Breach Control: Best Practices in Health Care Application Security

Brian Quick

Breach Control: Best Practices in Health Care

Application Security

GIAC (GCIA) Gold Certification

Author: Brian E. Quick, brian@brianequick.com
Advisor: Dr. Kees Leune
Accepted: 15 Feb 2016

Abstract

The risk of protected health information (PHI) being stolen has grown exponentially within the past year. Business associates, covered entities and the health care workforce as a whole must comply with HIPAA and HITECH data protection mandates despite the influx of electronic health records (EHR) from interoperability initiatives. This paper will discuss the threat landscape for patient medical devices and personal mobile devices. This paper will also discuss best practices in application security as part of the Software Development Lifecycle (SDLC).

1. Introduction

Data breaches in the health care industry have surged in the past few years. The health care industry is currently the largest attack surface of the critical infrastructure. Among all of America's critical infrastructures, the health care sector is the most targeted and is plagued by perpetual persistent attacks from numerous unknown malicious hackers, intent on exploiting vulnerabilities in insecure and antiquated networks in order to exfiltrate patient health records (ICIT, 2016).

Medical identity theft continues to rise and is predicted to worsen in 2016. Medical identity theft occurs when personally identifiable information (PII) is used by someone else for health care, health coverage, disability benefits, financial fraud and more. Recently the U.S. Senate Committee on Health, Education, Labor and Pensions (HELP) pressured the Department of Health and Human Services (HHS) in a 10 November 2015 letter to gain information on how the HHS intends to protect the integrity of health care data in spite of the growing alarm that the health care industry is ripe for more data breaches (United States Senate, 2015).

Electronic protected health information (ePHI) is digital information that is recorded in electronic form or medium created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and relates to the past, present, or future physical or mental health condition of any individual (2004, CFR). The health care industry continues to move forward with the widespread use of personal mobile devices utilizing mobile Health (mHealth) applications. Many health settings allow personal devices to connect to the very same WiFi networks that provide connections for critical medical devices leaving the confidentiality and integrity of the ePHI at a high risk of loss.

Application developers are beginning to take greater interest and responsibility in authoring secure code to design safer applications (DZone, 2015). The vast majority of applications are accessible over networks and consequently, more vulnerable to a wide variety of threats. Meticulous security planning and development for new applications

brian@brianequick.com

help minimize the possibility that unauthorized code will be used later against these applications to access, steal, change, or delete protected data.

Organizations that create applications can improve security by simply concentrating on the common flaws that have been well documented for many years but according to the DZone 2015 Application Security Guide, most developers are not familiar with these common flaws (DZone, 2015). In the case of web applications, an excellent source of knowledge for developers is the Open Web Application Security Project (OWASP) Top 10, which was created to increase awareness of critical web application security flaws and how to avoid creating them. The ongoing demand for public facing medical web application portals brings common challenges to the security and privacy of protected health information (Filkins, 2015). Mobile application developers should utilize the OWASP Mobile Apps Checklist, which outlines security checks for mobile applications and requirements to develop a secure design and baseline for all mobile applications (OWASP, 2015).

2. The Health Care Landscape

Every industry has technology, and heath care is no different. Health care has evolved into a critical function for organizations amid the turmoil of industry reform, innovations, and regulatory disorder. Providers and patients can benefit from access to medical data and information technology provides a fast and efficient way to communicate information necessary to diagnose and treat ailments. Critical infrastructure is defined as critical because of the importance it has to society with regards to safety, economies and the livelihood of citizens. Health care information technology impacts the very lives of the people it touches and should receive even more attention to ensure that the patient health information transmitted over it is protected as promised. A new proposed best practice issued by the Food & Drug Administration (FDA) calls for medical device manufacturers to focus more on vulnerability disclosure, remediation programs, cyber threat intelligence sharing and other security best practices critical to patient care and safety (FDA, 2016).

brian@brianequick.com

A medical device is generally any item that is used to diagnose, prevent, monitor, or to treat disease, injury, or physiological activity. Examples are blood pressure monitors, x-ray machines, infusion pumps, and sensors of all types. Medical devices have become increasingly networked and function using similar operating systems that many devices utilize such as desktop computers. There are also many personal devices brought in by visitors and patients such as mobile devices, laptops, and the de facto standard is that all visitors expect an internet connection upon arrival.

