SONICWALL

EXECUTIVE BRIEF

Healthcare Cybersecurity in the Pandemic

Identifying and Preventing Increased Risks

Abstract

Keeping healthcare systems operational is a matter of life and death. During the current COVID-19 pandemic, this fact is only magnified – and taken advantage of by cybercriminals. This brief[1] considers the unique vulnerabilities of healthcare cybersecurity, examines how the pandemic has exacerbated risk, and presents recommendations for protecting your organization.

Introduction

In the months that have passed since shelter-in-place orders came into place across Europe and North America, we have witnessed a major shift in the way enterprises, educational institutes and even government agencies work. Almost everyone has shifted to working from home.

Hospitals, care and research facilities, however, are one of the key exceptions to the trend towards remote work, and by necessity have maintained "business as usual."

The spread of the pandemic meant that these institutes were (and still are) at the forefront of the global human effort to fight the virus. As such, some of us might have imagined that this critical sector would be spared by cybercriminals, but that's not what has happened. The COVID-19 era is characterized by a steep rise in cyber-attacks, from different perpetrators and for different motivations, and the healthcare sector hasn't been spared.

By August, the situation had become so severe that the president of the International Committee of the Red Cross warned the U.N. Security Council about the increase in cyberattacks targeting hospitals: "If hospitals cannot provide life-saving treatment in the middle of a health crisis or an armed conflict, whole communities will suffer."

Inherent vulnerabilities in healthcare cybersecurity

To formulate an effective response, we must first review the factors that contribute to the healthcare sector being at high risk from cyber threat actors.

Weak infrastructure, under extreme stress

Hospitals' IT infrastructure is big, complex and oftentimes dated. Hospitals and healthcare facilities have not been required in the past to adhere to stringent cyber regulation in the same way that banks, insurance companies and critical facilities have. Many of them rely on old, legacy systems and lack the qualified people power to maintain these and face novel security threats. The entire IT infrastructure of hospitals is under extreme stress nowadays, due to remote work and under constraints related to the pandemic, as well as growing demand for their services.

Rogue devices

In addition, hospitals and care facilities were forced to implement remote monitoring technologies overnight to accommodate COVID patients. This meant that they purchased off the shelf IT, communication equipment (such as home routers), IP cameras and other sensors, all connected to the local networks. This means that alien devices were introduced to sensitive environments without proper due diligence. Many of these devices have default credentials and could serve as an entry point to the network from afar.

[1] Adapted from SentinelOne

Telehealth

Shelter-in-place orders also sped the adoption of Telehealth (aka Remote health), health apps and remote monitoring equipment. If we were to speculate, the speed of which these technologies were adopted did not allow for proper penetration testing and verification- meaning that the attack surface has been increased multiple times.

Third-party risks

Healthcare institutes work with a multitude of 3rd party vendors- suppliers, service providers, state and federal agencies, universities and NGOs. This supply chain embodies a significant risk, since it is extremely difficult to ensure that all these providers are up to the same cybersecurity standard, a weakness that attackers often exploit.

Children's Minnesota, one of the largest children's healthcare organizations in the US, recently announced that the personal data of more than 160,000 patients may have been compromised due to a previous hack of Blackbaud, a cloud software company.

Even vendors that are specifically hired to assist with security operations can sometimes make mistakes with serious consequences. Elite Emergency Physicians, for example, hired a 3rd party vendor to securely dispose of two decades' worth of medical records. However, the records were instead found discarded in a local dump site, which resulted in a massive data breach of some 550,000 patient details and was the third largest healthcare breach of the year.

Tired staff, weak security culture

It's no secret that tired, overworked professionals make more errors. One study found that physicians rarely locked their workstations when walking away to treat a patient, even though they were supposed to. Add in the fact that they have been working extra hard for many months, it's unsurprising that there will be more IT-related mistakes, ones that could put the entire organization in jeopardy.

How the pandemic has increased risk

All the factors discussed above contribute to the fact that healthcare facilities suffer badly from cyber-attacks. But how has that changed during the pandemic?

