare services and valuable equipment and drugs for personal use or resale, and such fraudulent activity is difficult to detect.

Healthcare organizations store increasingly large volumes of sensitive data due to the transition to electronic health records (EHRs). That data is often maintained in multiple clinical, operational and payment systems, making it difficult to protect. The growing use of mobile devices and network-attached medical equipment has broadened the attack surface and created new points of potential data loss.

However, the healthcare sector has a reputation for inadequate security measures — a recent Gartner survey found that healthcare organizations dedicate just 5 percent of their IT budgets to security, last among 13 industries surveyed.

What You'll Learn

The cost of a security breach is higher in healthcare than in other industries given that patient safety may be at stake. Healthcare organizations need a comprehensive approach to security that addresses the most significant threats. This whitepaper will explain how a defense-in-depth strategy based upon fully managed security solutions can enable healthcare organizations to boost their security posture efficiently and cost-effectively.

Top Healthcare Threats

Effective cybersecurity begins with an understanding of the most significant threats. In the healthcare industry, these six threat vectors account for the vast majority cyberattacks:

Ransomware. A report from Emsisoft found that 80% of identified ransomware attacks targeted U.S. healthcare providers. Healthcare organizations are attractive targets because they tend to be willing to pay up to regain access to their data. Unlike other industries that might lose revenue or customers due to an interruption, ransomware attacks are literally life-and-death matters for healthcare organizations.

Phishing: Cybercriminals frequently use phishing emails to gain access to a healthcare organization's systems. According to the IBM X-Force Threat Intelligence Index 2020, about 30 percent of healthcare security breaches originated in a phishing attack. Because phishing emails use social engineering techniques to dupe users into opening malicious links or attachments, human error plays a key role in these attacks.

Risky User Behavior: In addition to being lured in by phishing emails, users in healthcare organizations often engage in risky behavior that puts systems and data at risk. For example, users may store data on consumer-grade cloud platforms or attach unencrypted information to emails. Malicious insiders who steal data when they leave the organization are a very real threat in healthcare.

Vulnerable Systems and Devices. Healthcare organizations are increasing their use of mobile devices for clinical applications, and many medical devices are now connected to the wired or wireless network. This creates a larger attack surface and the risk that data will be exposed if a device is compromised. Legacy medical devices often run older operating systems and applications that are vulnerable to attack.

Stolen User Credentials. The IBM-X-Force report found that stolen credentials were used in 29 percent of data breaches. When attackers use legitimate credentials to gain access to systems, they can steal data and even disable security systems as they move through the network. These types of attacks can be very difficult to detect.

Third-Party Attacks. The 2019 Healthcare Data Breach Report found that 23.33 percent of healthcare data breaches "involved business associates to some extent." For example, the 2019 attack on American Medical Collection Agency exposed more than 26 million records across 24 healthcare organizations. According to the Ponemon Institute, the average cost of a data breach rises by more than $370,000 if a third party is the source.

Rise of Telemedicine Comes with Increased Risk

Telemedicine uses video conferencing and other technologies to enable real-time, two-way consultations between doctors and remote patients. Studies have shown that telemedicine can increase staff efficiency and reduce costs while simultaneously improving quality of care, patient satisfaction and clinical outcomes. According to the American Medical Association, telemedicine usage is growing at better than 50 percent a year.

However, telemedicine can introduce alarming security risks. Telemedicine security must address multiple attack surfaces, including wireless LANs, IP networks, cellular networks, video conferencing platforms, PACS & a plethora of connected devices.

THE DEFENSE-IN-DEPTH APPROACH

> **Traditionally, organizations have used a fortress strategy to protect their IT assets. Firewalls, intrusion detection systems & other perimeter defenses are deployed to keep outside security threats from getting inside the network.**

However, the growing mobility of employees, diversity of network-connected equipment and increasingly complex interconnections with business partners have combined to make network boundaries fluid. **Healthcare organizations cannot assume that the network is safe because it's protected from the Internet.** Attackers can very quickly find any vulnerability that allows them to gain access to the network.

A new approach is needed, one that integrates security controls throughout the IT environment. **This philosophy, known as defense in depth, requires that organizations consider every possible avenue of attack.** Perimeter defenses are still vital but must be supported by an array of security tools in a layered approach. If one control fails, there are others in place to step in and thwart an attack.