Sharing information in health care is an essential part of patient care, but information sharing should never become more important than the safety and security of personal or private data. Health care information is generally more valuable to hackers than even credit card data because financial information is almost always found in the same networks that carry protected health information. Credit cards can be canceled, but the disclosure of personal health information is most often static and will not change. According to a Ponemon Institute 2015 annual study on medical identity theft, 65% of medical identity theft victims had to pay an average of $13,500 to resolve the crime. The study also showed that medical identity theft is a very complicated crime to resolve. Unlike credit card fraud the health care provider or insurer seldom informs the victim of the theft and the victim is often still responsible for covering the cost of the incident (Ponemon, 2015).

2.1 Recent Health Care Breaches and Electronic Protected Health Care Information (ePHI)

Recent survey results from the University of Phoenix reveals that more than 76% of U.S. adults are concerned that their health care records are vulnerable to hackers (2015, Phoenix). A 2015 Protected Health Information Data Breach Report by Verizon stated that people may even be withholding information from their health care providers because they are concerned about the confidentiality of their records. The report also stated that the data gathered between 2004 and 2014 has consistently shown that adversary tactics are

brian@brianequick.com

influenced by the data they are interested in stealing and the assets in which that data is stored, not the country in which the data resides (Verizon, 2015).

In 2015 the health care industry suffered breaches resulting in the loss of millions of health-related records. Anthem Insurance suffered from a breach where hackers managed to break into a database containing personal information in the form of 80 million records. Premera Blue Cross also experienced an intrusion resulting in the loss of an estimated 11 million financial and medical records. Rather than focusing on intrusion headlines, it would be more constructive to concentrate on what the health care industry can do to acquire applications built with security in mind or fix applications already implemented. Figure 1 below highlights additional breach statistics from Bitglass (2016, Bitglass).

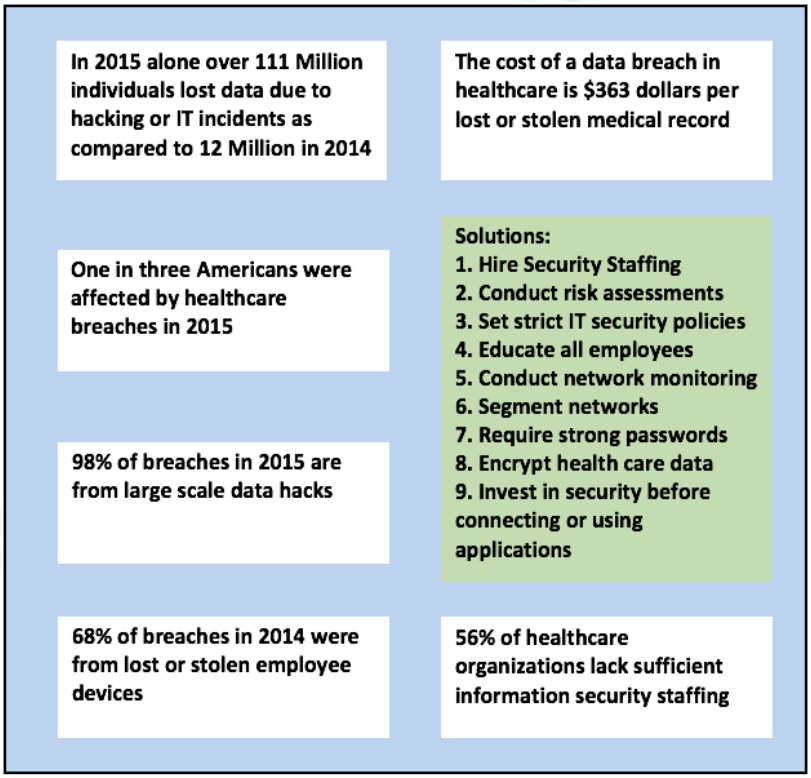

Figure 1 - 2016 Bitglass Health Care Breach Report Sample Results

brian@brianequick.com

2.1.1 HIPAA/HITECH Compliance and Applications

The Health Information Portability and Accountability Act (HIPAA) was first created to help the public with insurance portability, empowering patients to get their medical records from one provider to another. However, along with this portability came privacy and security concerns. HIPAA was amended in 2013 to help clarify the definition of who needed to be compliant, and any entity that will store, manage, record, handle or even pass ePHI is required to be HIPAA compliant. According to the HHS health care providers, health plans, and health care clearinghouses are all considered covered entities. A business associate is a vendor or subcontractor who accesses ePHI or any entity that uses or discloses PHI on behalf of a covered entity. Health care providers are exactly who one might think: hospitals, doctors, clinics, dentists, and pharmacies are considered and need to be HIPAA compliant. The goal of each developer, engineer, architect or information security analyst should be to design and implement the effective administrative, technical and physical safeguards listed in Table 1, which must be validated in order to protect ePHI.

