RANSOMWARE DEFENSE PRESCRIPTION

FOR HEALTHCARE 2021

Airgap delivers industry's first Ransomware Kill Switch built on Zero Trust Isolation platform to help improve your enterprise security posture and stop any malware propagation in seconds.

AIRGAP

Table of Contents

1 Part 1:
THE REASONS FOR VULNERABILITIES

2 | Ransomware and Healthcare

4 Part 2:
RANSOMWARE AND HIPAA COMPLIANCE

6 Part 3:
SAFEGUARDING CARE GIVERS

6 | Single Sign-On (SSO) or Multi-Factor Authentication (MFA) in Place

7 | Telehealth growth and mHealth

8 | Zero-Trust Network Access and Ransomware Protection

Part 1

THE REASONS FOR VULNERABILITIES

Before 2016, healthcare institutes were not considered to be a primary target for ransomware.

However, 14 hospitals had become the victim of ransomware, and a total of 173 hacking/information technology (IT) event data breaches had been officially reported[1]. Hospitals have become an obvious target for hackers for two reasons: (1) the requirement of computer storage of information associated with patient care and (2) the security loopholes in IT systems. When hit with ransomware, some hospitals have been despairing to pay the ransom because of their requirement for the most up-to-date information, such as drug communications, care directives, and medical history, to provide critical care to patients. Accordingly, the healthcare industry is presently considered at substantial risk of a ransomware attack, mainly due to trails of other leading industries in securing important data.

Recently, Universal Health Services, one of the largest healthcare providers in the U.S., had been hit by a ransomware attack[2]. The attack hit UHS systems to lock computers and phone systems at several UHS facilities across the country, including California and Florida. The Ryuk Ransomware, which is anticipated to be associated with the UHS attack, is commonly distributed via email from phishing links or attachments.

In this multi-part series we will discuss why hospitals are one of the most vulnerable victims for ransomware, how healthcare arena has to maintain critical compliance, why their data is vulnerable. We will also discuss the pitfalls of Multi-Factor Authentication and Single Sign-On which are presently being utilized by the sector. We will also understand how with the rise of telehealth owing to the pandemic the arena maybe getting subjected to further attacks and whether the implementation of PCoIP zero clients eliminates the risk of data theft through USB devices, or damage to data from viruses or malware, as well as data loss from hardware failure.

[1] *https://digitalcommons.law.seattleu.edu/cgi/viewcontent.cgi?article=2416&context=sulr*

[2] *https://healthitsecurity.com/news/uhs-health-system-confirms-all-us-sites-affected-by-ransomware-attack#:~:text=October%2005%2C%202020%20%2D%20Universal%20Health,clinicians%20into%20EHR%20downtime%20procedures.*

Ransomware and Healthcare

Hackers have found it simple to attack hospitals with ransomware because of hospitals' speedy IT adoption without a concomitant increase in IT support staff's number and refinement. After the government allocated reserves for the Meaningful Use program, this IT adoption occurred, which encouraged electronic health records (EHRs). With the Meaningful Use incentives, EHR utilization progressed from 9.4 percent in 2008 to 96.9 percent in 2014[3].

With such a large increase in IT utilization in a short time frame, many healthcare facilities have been incapable of adopting adequate network security and other information technology support to combat potential attacks. Without enough funds, many hospitals do not have the workers to employ simple barriers to hackers, such as the quick installation of electronic patches.

Cybercriminals are becoming clever by the day as they move towards creating ransomware that attacks essential systems, thereby enhancing the scope for demanding more ransom.

