Check Point
SOFTWARE TECHNOLOGIES LTD

NEW PARADIGMS IN PATIENT CARE: ADVANCED CYBER SECURITY

Introduction

Eighty-two percent of hospitals have reported significant cyber security incidents, but only 5% of hospital spending is directed towards cyber security[1]. Given the recent spate of ransomware attacks, hospitals are beginning to see how cyber security is not only an IT issue, but how it is also inextricably linked to patient care. Although you may have HIPAA-compliant cyber security in place, granular visibility, an automated architecture, and comprehensive IoMT protection can help you go beyond mere regulatory compliance; build a system that safeguards patient data, and the patients themselves. This paper will discuss foundational concepts for establishing excellence in cyber health.

The role of HIPAA

For all of its utility, The Healthcare Information Privacy and Accountability Act (HIPAA) data privacy law only pertains to data, meaning that it is a low bar when it comes to securing your system. The law does not mandate that healthcare organizations take steps to secure all attack vectors, including devices and other accessories that are critical in delivering high-quality patient care.

Says one medical IT expert, HIPAA represents "...a floor, not a ceiling, and that you can be compliant, but not secure."[2]

For optimal patient care outcomes, hospitals should set their target levels of security beyond that of outdated, federally imposed policies. HIPAA was first introduced to the US congress in 1996, and updated in 2006. Since then, technologies have evolved and cyber criminals have developed more sophisticated tactics. Security must correspond to the modern threat landscape, even if the laws haven't kept pace.

In the eyes of another expert, "...most hospitals are just a few clicks away from a multi-million dollar due care/due diligence lawsuit."[3]

[1] "5% of Hospital IT Budgets go to Cybersecurity Despite 82% of Hospitals Reporting Breaches", Mackenzie Garrity, March 12th, 2019

[2] "Cybersecurity in Hospitals: A Systematic, Organizational Perspective," Journal of Medical Internet Research, Mohammad S. Jalali, MSc, PhD., and Jessica P. Kaiser, Vol 20, No. 5, May 2018.

[3] Luis Ayala, *Cybersecurity for Hospitals and Healthcare Facilities: A Guide to Detection and Prevention*, (Fredericksburg, Virginia: Apress, 2016), Preface.

Granular visibility

To ensure the smooth and consistent delivery of patient care, and to ensure business continuity, hospitals need clear visibility into cyber security data analytics. You need to be able to obtain a quick drilldown of what's on your system, and who's on your system in order to prevent and detect cyber threats.

As a system administrator, you're responsible for knowing what's on your system. Do you have a precise inventory of how many devices, applications, and building control systems are connected to your network? It's time-consuming to keep track, and tough to untangle as an emergency unfolds. A solution with unified threat visibility insights can help quickly isolate a suspicious device or activity, and rapidly help you transition from analysis to action.

In addition to tracking what's on your system, you also need visibility into what's out there about your system. In the interest of highlighting successful client relationships, third-party vendors may electronically publish information describing the types of services their clients have purchased, and how the services were installed. Cyber security consultants have obtained maps of organizations' networks, information about firewall policies, source code for key applications, and more from simple internet searches. Hackers can also find this information, and use it to exploit your system.

Once on your system, it's imperative that you can see the intruder/s before any damage can occur. Unfortunately, hackers have plenty of options for probing a computer network undetected. Using spyware, for example, hackers can collect login information, financial data, and other records that they can later use against you. Advanced Persistent Threats (APTs) can continue for months or years before anyone notices.

Real-time alerts, precise CVE matching, network segmentation, and log data analysis can assist with detection. When hackers can see into your network, you need to see them[4].

REAL-TIME ALERTS

Real-time alerts help protect your organization from Advanced Persistent Threats (APTs), malware, and ransomware. Real-time threat analysis can also engage machine learning tools that identify previously unknown threats.

PRECISE CVE MATCHING

Identify assets with known vulnerabilities (CVEs)—all the way down to firmware versions for industrial devices. See into the unknown.

LOG DATA ANALYSIS

Most organizations understand the importance of collecting and analyzing raw log data, however the sheer volume of data can create operational paralysis. Typical intrusion detection systems generate hundreds of messages every few seconds, making data analysis a mess. However, with advanced regression cyber security technologies, you can effortlessly obtain comprehensive and granular visualizations.

Automated security

Investing in an automated cyber security solution can improve your team’s productivity, adverse event reaction time, and error rate.