Technical Safeguards	Physical Safeguards	Administrative Safeguards
Access Controls	Facility Access Control	Security Management Processes
Audit Controls	Workstation Use	Security Responsibilities
Integrity	Workstation Security	Workforce Security
Authentication	Device and Media Controls	Information Access Management
Transmission Security		Security Awareness & Training
		Security Incident Procedures
		Contingency Plans
		Evaluation
		Business Associate Agreements

Table 1 - HIPAA Security Rule Requires Safeguards

The Health Information Technology for Economic and Clinical Health (HITECH) Act and HIPAA Omnibus Rule seek to improve health care delivery and patient care by promoting electronic access to personal health information across the health care community,

brian@brianequick.com

including using web-based patient portals. HIPAA violations can be expensive. Penalties for noncompliance are based on the level of negligence and can range from $100 to $50,000 per violation (or record) with a maximum penalty of $1.5 million per year. The security of health care applications and networks that carry ePHI are the focus of this paper.

2.1.2 Information Security Builders and Defenders

Information technology professionals continue to field applications that provide a means of exploitation to attackers because the design or implementation is not done with security in mind. Applications continue to be installed without proper maintenance by providing vulnerability mitigation for already installed applications. The health care industry needs more effective ways to pre-certify and mitigate application vulnerabilities before fielding and then conducting ongoing security assessments for safety and security. A recent SANS 2015 State of Application Security Survey identified gaps in application security and it defined two primary roles in this effort: one role as the builders of applications and defenders of applications that have already been fielded as the other. The builders faced challenges in rapidly delivering features to market, a lack of skills or knowledge to build secure software, and a lack of management support or funding to help developers build better application security during the design and development stages. The defenders faced different challenges such as identifying all the applications in the application portfolio, the inability to modify production code due to fear of breaking functionality and poor communication with developers and the rest of the organization (2015, SANS).

Security is an important concern to most developers, and those responsible for the overall business objectives of the developed software should aid in the effort to embed security into the Software Development Lifecycle (SDLC) as early as possible. Agile software development moves very quickly, but organizations have an obligation to incorporate a security risk management program that is aligned with software development objectives.

brian@brianequick.com

2.1.3 The Software Development Lifecycle (SDLC)

There are various software development approaches or models and each one follows a general lifecycle to help ensure success in the process of development. The most popular development model is the agile model. Software developed in the agile model follows an incremental or rapid cycle. The primary disadvantage of the agile model is the lack of emphasis on design resulting in application security defects. According to a DZone 2015 Application Security Guide, organizations usually introduce security defects because of incomplete requirements and poor coding (2015, DZone).

As seen in figure 2, as much as 80% of application security defects can be reduced during the testing phase; however, after deployment, the security related defects are exponentially more expensive to fix. Using automation to secure development operations may be a potential solution in order to help agile developers who may be pressured to get software out to market quickly.

