Health Information Security in the age of EHRs and the 3rd Platform

White Paper

Introduction

The last time Health Information Technology (HIT) changed this quickly was when barcoding was introduced to HIT networks in the 1990s. While the federal government pushes adoption of Electronic Health Records (EHRs), patient engagements are migrating to smartphones, tablets, and social media. Healthcare providers are also using cloud computing to analyze "big data" collected about treatments and procedures. Together "big connectivity" and cloud computing along with social media are being hailed as the "3rd Platform;" the successors to mainframe and client-server computing architectures. The challenge is how to add EHRs and 3rd Platform services to HIT mainstay services like email, Web access, and other applications while maintaining privacy for HIPAA compliance in today's high-risk environment.

As evidence of today's risk, the Department of Health and Human Services' Office for Civil Rights reported that 2016 was a record-breaking year, with more data breaches reported since they started publishing healthcare data breach summaries in 2009.[1]

Since 2002, Barracuda Networks' strategy has been to protect and simplify diversifying IT infrastructures by converging security, performance optimization, and data loss prevention (DLP) features in solutions that are easy to deploy and manage. This white paper deals with the security and DLP issues facing IT professionals in the healthcare industry and how Barracuda technology addresses these issues.

EHRs: Security, Storage, and Compliance

Three issues to consider when you deploy EHRs are: avoiding data breaches by blocking cyber-attacks on the EHR application, demonstrating "meaningful use" of EHRs for certification, and providing safe, economical backups for a fast-growing volume of EHR data. The following sections address these topics.

Protecting EHR Software and Other Web Applications

Any Web application that accepts input from users, such as EHR software, is vulnerable to a variety of attacks including SQL injections, cross-site scripting (XSS) and denial of service among others. For example in a code injection attack, instead of entering personal data into a Web form, an attacker enters a bit of SQL code that pulls patient data from the database. This type of attack generally happens in stages starting with surveillance of the website to determine vulnerabilities.

The Barracuda Web Application Firewall disrupts application attacks at three stages. To disrupt surveillance, it cloaks websites to hide clues such as error messages that help attackers figure out the next stage of the attack. Next, it inspects user input to the application to block code injections, cookie tampering, DoS, and other attacks. Lastly, it inspects all outbound application traffic to prevent sensitive information from leaving the network, even if the data is accidentally left in the open. The Barracuda Web Application Firewall also delivers essential DLP protection against data theft and accidental exposure when using EHR software and other Web applications.

To safeguard applications hosted in the cloud, the Barracuda Web Application Firewall is available as a virtual appliance and as Security as a Service (SaaS) on the Microsoft Azure and Amazon Web services cloud platforms.

[1] *Reference: http://www.hipaajournal.com/2017-shaping-up-to-be-another-record-breaking-year-for-healthcare-data-breaches-8761/*

Reporting for EHR Certification

Along with protecting EHR software and other applications, Barracuda Web Application Firewalls can be easily configured to automatically create detailed application activity reports. These reports can be helpful for documenting meaningful use of EHRs in support of certification and compliance audits.

Optimized Data Backup for EHRs

Converting patient records from paper to digital puts undue burden on data-backup resources, driving up costs. Going digital also makes patient information vulnerable to theft and accidental leakage if backup tapes are lost during shipping and storage. Barracuda Backup reduces the burden of data backup by deduplicating and compressing data before backing up data on an onsite appliance and offsite in secure cloud storage.

Barracuda Backup typically reduces the amount of data entering standard network backups by 20 to 50 times compared to tape backup systems, which more than compensates for the data EHRs add to backups. Barracuda Backup also encrypts backup data to strengthen HIPAA compliance.

Together, the Barracuda Web Application Firewall and Barracuda Backup provide critical functionality and safeguards for coping with the added burden and risk of deploying EHRs.

Strengthening Security for HIPAA Compliance

Email: Preventing PHI Data Leaks

Email remains a prime conduit for malware infections, phishing, and other attacks on the email server and the network, resulting in data theft. Also, many administrators fail to consider when well-intentioned employees send emails where the body or attachment contains PHI. Even in these cases, your organization has violated HIPAA and possibly PCI-DSS regulations as well.

The Barracuda Email Security Gateway blocks malware, phishing, DoS and other threats from reaching the email server. Next, it scans all outbound email traffic to block theft and accidental exposure of sensitive PHI and credit card information. Lastly, it integrates an email encryption service (at no added cost) so healthcare providers can safely send sensitive information to patients via email without compromising PHI or payment information.

Web Security

The Web is another major source of data insecurity. It's a vector for spyware that can target PHI and credentials from users including healthcare administrators. Additionally, Web applications used in social media can be a venue for users to expose PHI, credit card numbers, and other personal information accidentally, or maliciously resulting in HIPAA violations.

The Barracuda Web Security Gateway blocks users from downloading spyware to block user-based data breaches. Barracuda Web Security Gateway's extended web application monitoring (WAM) also inspects Web traffic for HIPAA-related medical terms as well as other personally identifiable information (PII) such as social security and credit card numbers. The Barracuda Web Security Gateway reports WAM violations to network administrators for follow-up. It also provides Web security and, if desired, granular content policy enforcement to all networked devices including smartphones and tablets using agents and apps.