An increase in attacks

Cyber-attacks, and especially ransomware attacks, against hospitals have increased in number and severity over the last 7 to 8 months. At least 41 healthcare providers experienced ransomware attacks in the first half of 2020, and since then, an increasing number of hospitals have been targeted. In the most recent incident, Universal Health Services (UHS), a Fortune 500 hospital and healthcare services provider, was hit by Ryuk Ransomware, that has impacted all of its U.S. sites.

Attacks are almost always result in data breaches

Given the more aggressive types of ransomware and other data stealing malware, it's no wonder that almost every successful cyber-attack now results in a data breach. These are financially costly, damage reputation, cause residual damage to patients and inevitably result in a regulatory headache for the breached facility.

The number of records compromised in cyber-attacks and data breaches is rising, according to HIPAA Journal:

> *Costs are also rising. An IBM study found that the average cost of a healthcare data breach stands at around $7.13 million globally and $8.6 million in the United States. This represents a 10.5% year-over-year increase.*

First-ever cyber-related casualty

It has long-been speculated that hackers would someday breach a medical device and cause harm to a patient. When that came to pass, the nature of the incident was far more mundane, and far sadder. A patient died after a hospital in the city of Düsseldorf was unable to admit her because its systems had been knocked out by a cyber-attack. While in transit to another hospital, the patient died, prompting a murder investigation by local authorities.

Hampering the efforts to find a COVID-19 vaccination

The world is eagerly awaiting a COVID-19 vaccine to help bring about the end of the pandemic, and many research programs are ongoing on many different vaccine technologies. Hackers from China and Russia, however, appear to be taking a "shortcut" by trying to steal COVID-19 vaccine research. These attempts are slowing down the development process. Sometimes, the disturbance isn't even intentional: Philadelphia-based software company eResearchTechnology (ERT), which offers software used in hundreds of clinical trials, was hit by a ransomware attack. Its software is used by QVIA, a research organization (CRO) that is assisting AstraZeneca's COVID-19 vaccine trial.

As the healthcare cybersecurity situation degrades, there are some international, national and private initiatives attempting to improve things. For example, Israel has announced plans for a national program to defend hospitals. In the UK, a fund was set up to provide free government cyber certification and training. It is not only governments that are assisting the healthcare sector, either. CTI-league is an organization comprising more than 3,000 cyber experts that was founded earlier this year and provides free assistance to healthcare facilities fighting cyber-attacks. They offer four pro bono services: Neutralization, Prevention, Supporting, Health-related support.

These are great initiatives that should have real impact in places where they can have influence, but no matter how positive and encouraging these initiatives are, it is still mostly up to the healthcare institutes themselves to fight off this offensive.

Recommended Actions

In medicine, it's often said that an ounce of prevention is worth a pound of cure. This is true in cybersecurity as well. Here are some fundamental actions that could immediately improve the cybersecurity posture of your healthcare facility.

Awareness and email security

Many cyber-attacks utilize the humans working at healthcare facilities. Better awareness will reduce their chances of downloading suspicious documents or clicking suspicious links. There have been so many examples of recent attacks on healthcare facilities that creating a realistic phishing simulation should not be too difficult.

Protect internet-facing devices

Email isn't the only penetration vector. Many cyber-attacks utilize open ports and remote access protocols. This is a pure IT hygiene issue that requires care and attention, but it is doable. Only necessary ports should be opened to the internet. In fact, researchers found vulnerable RDP ports increase the likelihood of a successful ransomware attack by 37%, and certain hackers are specifically stealing and selling RDP credentials on the dark web.

Prevent credentials theft

Once entry is gained, attackers utilize readily available tools such as Mimikatz to access servers and spread across the network. These utilize aggressive password spraying and other credentials stealing techniques. Having robust passwords will reduce the chances of these succeeding.

Implement endpoint security

Endpoints are the critical means of entry to your network and your assets. Having an advanced endpoint security solution on all endpoints and servers is a necessity to improve your healthcare organization's cybersecurity resilience.

Conclusion

Healthcare institutions are bearing the brunt of cyberattacks during the COVID-19 pandemic. Fortunately, there are steps you can take to protect your organization.

Learn more. For additional information on how SonicWall deploys Capture Client endpoint security, please visit www.sonicwall.com/endpoint.

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

SONICWALL

ExBrief-HealthcareCybersecurityInThePandemic-VG-3316