A true defense-in-depth strategy questions the integrity of every device attempting to access the network. Malicious email is blocked before it reaches users' inboxes and content is continuously monitored to detect unusual behavior that could indicate a stealth attack. Email is encrypted to prevent the exposure of sensitive data.

These security controls must work together in an integrated approach. Because today's blended threats use a variety of techniques to exploit multiple vulnerabilities, security tools must be able to share data and track activity across multiple systems.

Too Many Security Tools Can Actually Increase Risk

In a recent survey of cybersecurity and IT professionals conducted by Enterprise Strategy Group (ESG), 78 percent of respondents said their organizations use more than 50 different cybersecurity tools, with 37 percent using more than 100. However, more tools do not equate to stronger security. The ESG survey finds that security tools are often misconfigured, leaving organizations vulnerable to cyberattack. The alerts generated by these tools also create "noise" that makes it difficult for IT teams to identify and prioritize the most serious threats.

How to Implement a Defense-in-Depth Strategy

Many healthcare organizations have added security products in response to specific threats or to protect specific systems, creating an overly complex environment that's difficult to manage.

A defense-in-depth strategy begins with an assessment of the IT environment to identify the most serious threats and any gaps in cybersecurity that could elevate risk. Armed with that information, the organization can prioritize investments that will have the greatest impact. Generally, a layered security environment includes the following controls:

Perimeter security: The network perimeter should be protected by one or more next-generation firewalls (NGFWs) that use application-aware deep-packet inspection to filter traffic. The NGFW should be complemented by an intrusion prevention system (IPS) that uses known signatures, anomaly detection and threat intelligence to spot and automatically block attacks that attempt to evade traditional security tools.

Content filtering: Content filtering restricts the flow of malicious or undesirable content over the network and prevents users from accessing inappropriate websites. It can help prevent a wide range of attacks and reduce legal and regulatory compliance risks.

Access controls. Identity-based and device-aware access controls enable the enforcement of policies according to the user, device type, location and other criteria. Access control solutions should continuously monitor all processes and file activity to detect and mitigate threats.

Data loss prevention: A data loss prevention system prevents users from performing risky activities, such as sharing unencrypted information via email or uploading documents to cloud storage. A highly configurable data loss prevention engine continuously monitors sensitive data and provides automated, policy-driven actions to reduce the risk of a data breach.

Email security: In addition to preventing phishing and other attacks from ever reaching users' inboxes, best-in-class email security tools use continuous analysis to determine if delivered emails could be malicious.y attacks begin with a phishing email that contains a malicious link or attachment that launches malware that is capable of evading traditional defenses.

Fully Managed Security Tools Provide the Best Defense

Cybersecurity is not a "set and forget" proposition. Simply implementing security tools is not enough — they should be monitored around the clock by experienced professionals who can rapidly respond to attacks and kept up-to-date as new threats emerge. However, this requires significant IT resources that many healthcare organizations lack in-house. That's why it makes good business sense to partner with a managed security services provider. GDS delivers all of the security tools healthcare organizations need as a fully managed service. Each solution includes best-in-class hardware and software backed by 24x7 monitoring, management and support by cybersecurity experts. GDS will keep the tools up to date as new threats emerge and the IT environment changes. The GDS team will also respond rapidly to security incidents to minimize the impact of a cyberattack.

CONCLUSION

Healthcare organizations are attractive targets for cybercriminals looking to get their hands on valuable data. That's why it's critical to develop a defense-in-depth strategy and maintain effective security policies and architectures throughout the enterprise.

In addition to protecting the network perimeter, **healthcare organizations must implement an array of security tools** that embed security throughout the IT environment. These tools must work together in a layered approach — if an attack gets past one defense, the remaining security controls should be able to detect and block it.

The security environment must be monitored and managed to ensure up-to-date protection against the latest threats and rapid response to incidents.

However, **many IT teams are scrambling to support growing numbers of locations, users and devices,** while ensuring performance and availability of systems and applications. Fully managed security solutions can relieve the pressure on in-house IT staff by with 24x7 monitoring, management and support by security experts.

GLOBAL DATA SYSTEMS

Protect Your Organization Against Cyberattacks

Contact Global Data Systems: 888-435-7986