Some of the significant examples of ransomware hitting the healthcare industry are:

- Sonoma Valley Hospital suffered a ransomware attack that impacted all of the hospital's computer systems[4]. In response to the attack, the hospital quickly stopped the incident by taking its electronic systems offline and didn't pay any ransom;
- Ascend Clinical was breached after an attacker deployed a successful phishing scheme that led to a ransomware attack[5]. As a result, the data of over 77,000 individuals was compromised. It was unclear whether the ransom was paid or not;
- Hackers breached the Singapore government's health database and successfully accessed about 1.5 million patients[6], including demographic information and patient identification numbers;

[3] *https://www.cms.gov/newsroom/fact-sheets/record-progress-health-information-technology*

[4] *https://healthitsecurity.com/news/mount-locker-ransomware-actors-claim-sonoma-valley-hospital-attack#:~:text=Initially%2C%20the%20attack%20was%20reported,it%20was%20a%20ransomware%20attack.&text=But%20before%20system%20access%20was,of%20data%20from%20the%20network.*

[5] *https://www.infosecurity-magazine.com/blogs/healthcare-ransomware-attacks/#:~:text=Sonoma%20Valley%20Hospital%20suffered%20a,of%20the%20hospital's%20computer%20systems.&text=Ascend%20Clinical%20was%20breached%20after,over%2077%2C000%20individuals%20was%20compromised.*

[6] *https://www.healthcareitnews.com/news/hackers-breach-15-million-singapore-patient-records-including-prime-ministers#:~:text=Hackers%20breach%201.5%20million%20Singapore%20patient%20records%2C%20including%20the%20prime%20minister's,-In%20what%20officials&text=Hackers%20breached%20the%20Singapore%20government's,for%20almost%20a%20full%20week*

- One of the largest health insurers, Anthem of the United States, was hit by a massive breach of this century, which compromised PHI & PII of around a million patient records[7].

More than 80 publicly promulgated ransomware attacks on health care providers in 2020 are more than in all of 2019[8]. Health facilities large and small have been influenced by the ransomware scourge as the sector's longstanding cybersecurity difficulties, including resource constraints and managing software updates, have come to a peak during the pandemic.

It's also become prominent as we head into 2021 that the bad guys aren't giving the healthcare arena a pass just because of the potential risks to patient care. The extent of the COVID-19 pandemic on the healthcare sector, combining the influence of increasing medical demands with revenue pressure from decreased elective procedures, make it especially challenging for those healthcare chief information security officers to reinforce their defenses.

It's an invaluable battle to fight, acquiring the necessary technology and finding the right expertise to utilize it. That makes it vitally important in 2021 and beyond to take a smart, focused strategy to build defenses to mitigate against ransomware, rather than launching the kitchen sink at the threat.

[7] *https://digitalguardian.com/blog/history-data-breaches*
[8] *https://www.securitymagazine.com/articles/92575-increase-in-reports-of-ransomware-attacks-on-health-*care-entities

Part 2

RANSOMWARE AND HIPAA COMPLIANCE

In this multi-part series we will discuss why hospitals are one of the most vulnerable victims for ransomware, how healthcare arena has to maintain critical compliance, why their data is vulnerable.

In this context, adhering to HIPAA Security Rule is absolutely relevant. In this case, the healthcare area will be able to curb a portion of ransomware attacks, where hospitals are required to implement security divisions that can help prevent the introduction of malware, inclusive of ransomware. Some of these required security measures include:

- executing a security management process, which includes conducting a risk analysis to recognize threats and vulnerabilities to electronically protected health information (ePHI) and implementing security measures to alleviate or remediate those identified risks;
- implementing methods to guard against and detect malicious software;
- educating users on malicious software protection so they can assist in identifying malicious software and know-how to report such detections;
- realizing access controls to limit access to ePHI to only those persons or software programs needing access.

The Security Management Process norm of the Security Rule includes requirements for all observed entities and business associates to conduct an accurate and out-and-out risk analysis of the potential risks and vulnerabilities to the confidentiality, sincerity, and availability of all of the ePHI the entities create, secure, maintain, or transmit and to implement security measures adequate to reduce those identified risks and vulnerabilities to a consistent and appropriate level.

The HIPAA Security Rule expects covered entities and business associates to implement strategies and procedures to assist an entity in responding to and healing from a ransomware attack. Because ransomware denies entry to data, maintaining frequent backups, and ensuring the capability to recover data from backups is important to recovering from a ransomware attack. Test rehabilitation should be periodically conducted to confirm the integrity of backed up data and provide assurance in an organization's data restoration capabilities. Because some ransomware modifications have been known to remove or otherwise disrupt online backups, entities should reflect maintaining backups offline and unavailable from their networks.

