WEBCAST HIGHLIGHTS

HIPAA Data Security Best Practices

Healthcare providers face an onslaught of cybersecurity risks and threats. From cybercriminals infecting systems with ransomware to employees disclosing ePHI, a provider's security team is often hard pressed to keep the organization secure.

According to Sentara Healthcare Vice President and Chief Information Security Officer Dan Bowden, the best way to protect patient information and stop ransomware attacks is to adopt and deploy HIPAA data security best practices.

In a recent *HealthITSecurity.com* webinar, Bowden explained that the first step for healthcare organizations is to join the National Health Information Sharing and Analysis Center (NH-ISAC). NH-ISAC is a non-profit, member-driven organization offering health sector stakeholders a forum for coordinating, collaborating, and sharing physical and cyberthreat intelligence and best practices.

"NH-ISAC has been an invaluable tool to what we do at Sentara. We have it built into our process that our team grabs the notices that come out and treat those as threat intel. You have a lot of really smart people on those threads who are willing to collaborate and share great information," Bowden said.

The top threats to healthcare organizations include phishing, malware/ransomware, insider threats (malicious or nonmalicious), lost or stolen devices containing ePHI, and unmanaged vulnerabilities.

To combat phishing attacks, Bowden recommended deploying Domain-based Message Authentication, Reporting, and Conformance (DMARC), tagging external inbound email, conducting anti-phishing campaign and training, using two-factor authentication, focusing on detection and reporting, and automating response and recovery.

The DMARC protocol is designed to identify forged email sender addresses that appear to be from legitimate organizations by providing the exact domain name in the "From:" field of email message headers.

"DMARC helps you combat spearphishing. It makes it much more difficult for someone to send email into your system that looks like it came from inside your organization," Bowden explained.

External inbound email tagging provides a warning to the recipient that the email is coming from the outside. Bowden said that using tagging significantly decreased the percentage of employees who clicked on "malicious" links during phishing campaigns, from a click rate of 12- to 14-percent down to 2 percent.

Bowden explained that detecting and reporting tools for phishing attacks provide useful analytics, such as how many phishing emails came in, how many where clicked on, and how they were disposed of.

"These tools help quantify the threat to help the organization understand when more controls are needed to thwart attacks," he said.

The Sentara CISO also recommended automating the response and recovery for phishing attacks, including blocking URLs and triaging file attachments.

This year's Verizon DBIR found that ransomware accounted for close to three-quarters of malware incidents in healthcare. To thwart ransomware attacks, Bowden recommended that organizations adopt the NIST security pillars: identification, protection, detection, response/containment, and recovery.

HealthIT Security

WEBCAST HIGHLIGHTS

While technical requirements under HIPAA help inform data security best practices, they do not provide detailed prescriptions for covered entities to follow to secure sensitive health data across the continuum of care.

Sentara Healthcare Vice President and Chief Information Security Officer Dan Bowden detailed the integrated health system's efforts to comply with HIPAA and protect sensitive files and patient information wherever and whenever accessed in a recent HealthITSecurity.com *webcast.*

SPONSORED BY

helpsystems

Xtelligent Media

- Identify assets, threats, and vulnerabilities
- Deploy protection, such as antimalware software and network segmentation
- Use tools that enable detection of anomalies and command and control events and security operations center monitoring
- Respond and contain ransomware attacks by triaging and taking action (Bowden supported holding table top exercises to see what impact the planned response and containment has on clinical availability of systems)
- Have a recovery strategy and a business continuity plan in place

According to Verizon, privilege misuse, errors, and lost and stolen devices account for 80 percent of healthcare breaches last year. The report also found that 68 percent of threat actors are internal. To counter insider treats, Bowden backed using privileged access management (PAM). "Doing PAM well is probably more difficult than doing two-factor authentication well. You must get to know who does what on your IT organization. You'll need to make a detailed list of who should have access to what," he said.

In addition, he recommended deploying an EHR patient record access monitoring tool which enables an organization to provide a patient with an accounting of who accessed their records and ensures that staff members are only looking at records that they are authorized to access.

Then there's the matter of lost or stolen devices. "I keep thinking one day something will happen and we don't talk about this anymore. Until then, the problem is still very prevalent," Bowden observed. He advised organizations to use encryption for laptops, mobile phones, tablets, and USB devices and to acquire a sanctioned, business associate agreement-based cloud storage solution to prevent the unauthorized use of USB drives. In addition, organizations should utilize encryption for data in motion as well as data loss prevention tools, so they know what is going in and out of their Software-as-a-Service (SaaS) storage environment, he said.

Given the ubiquity of software vulnerabilities, providers must work diligently to address these potential target vectors. Securing medical devices from vulnerabilities entails creating inventories of devices, identifying the unique threats and vulnerabilities of specific device, and determining whether to patch the vulnerability or block the exploit. Bowden recommended subscribing to a threat intelligence service and running scans on any threats that are highlighted by the service. He also supported developing policies and procedures for dealing with vulnerability management.

"You can't patch everything. You need to document compensating actions if you can't patch something," he said. These actions include segmentation, locking down TCP/IP ports, and app whitelisting. "If you are going to have an exception to the policy, document the exception and how long it will be in place, or if there is an item that you have decided is going to be an ongoing accepted risk, that needs to be documented as well.".

Regarding two-factor authentication, Bowden advised organizations to adopt the technology for all the people with remote access as well as all remote access points. If the organization decides to have an exception to this remote access policy, it needs to document that exception so that people know for whom or for which remote access point the exception applies and how that is going to be managed, he stressed.

"If you mature your data security best practices and tools quarter after quarter, you won't be an easy target, like a sitting duck. Instead, you will be a high, fast-flying duck that is difficult to shoot down," Bowden concluded.

ABOUT THE SPONSOR

helpsystems

HelpSystems aligns IT and business goals to help organizations build a competitive edge. More than 13,000 organizations around the world rely on HelpSystems to solve their most pressing challenges and keep business running smoothly every day.

GoAnywhere MFT is a HelpSystems file transfer solution that uses OpenPGP or AES encryption and industry-standard protocols to comply with HIPAA and HITECH regulations. The software exchanges files via batch, collaboration, and ad-hoc methods, uses workflows to execute tasks before and/or after transfers, and offers healthcare teams multiple options for secure data exchange. Try a 30-day trial at www.goanywhere.com/trial.

Xtelligent Media