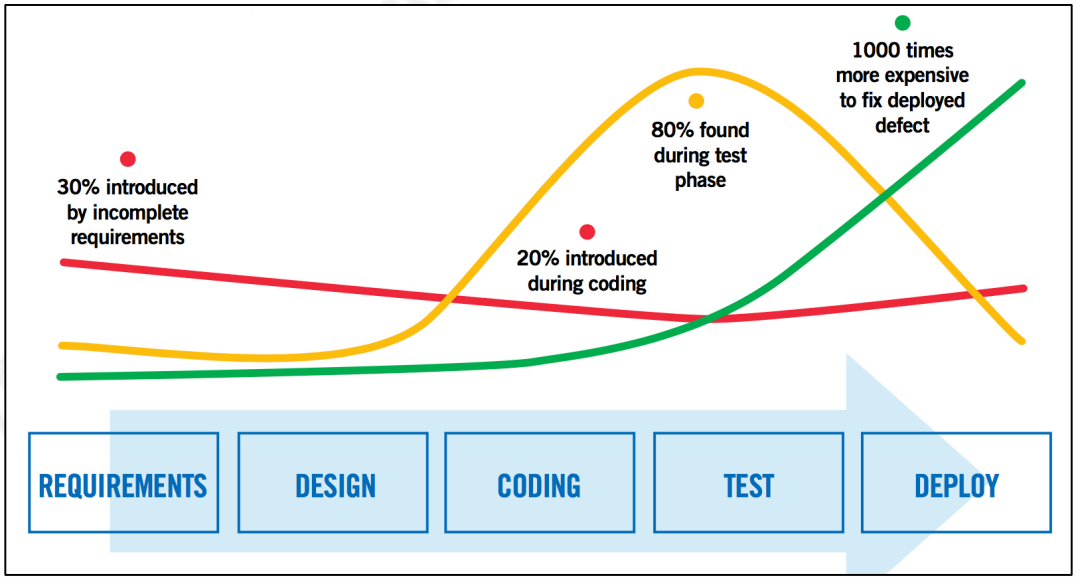

Figure 2 - Developmental security defect statistics

brian@brianequick.com

The DZone guide recommends the use of automation to help find and fix security defects while in the development process. Development organizations should use source code management tools like Git or Subversion, which are both open-source. The next step is to implement a continuous integration tool that supports the source code management system such as open-source options Jenkins, TravisCI or BuildBot. These continuous integration tools are used as best practices to increase productivity while evaluating code on every commit ensuring that defects are fixed as soon as possible rather than being ignored and sent out to market (DZone, 2015). Training developers on how to develop secure code is an effective way to address security in the SDLC. Java and .NET, the most popular development languages are recognized as the highest sources of risk. It is critical that developers use resources on secure coding that are based on the recommendations of the secure coding community. Java and .NET developers can utilize the Source Code Analysis Laboratory (SCALe) conformance process to learn more about how to apply these secure coding principles into the proprietary software or code they manage. The program defines a prospective set of rules and recommendations by which source code can be evaluated for compliance. SCALe points out that coding errors are the primary source of software vulnerabilities. Java developers can utilize and apply the Oracle coding standard for Java and .NET developers should utilize and apply the principles found on the OWASP .NET Project or Microsoft's main site using the Security Development Lifecycle (SDL).

- **Secure Coding** - http://www.cert.org/secure-coding/index.cfm
- **SCALe** - http://www.cert.org/secure-coding/
- **JAVA** - https://www.securecoding.cert.org/confluence/display/java/
- **.NET** - https://www.owasp.org/index.php
- **Microsoft** -https://www.microsoft.com/en-us/sdl/default.aspx

Developers are in the best position to help reduce security defects by authoring secure code in the applications they create whether it be middleware or an application designed

brian@brianequick.com

specifically for a mobile device. Organizations are beginning to realize the importance of security and that application security is not the same as web application security. Another unique challenge facing the health care industry is the development and maintenance of web-based applications used for patient portals. These web portals typically offer messaging, patient educational resources and access to other sensitive ePHI, thereby making them very attractive targets for attacks.

2.1.4 Web Application Portals

Web Application portals are attractive information sharing solutions because the web browser has become so ubiquitous. The public face of a web application portal can be found by sharing a simple domain name, and the customers begin coming in from desktop computers, mobile devices, tablets and even special command-line based utilities that perhaps no one thought about. Security for web application portals can get complicated because it involves an operating system (OS), a web application and a database that is frequently owned and operated by different entities. Securing all these components step-by-step is outside the scope of this paper, but it is critical to practice defense-in-depth to ensure that any vulnerabilities present in the operating system or web server do not adversely affect the web application. The National Institute of Standards and Technology (NIST) has an excellent publication on securing web servers titled SP 800-44 - Guidelines on Securing Public Web Servers (2007, NIST). Since heath care data is extremely valuable to attackers, a focus on the most common areas of web application security that continue to be neglected by developers would be the most constructive.

As mentioned previously in this paper the OWASP Top 10 is an excellent free resource designed to educate developers, engineers, designers, and architects on the consequences of the most common web application weaknesses. Table 2 below provides a list of the most common weaknesses with an explanation on how the web application can be compromised by each weakness. This list also represents the top ten weaknesses that are the easiest to prevent.

brian@brianequick.com

A1 - Injection	Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
A2 - Broken Authentication and Session Management	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.
A3 - Cross-Site Scripting (XSS)	XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A4 - Insecure Direct Object References	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.
A5 - Security Misconfiguration	Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.
A6 - Sensitive Data Exposure	Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

brian@brianequick.com

	Sensitive data deserves extra protection such as encryption at rest or in transit.
A7 - Missing Function Level Access Control	Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.
A8 - Cross-Site Request Forgery	A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. The attacker can then force the victim's browser to generate requests the vulnerable application treats as legitimate requests from the victim.
A9 - Using Components with Known Vulnerabilities	Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.
A10 - Unvalidated Redirects and Forwards	Web applications frequently redirect and forward users to other websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

Table 2 - OWASP Top 10 Web Application Weaknesses

Table 2 simply provides an overview of the most common weaknesses found in web applications, but what can a developer use to verify a design and develop security into

brian@brianequick.com

their applications? The OWASP Application Security Verification Standard (ASVS) is an excellent guide to provide developers ways to validate web application design and prevent security defects. The OWASP Top 10 represents the easiest and most common weaknesses to prevent but ASVS takes prevention a step further by providing a guide for application penetration testers to validate applications already deployed or as a basis of an agile secure development lifecycle (Manico, 2015).