Executing a data backup plan is a Security Rule requirement for HIPAA covered entities and business partners as part of maintaining an overall contingency plan. Extra activities that must be included as part of an entity's contingency policy include disaster recovery planning, emergency operations planning, interpreting the criticality of applications and data to ensure all required applications and data are accounted for, and periodic testing of contingency arrangements to ensure organizational readiness to execute such plans and present the confidence they will be effective.

During replying to a ransomware attack, an entity may find it necessary to activate contingency or business continuity plans. Once initiated, an entity will continue its company operations while continuing to respond to and recover from a ransomware attack. Managing confidence in contingency plans and data recovery is decisive for effective incident response, whether the event is a ransomware attack or fire, or natural catastrophe.

The increase in ransomware attacks on hospitals underlines that smart investment in security defense approach is well worth the cost. Even if the ransom isn't paid, a successful attack can exact a very high cost in disrupted operations and reputational impact.

Part 3

SAFEGUARDING CARE GIVERS

Healthcare is leaving out the proverbial welcome mat for hackers, failing to address key vulnerable endpoints, which later become top access points and exploits for ransomware attacks. In this final part of our multi-part series, we look at how the care provides can safeguard themselves and keep the loopholes in check.

Single Sign-On (SSO) or Multi-Factor Authentication (MFA) in Place

As per the 2020 Breach Barometer published by Protenus, more than 41 million patient records were breached in 2019[1]. Fifty-nine percent of the respondents surveyed in Europe and the U.S. were bothered about their medical data security, while 39% were troubled that hackers would play foul with their digital data[2]. A complete device can be infiltrated by advanced ransomware and phishing programs. Hackers can efficiently plant malicious scripts on a computer or steal login credentials. Likewise, IoT devices like insulin pumps, ventilators, and other medical instruments are vulnerable network access points, and they should be reviewed for software updates, patches, and other updates.

The simplistic combination of a user ID and password is no longer good enough to protect exposed information. Identity theft, data breaches, malware, and malicious person suggest that digital security must evolve to stay one step ahead of security perils. The concept behind single sign-on is candid—users carry out a master sign-on to authenticate themselves at the start of their work period. Then, whenever they require to log into another part of software, the SSO solution logs in on their account. The SSO solution internally collects the various credentials for every piece of software users need to reach and then validates them with those systems when they need to be obtained. If a hacker, malicious character, or malware gets

[1] *https://blog.protenus.com/2020-breach-barometer-41m-patient-records-breached-as-hacking-incidents-escalate*
[2] *https://www.rsa.com/content/dam/en/e-book/rsa-data-privacy-report.pdf*

SSO access, it intervenes in any SSO systems. Relying on a single authentication factor to guard sensitive information puts your company a single mistake on the part of an accidental end-user away from a breach.

This is where multiple authentication factors can make all an exception. Incorporating a multi-factor authentication (MFA) solution puts additional security zones in place that prevent cybercriminals from accessing a hospital's network, even if an end-user yields victim to a social attack. Without the second authentication factor, the attempt would be unsuccessful, even if the attacker obtains the user's username and password.

While MFA offers effective protection against social attacks, it's also critical that this added security doesn't negatively impact hospital productivity, especially for busy clinicians who need prompt, efficient access to electronic medical records (EMRs) and other clinical apps. Therefore, it's important to find a flexible solution that only needs additional authentication when the circumstance warrants it—keeping friction and user trouble to a minimum.

Telehealth growth and mHealth

Recently SecurityScorecard and DarkOwl LLC released a report that found that the rapid development in telehealth use during the COVID-19 pandemic[3] has led to an enhanced data footprint, leaving both provider and patient data risk. The ongoing emergency has also regrettably, but quite incontrovertibly displayed one of the key challenges of mobile health apps: security. In recent months there has been a wave in the deployment of apps that deliver several COVID-19 related assistances critical to managing the pandemic.