An automated solution can reduce the volume of repetitive and time consuming tasks that your team manages. Automation can take care of laborious items like conducting cyber forensics investigations, managing user permissions, and tracking and patching devices. It can review and assess massive quantities of data, a task that’s often too large for any one person, or even a small team. The number of data sources, especially when tied to disparate tools, impedes the rapidity of real-time review. Automated security offers relief to your team, functions at a fast-pace, and detects patterns that may otherwise go unnoticed.

[4] “AAD-Asset and Anomaly Detection Datasheet”, October 21, 2018, Check Point Software Technologies

Automated security offers relief to your team, functions at a fast pace, and detects patterns that may otherwise go unnoticed.

Offloading certain tasks to an automated system reduces productivity bottlenecks and frees employees to devote their time to more complex responsibilities. With an automated solution, your team can optimize the workflow, elevating your organization's cyber security posture.

Ten percent of all US deaths are caused by hospital error, making hospital error the third leading cause of death in the country. Well-intentioned, but overworked IT staff are just as prone to making mistakes as nurses and physicians. By removing humans from the equation, automation can lower your risk of negative outcomes; both when it comes to everyday hospital functionality and patient care.

When it comes to hospital functionality, automated detection of a cyber intrusion can prevent building control and emergency control disruptions. Unauthorized access to building controls can potentially lead to electrical failures, render water unpotable, disable the public address system, trigger alarms, cause problems with fire sprinklers, and more.

An automated detection system can also identify instances of hackers attempting to manipulate patient care. The wrong IV dosage can be lethal. Patients and family members should never endure additional trauma on account of preventable mistakes. Leveraging automation could be life-changing, and life-saving.

> " Anything you're [hospitals] are buying today has not been built as secure by design..."

The Internet of Medical Things (IoMT)

IoMT has done wonders for the medical profession, and for patients. It has facilitated improved care coordination, better data analytics, and more favorable patient outcomes. However, securing the Internet of Medical Things has become a prescient problem that healthcare organizations are struggling to address. "Anything you're [hospitals] are buying today has not been built as secure by design, most likely" notes one expert[5].

Healthcare systems have arranged IoMT devices so that they can communicate patient-specific data from one device to another. Electrocardiogram waveforms can transfer information to electronic health records, enabling physicians and patients to make better healthcare decisions. However, these interconnected devices or platforms are vulnerable to attack.

To see just how vulnerable, the Mayo Clinic requested for a team of white hat hackers to probe 40 active devices. The investigative team discovered that every single tested device contained vulnerabilities. They noticed, for example, that monitoring equipment at a nurses' station would not pick up unauthorized and illegal changes made to the dosage within a patient's infusion pump. As a result, a patient could suffer severely.

It's not just interconnected devices that are at risk of unauthorized cyber manipulation. Isolated, but internet networked, devices are also at risk. Research indicates that X-ray machines, picture archives, blood analyzers, ultrasounds, PET scanners, CT scanners, MRI machines, therapeutic equipment, and life support equipment can be hacked. Modern ECG and EEG monitors, blood pressure machines, and electronic stethoscopes aren't immune either[6].

While hackers' current motives in attacking healthcare institutions are largely financial, experts suggest that, "It's just a matter of time before terrorist hackers take control of hospital diagnostic, treatment, and surgical machines and attempt to injure patients."[7]

[5] "Medical Device Cybersecurity will be Rubbish for 20 More Years," ZDNet, Stilgherrian, August 21st, 2019

[6] Luis Ayala, *Cybersecurity for Hospitals and Healthcare Facilities: A Guide to Detection and Prevention*, (Fredericksburg, Virginia: Apress, 2016), p.19

[7] Luis Ayala, *Cybersecurity for Hospitals and Healthcare Facilities: A Guide to Detection and Prevention*, (Fredericksburg, Virginia: Apress, 2016), Introduction

Secure overlays to protect and segment these insecure IoMT devices are essential. Increasingly advanced IoMT cyber security solutions are making their way onto the market. As you begin to explore hospital asset detection systems, search for multi-pronged, consolidated solutions.

In conclusion

Managing cyber threats is an acute pain point for many healthcare and hospital systems. The frequency and intensity of cyber threats are increasing, and it's time to prioritize your organization's cyber health.

A case in point

"Check Point lets us block threats before they can get into our system. It's an ideal way to keep our employee, patient, and business information safe." — IT Security Engineer, Premier U.S. Regional Hospital

This healthcare facility wanted to meet government healthcare regulatory requirements, but also invest in security that goes above and beyond. Get the details here.

To learn about how a single, consolidated architecture with granular visibility, automated tools, and IoMT protections can help your organization, visit the Infinity web page, or contact your Check Point representative.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233
www.checkpoint.com