Application Weakness	Verification Solution
A1 - Injection	V5 - Input Handling
A2 - Broken Session and Authentication	V2 - Authentication
A3 - Cross-Site Scripting (XSS)	V5 - Input Handling
A4 - Insecure Direct Object References	V4 - Access Control
A5 - Security Misconfiguration	V19 - Configuration
A6 - Sensitive Data Exposure	V9 - Data Protection
A7 - Missing Function Level Access Control	V4 - Access Control
A8 - Cross-Site Request Forgery	V18 - Web Services
A9 - Known Vulnerabilities in Components	V19 - Configuration
A10 - Unvalidated Redirects and Forwards	V16 - Files and Resources

Table 3 - Verification Solution for Secure Design

Building an application with security in mind during planning and development is still much easier and more cost effective than fixing damages later. Overwhelming evidence from sources like the 2014 SANS Norse Health Care Cyber Report, 2015 Ponemon Fifth Annual Study on Medical Identity Theft and many others conclude that hundreds of vulnerable and misconfigured applications are in critical need of attention by the health care industry. Sometimes, flexibility and adaptation in the IT field breed security vulnerabilities as device operators alter configurations or combine technologies in favor of convenience. A secure-by-design approach should include detective approaches such as automated logging and network monitoring solutions fundamental to analyzing application communications.

brian@brianequick.com

2.2 Devices and Application Connections

2.2.1 Sources of Risk in Patient Medical Devices

Hundreds of thousands of medical devices such as infusion pumps, ventilators, patient monitors, and imaging equipment currently reside on hospital networks across the United States. There is compelling evidence of networked medical device vulnerabilities and the potential for threat agents to exploit them (FDA, 2015). The FDA has released draft guidance proposing that cybersecurity features be integrated into device firmware and software during development. FDA guidance from 2013 described three specific areas: 1. limiting access to trusted users, 2. determining trusted content, and 3. use of fail-safe or recovery features. This guidance recommends that medical device manufacturers and health care providers verify that appropriate safeguards are in place to reduce the risk of device failure due to threats. Manufacturers are expected to help limit unauthorized access to medical devices and review policies and practices regarding appropriate safeguards. Health care facilities should evaluate network security, protect individual network components through routine evaluations and protect the hospital system to restrict unauthorized access to the network and networked medical devices. Health care facilities should verify that appropriate antivirus software is in place, that firewall rules are up-to-date and that network activity is monitored for unauthorized practices that endanger data confidentiality and data integrity. Another area of concern in health care is the growth of personal mobile devices and how network connections of these devices impact the security of ePHI.

2.2.2 Personal Mobile Devices in the Health Care Setting

The use of mobile devices such as iPads, tablets, iPhones, and android phones have transformed many aspects of clinical practices, which has led to the growth of medical software applications designed specifically for mobile devices. Many applications are being developed to help patients and providers connect in areas such as: scheduling; health

brian@brianequick.com

care record maintenance; messaging, and medical education. There are many benefits, that make mobile devices attractive for use in health care. Despite the clinical benefits more effort is required to establish validation standards to ensure the safety of the health care information these mobile applications are designed to store, process and communicate.

BMC Medicine recently conducted a six-month long assessment of 79 accredited applications for mobile applications to characterize personal information collection, local-device storage and information transmission behavior. The study revealed that 89% of the mobile applications transmitted information to online services. 66% of the mobile applications sending personal identifying information over the internet did not use encryption, and none of the 79 applications encrypted personal information stored locally. Only 4 applications sent both personally identifying information and health information without encryption (Huckvale, 2015). All 79 applications were considered accredited.

HIPAA compliance demands that mHealth applications that process ePHI meet all six primary security requirements if transmitted over the Internet. These requirements should, of course seem reasonable and appropriate given the high risk of medical and financial identity theft already discussed in this paper. The biggest obstacles to the success of application security initiatives may remain at the business level. The sooner these security requirements are integrated into the development lifecycle, the less disruptive the remediation process will be.

