SECUREKLOUD

Top 9 Security Threats in Healthcare Industry

Major concerns focusing around the healthcare industry are access to care, quality of care, frequency of incorrect medical diagnoses and increasing costs. In order to provide patient-centric services and cut down costs, the healthcare industry started embracing digital technologies, including Cloud, Big Data, IoT and containers. These technologies allow them to create and manage data better, as well as store critical health data more efficiently. Consequently, these organizations have emerged as a prime target for hackers, putting valuable medical data at risk.

2017 was the year when persistent cyber-attacks happened in the healthcare industry. Who will ever forget the WannaCry malware that caused problems to different hospitals all over the United Kingdom? The thing is that this incident is not isolated and that the healthcare industry is known to have the worst cybercrime incidence of all sectors. In fact, the cost of a breach in the healthcare security is $380 per capita. In this article, let's see the top security threats that the healthcare industry should watch.

Ransomware and Other Malware

Malware is a serious threat in the healthcare sector. As we know, healthcare industry works in a complex and interrelated network of information where malware and ransomware can result in inaccessibility to information within the industry. For example, the WannaCry attack enforced hospitals to blackout because they could not access the critical data of their patients.

Phishing

Like any other industry, healthcare is also at risk from Phishing. They are initiated with an email attachment that are embedded with malware. Once it's opened, it releases the malware that can phish for data such as login credentials to access vital patient information. The National Health Information Sharing and Analysis Center have recently stated that the healthcare industry is at the most risk of fraudulent emails. However, little is being done to combat this, with 98% of healthcare organizations not taking the first steps in helping to prevent phishing by setting in place Domain-based Message Authentication, Reporting & Conformance (DMARC).

Insider Threats

Insider threats are the ones carried out by patients or staff that are either accidental or intended. According to the recent survey by HIMSS survey, insider threats pose as much as 75% of the cyber threats in the healthcare industry.

Increased Use of Cloud Computing and Online Security

Online security in cloud computing is often taken for granted. While the use of cloud computing in the healthcare industry is projected to rise to 20.5% by 2020, little is done when it comes to online security. Protecting the data during transit across different web services require not only robust encryption methods but also efficient authentication.

Internet of Things Attacks

The healthcare industry has embraced the IoT to improve the patient experience. While it is done to improve the patient outcomes, IoT poses threats as the data stored can be stolen by hackers. Hackers can either make the data inaccessible or skewed, thus disrupting the treatment of patients.

Authentication Issues

Many massive breaches within the healthcare industry are caused by authentication issues. Using weak passwords can be dangerous and for this reason two-factor, as well as risk-based authentication, are popular as they offer more mitigation against phishing and security attacks.

Legacy Apps are vulnerable

Many hospitals are still using legacy applications to store and manage their patien records. However, using such legacy applications give cybercriminals a significant opening to take advantage of the vulnerability of legacy OS and architectures.

Poor Funding Affecting Security

Many hospitals are still up against the funding for cybersecurity. The robust security programs need huge investments for both training and implementation. Unfortunately, not too many healthcare organizations are interested in spending money on high-end security infrastructure. But the continuous cyber-attacks within the industry should change their minds.

Poor Security Awareness Program

Security is a problem for everyone within the organization. While most hospitals are using technology to integrate information, employees are not fostering a culture of security. They still use weak passwords and tend to be least careful in opening emails. This is a big and a habitual problem which is often hard to correct. Hospitals and medical practices must find ways to build more awareness about security and its importance in the workplace.

Reference:

Infosec Institute, WannaCry, The Aftermath: How WannaCry Could Have Been WannaSmile:
http://resources.infosecinstitute.com/wannacry-aftermath-wannacry-wannasmile/

http://resources.infosecinstitute.com/top-10-threats-healthcare-security/

https://www.arrowsolutionsgroup.com/

www.med-technews.com

http://www.csoonline.in

About SecureKloud

300+ Solutions Architects /DevOps Engineers with deep expertise on multiple stacks

Specializing in Cloud DevOps, Security, Automation, Big Data and Anayltics

Born on the Cloud. Early partners of AWS & leading Microsoft Azure Partner

Expertise in development & operations of Secure & Compliant cloud utilizing agile practices and IP tools

Leader in Cloud Compliance. Support HIPAA, PCI, GxP, SOX systems transition to Cloud

SecureKloud Technologies: 12647 Alcosta Boulevard, Suite 450, San Ramon,
CA 94583 San Ramon, CA | East Brunswick, NJ | Chicago, IL | Dallas, TX | Chennai, India | Sharjah, UAE
mail to: info@securekloud.com website: www.securekloud.com