In this situation, the potential of widespread adoption of mobile healthcare apps is a great occasion as it is a significant risk. Most mHealth apps have entrance to extremely sensitive information, including personal identifiers, medical reports, and financial details, making them prime targets for hackers. Without negotiating app functionality, usability, and utility in enhancing healthcare issues, securing access to this data has to be the overarching design policy for every medical app development program. Nevertheless, that does not seem to be the case, according to Verizon's 2020 Mobile Security Index study 's conclusions.

[3] *https://www.prnewswire.com/news-releases/securityscorecard-names-telehealth-biggest-healthcare-threat-in-new-report-301127130.html*

[4] *https://enterprise.verizon.com/resources/reports/mobile-security-index/*

The fact is that there are mobile security solutions that can prevent almost every prevalent mobile attack vector. Simultaneously, healthcare organizations also need to institute robust security policies and educate users on mobile security hygiene to neutralize the risks and maximize the security of mHealth apps. It is positively impossible to ignore the transformative potential that mHealth signifies for both patients and healthcare professionals. It allows an extensive range of benefits that includes enhanced healthcare efficiency and productivity, lower healthcare costs, and enhanced decision-making, to name a few. However, accessing these advantages comes with a quantum of risk that has to be addressed upfront. The healthcare sector covers the same risks almost every other industry faces as it comprises the transitions towards a mobile-first norm. In healthcare, the outcomes of these risks happen to be more catastrophic and costly. Advanced security technologies can help simplify and accelerate healthcare's inexorable evolution toward telemedicine. However, there also has to be a harmonious and coordinated effort to educate the industry about the long-term repercussions of just concentrating on doing the job.

Zero-Trust Network Access and Ransomware Protection

By moving toward a Zero-Trust paradigm incorporating micro-segmentation, cities and hospitals can create a much more challenging environment for cyber attackers to gain success. A Zero-Trust architecture needs authorization for any person or device attempting to connect to a network or access network resources, even for users now within the network perimeter[5]. Any entity that strives for a network connection must have its identity authenticated before the connection is finished — and, once access is authorized, this identity must be utilized to further control access to critical servers and data.

Executing micro-segmentation with assured identity to achieve a zero-trust network environment will support cities and hospitals defeat these attacks[6] — and significantly decrease the risk of having to make a costly ransom payment or start on massive data restoration and system rebuild and applying Zero-Trust as leading principles puts a specific focus on an anticipated outcome during the design phase. It is by no means a way to define the relevance of security controls from controls structures. Applying Zero-Trust

[5] https://www.google.com/aclk?sa=l&ai=DChcSEwjl07e8qp3uAhU3nUsFHXQyBBMYABAAGgJzZg&ae=2&sig=AOD64_1Dxc8DEJojL4upiEaqKCSdZffhMg&q&adurl&ved=2ahUKEwjpkZO8qp3uAhXUlOYKHcvZDyEQ0Qx6BAgSEAEaclk?sa=l&ai=DChcSEwjl07e8qp3uAhU3nUsFHXQyBBMYABAAGgJzZg&ae=2&sig=AOD64_1Dxc8DEJojL4upiEaqKCSdZffhMg&q&adurl&ved=2ahUKEwjpkZO8qp3uAhXUlOYKHcvZDyEQ0Qx6BAgSEAE

[6] https://iiot-world.com/ics-security/cybersecurity/using-a-zero-trust-approach-to-defeat-ransomware-attacks/

principles permits focusing on a specific subset of controls during design, such as controls and abilities needed for dynamic authentication and authorization applying all possible contextual information.

A Zero-Trust-based solution could inscribe some of these attack techniques, such as lateral movement technique. A Zero-Trust strategy requires significant investments of time and money and the possibility of disruptions as users adjust to hardened access controls.

In healthcare, it's not going to occur overnight, Touhill stressed. The process needs to start as soon as practicable, given the spate of targeted cyberattacks on healthcare and COVID-19 data. Some tools can assist the process, including a software-defined outline and single packet authorization, which complements a software-defined perimeter.