1. Encryption for data in transit and data integrity protection	45 CFR 164.312(e)
2. Data recovery	45 CFR 164.308(a)(7)
3. Data confidentiality	45 CFR 164.306(a)(1)
4. Data Integrity	45 CFR 164.312(c)(1)(2)
5. Encryption for data at rest	45 CFR 164.312(a)(1)

brian@brianequick.com

6. Permanent disposal of data when no longer needed	45 CFR 164.502(a)

Table 4 - Six requirements of HIPAA

As stated previously health care facilities should monitor network activity for unauthorized practices and application misconfiguration which may endanger the confidentiality and integrity of ePHI.

2.2.3 Common Health Care Application Misconfigurations

The 2014 SANS Norse Health Care Cyber Report disclosed the most common ports of compromise based upon 50,000 events captured between September 2012 and October 2013 within the health care industry (2014, Filkins). These ports reveal risk based on the related protocols involved. The number one protocol was the Hypertext Transport Protocol (HTTP) at 28%. HTTP communicates everything in plaintext, is vulnerable to (DDOS attacks and typically results in the loss of sensitive data. Another notable protocol, Remote Desktop Protocol (RDP) services are commonly used for remote, after-hours access. The default configuration is vulnerable to man-in-the-middle attacks, brute-force attacks, and in-memory credential harvesting. (2014, Filkins). The average breach in any industry goes undetected for 256 days according to Ponemon (2015, Ponemon). Information defenders must lobby business leaders to invest in detection capabilities that can enable rapid response to suspicious events and help prevent incidents from worsening over time.

2.2.4 Network Security Monitoring

Network security monitoring should be conducted so information technology stakeholders can gain visibility into current data flows and routinely inspect how applications and devices are communicating. Accurate documentation on the current network architecture is commonly hard to obtain while keeping it current can be even more challenging. Routine monitoring helps accomplish this task while also allowing network security professionals the opportunity to validate that security devices are

brian@brianequick.com

operating as intended or in need of important changes. It is recommended that the network is logically segmented based on the sensitivity of information and the criticality of medical devices. Intrusion Detection Systems (IDS) are just the beginning. The first signs of malicious traffic can prompt a cyber hunt team to go deeper into the source of the anomalies discovered allowing professionals to achieve identification and containment.