Security for Cloud Computing

To protect cloud-based applications, Barracuda offers Barracuda NextGen Firewalls and Barracuda Web Application Firewalls as virtual appliances compatible with leading hypervisors. Barracuda NextGen Firewalls and Barracuda Web Application Firewalls are also available to protect cloud-based applications and infrastructure hosted on Microsoft Azure, Amazon Web Services, and Google Cloud Platform (NextGen Firewalls only) in the form of Security as a Service.

Gateway Security for Instant HIPAA Compliance at Multi-Site Organizations

For large-scale healthcare providers such as HMOs and integrated delivery systems who require the comprehensive security only a network security gateway can provide—and need streamlined central management—the Barracuda NextGen Firewall with the Barracuda NextGen Control Center is ideal.

At the LAN level, the Barracuda NextGen Firewall integrates with Active Directory to enforce user -aware policies that govern security, applications, connectivity, and content for wired and wireless networks. The Barracuda NextGen Firewall also provides VPNs for secure site-to-site connectivity and for secure remote access by users, which is essential for preventing data leakage over non-secure channels.

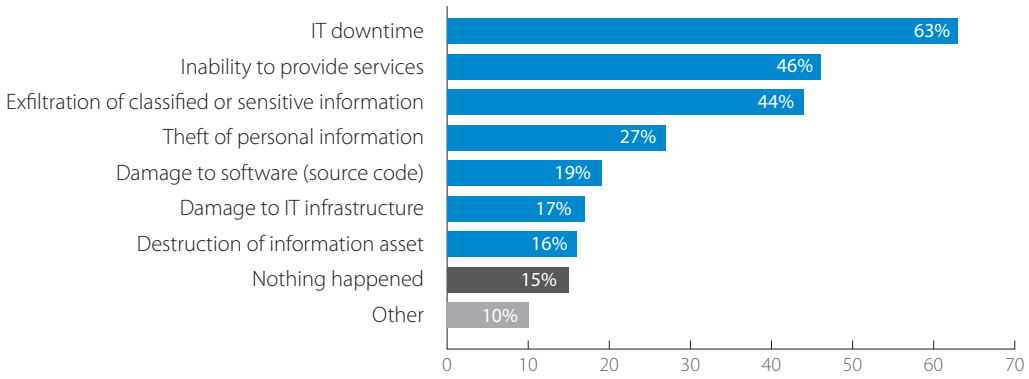
The Barracuda NextGen Control Center makes pushing user and application-aware policies to Barracuda NextGen Firewalls at distributed locations and configuring VPN tunnels among remote sites very easy to minimize impact on HIT staff requirements. The Barracuda NextGen Control Center eases the administration of highly complex and distributed deployments and keeps the total cost of ownership low. The role-based central management includes all functionalities provided by Barracuda NextGen Firewalls and Barracuda NextGen Network Access Clients, which are dedicated VPN clients available for Windows, Mac OS X, and Linux systems.

For cloud computing, the Barracuda NextGen Firewall is available as a virtual appliance and Security as a Service on Microsoft Azure, Amazon Web Services, and Google Cloud Platform.

Consequences of APTs and Zero-Day Threats

With the preceding framework for security in mind, it's worth noting that the number of security breaches continues to grow. A recent Ponemon study[2] surveyed 535 IT security practitioners from both private and public healthcare institutions and government agencies. When asked, "What happened as a result of the APTs or zero-day threats" (Note: more than one response permitted), respondents said that the following consequences occurred:

[2] *Reference: https://cdn2.esetstatic.com/eset/US/resources/docs/white-papers/State_of_Healthcare_Cybersecurity_Study.pdf*



As you can see, the infiltration of advanced threats is not only costly, but also creates a great risk to patient care. The ability to secure your threat vectors (network, email, web, mobile users, and web applications) against today's advanced threats has become increasingly challenging.

To help you secure your vectors, Barracuda offers Barracuda Advanced Threat Protection (ATP). It's a cloud-based service that provides in-depth defense against ransomware, malware, and advanced cyberattacks. It consists of multiple layers of detection technology, including signature, static, behavioral analysis—all the way to comprehensive sandboxing to provide accurate detection of a variety of polymorphic attacks. This service integrates with all Barracuda security solutions, protecting specific threat vectors across any deployment surface. Barracuda ATP is also connected to a global threat intelligence network that gathers threat data from diverse sources around the world, providing real-time protection.

Simplifying Procurement and Support

Barracuda offers the industry's largest family of solutions for security, storage, and networking. The broad availability of diverse solutions that can be centrally managed through Barracuda Cloud Control streamlines administering and managing HIT networks. Having Barracuda as a single point for technical support also minimizes the challenges of keeping HIT networks safe and available.

About Barracuda Networks

Barracuda (NYSE: CUDA) simplifies IT with cloud-enabled solutions that empower customers to protect their networks, applications and data regardless of where they reside. These powerful, easy-to-use and affordable solutions are trusted by more than 150,000 organizations worldwide and are delivered in appliance, virtual appliance, cloud and hybrid deployments. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network and data security. For additional information, please visit barracuda.com.

Barracuda®

Barracuda Networks Inc.
3175 S. Winchester Boulevard
Campbell, CA 95008
United States

t: 1-408-342-5400
1-888-268-4772 (US & Canada)
e: info@barracuda.com
w: barracuda.com