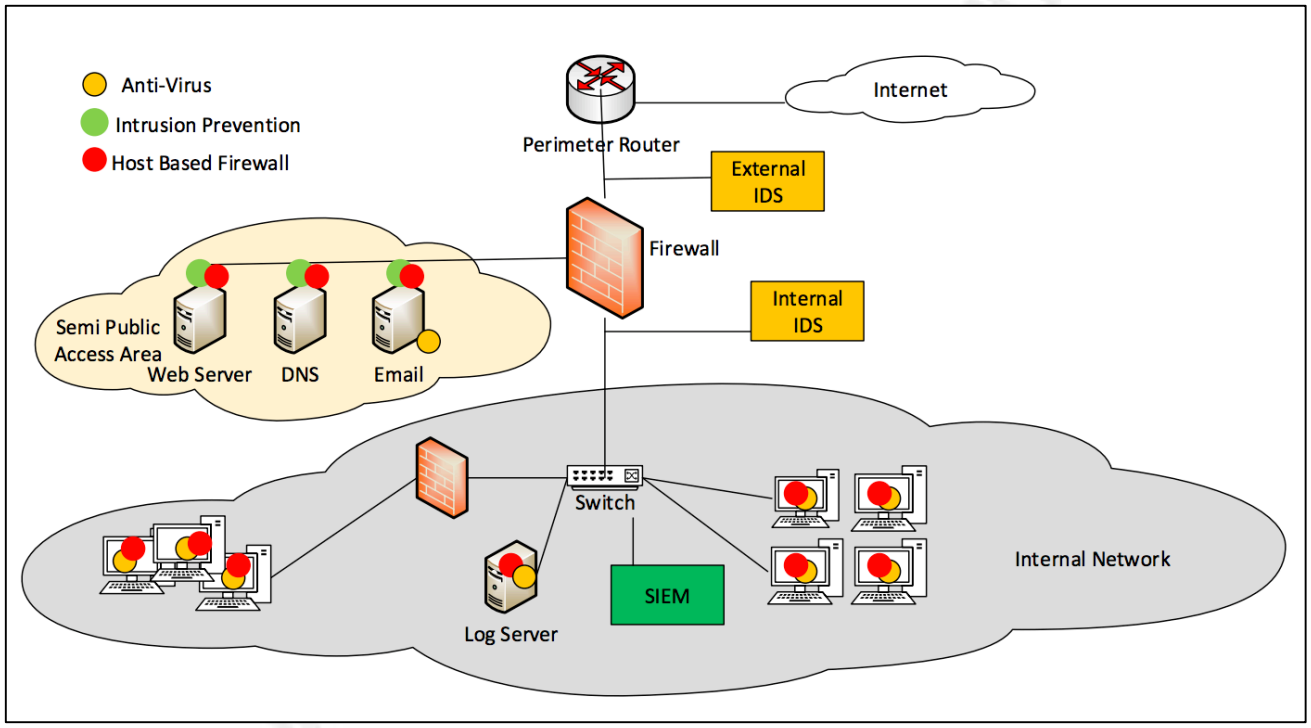

Figure 3 - A typical architecture with network monitoring

Open source solutions like security onion can offer economical solutions for an initial or even long term network security monitoring capability. Security Incident and Event Management (SIEM) solutions can be deployed to build security analytics allowing an incident response team to track and record response measures. Organizations should also consider keeping personal mobile devices logically separated or segmented from other networks with more critical patient medical devices or equipment.

brian@brianequick.com

3. Conclusion

Improperly configured and poorly developed applications are targets for attackers. Application security issues are definitely preventable and many health care applications are openly exploitable, as in the case of applications with default admin passwords. Designing secure software applications has always been an important part of the security lifecycle. Building an application with security in mind is still much easier and more cost effective when done early in development rather than trying to fix flaws or other damages later. Security training for developers should also be an important part of each organizations strategy to develop secure applications providing the core foundation of information security: confidentiality, integrity, and availability.

brian@brianequick.com

References

Bitglass. (2016). Bitglass Healthcare Breach Report 2016. Retrieved February 11, 2016, from http://pages.bitglass.com/Healthcare-Breach-Report-2016.html

Code of Federal Regulations (CFR). (2004). 45 CFR 160.103. Retrieved December 31, 2015, from https://www.gpo.gov/fdsys/pkg/CFR-2004-title45-vol1/pdf/CFR-2004-title45-vol1-sec160-103.pdf

Dzone. (2015). Retrieved December 30, 2015, from https://dzone.com/storage/assets/799727-dzone-guidetoapplicationsecurity-2015.pdf

Federal Bureau of Investigation (FBI). (2014, April 8). Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain. Retrieved January 1, 2016, from http://www.aha.org/content/14/140408--fbipin-healthsyscyberintrud.pdf

Filkins, B. (2014, December). New Threats Drive Improved Practices: State of Cybersecurity in Health Care Organizations. Retrieved December 31, 2015, from https://www.sans.org/reading-room/whitepapers/analyst/threats-drive-improved-practices-state-cybersecurity-health-care-organizations-35652

Food and Drug Administration (FDA). (2016, January 15). FDA outlines cybersecurity recommendations for medical device manufacturers. Retrieved January 31, 2016, http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm481968.htm

Food and Drug Administration (FDA). (2015, May). Vulnerabilities of Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems: FDA Safety Communication. Retrieved February 6, 2016, from http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm446809.htm

Hall, S. (2014, April). FBI warns healthcare of vulnerability to cyberattacks - FierceHealthIT. Retrieved December 31, 2015, from

brian@

http://www.fiercehealthit.com/story/fbi-warns-healthcare-vulnerability-cyberattacks/2014-04-24

Health and Human Services (HHS). (2015, August 31). Health app developers: Questions about HIPAA? - by IdeaScale | Popular. Retrieved December 31, 2015, from http://hipaaqsportal.hhs.gov/a/ideas/top/campaign-filter/active#

Health and Human Services (HSS). (2013, January). HIPAA for Professionals | HHS.gov. Retrieved December 2015, from http://www.hhs.gov/hipaa/for-professionals/index.html

Health and Human Services (HSS). (2015, October). Numbers at a Glance - Current | HHS.gov. Retrieved December 30, 2015, from http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/numbers-glance/index.html

Heath, S. (2015, December 17). 87% of PHI Data Breaches Occur in the US, Verizon Reports. Retrieved December 30, 2015, from http://healthitsecurity.com/news/87-of-phi-data-breaches-occur-in-the-us-verizon-reports

Huckvale, K., Prieto, J., Tilney, M., Benghozi, P., & Car, J. (2015). Unaddressed privacy risks in accredited health and wellness apps: a cross-sectional systematic assessment | BMC Medicine | Full Text. Retrieved February 7, 2016, from http://bmcmedicine.biomedcentral.com/articles/10.1186/s12916-015-0444-y

Imperva. (2015). 2015 Web Application Attack Report (WAAR). Retrieved December 30, 2015, from http://www.imperva.com/docs/HII_Web_Application_Attack_Report_Ed6.pdf

Institute of Critical Infrastructure Technology (ICIT). (2016, January). Hacking Healthcare IT in 2016 - Lessons the Healthcare Industry can learn from the OPM Breach. Retrieved from http://icitech.org/wp-content/uploads/2016/01/ICIT-Brief-Hacking-Healthcare-IT-in-20161.pdf

Manico, J. (2015). Category:OWASP Application Security Verification Standard Project - OWASP. Retrieved February 6, 2016, from https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

brian@

McGrath, M., & Scanaill, C. N. (2014). *Sensor technologies: Healthcare, wellness, and environmental applications*. New York, NY: ApressOpen.

Medical Identity Fraud Alliance (MIFA). (n.d.). 2014 Fifth Annual Study on Medical Identity Theft. Retrieved January 1, 2016, from http://medidfraud.org/2014-fifth-annual-study-on-medical-identity-theft/

Murphy, S. P. (2015). *Healthcare information security and privacy*. New York, NY: McGraw-Hill Osborne Media.

OWASP. (2015, September 4). Category:OWASP Top Ten Project - OWASP. Retrieved December 30, 2015, from https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Ponemon Institute LLC. (2015, February). Fifth Annual Study on Medical Identity Theft. Retrieved February 2, 2016, from http://medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf

Privacy Rights Clearinghouse. (2015, February). Health Privacy: HIPAA Basics | Privacy Rights Clearinghouse. Retrieved December 31, 2015, from https://www.privacyrights.org/content/health-privacy-hipaa-basics

Ransome, J. F., Misra, A., Schoenfield, B., & Schmidt, H. A. (2014). *Core software security: Security at the source*.

SANS Institute. (2015, May). 2015 State of Application Security: Closing the Gap. Retrieved February 3, 2016, from https://www.sans.org/reading-room/whitepapers/analyst/2015-state-application-security-closing-gap-35942

Snell, E. (2015, February 6). Lessons Learned from the Anthem Data Breach. Retrieved December 30, 2015, from http://healthitsecurity.com/news/lessons-learned-from-the-anthem-data-breach

Snell, E. (2015, December 9). Top 10 Healthcare Data Breaches of 2015. Retrieved December 31, 2015, from http://healthitsecurity.com/news/top-10-healthcare-data-breaches-of-2015

Strohm, C. (2015, February 24). FBI Is Close to Finding Hackers in Anthem Health-Care Data Theft - Bloomberg Business. Retrieved December 30, 2015, from

brian@

http://www.bloomberg.com/news/articles/2015-02-24/fbi-is-close-to-finding-hackers-in-anthem-health-care-data-theft

Trotter, F., & Uhlman, D. (2013). *Hacking healthcare*.

United States Senate. (2015, November 10). Medical Identity Theft Letter. Retrieved from http://www.help.senate.gov/imo/media/doc/Medical%20Identity%20Theft%20Letter--final.pdf

University of Phoenix. (2015, October 6). More than 75 Percent of U.S. Adults Express Concern About Security of Health Care Data, Reveals University of Phoenix Survey - University of Phoenix. Retrieved February 4, 2016, from http://www.phoenix.edu/news/releases/2015/10/us-adults-concerned-about-security-of-health-care-data.html

Verizon. (2015, January). 2015 Protected Health Information Data Breach Report. Retrieved February 2, 2016, from http://www.verizonenterprise.com/resources/reports/rp_2015-protected-health-information-data-breach-report_en_xg.pdf

brian@brianequick.com

Last Updated: October 25th, 2020

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Sydney 2020	**Sydney, AU**	**Nov 02, 2020 - Nov 14, 2020**	**Live Event**
SANS Secure Thailand	**Bangkok, TH**	**Nov 09, 2020 - Nov 14, 2020**	**Live Event**
APAC ICS Summit & Training 2020	**Singapore, SG**	**Nov 13, 2020 - Nov 28, 2020**	**Live Event**
SANS Community CTF	**,**	**Nov 19, 2020 - Nov 20, 2020**	**Self Paced**
SANS Local: Oslo November 2020	**Oslo, NO**	**Nov 23, 2020 - Nov 28, 2020**	**Live Event**
SANS OnDemand	**OnlineUS**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**