How Healthcare Organizations Can Protect Themselves From Increasing Cyber Threats

The Threat Is Real – The Time Is Now

The need for increased network security is an absolute must. Geopolitical uncertainty has dramatically increased the chances that healthcare organizations will experience more security attacks in the next couple years. Specifically, SecOps teams need to prepare for even more ransomware attacks to extort money along with “lights out attacks” designed to cripple day to day operations.

The last two years have proven that the statement, “No one would want to hurt a hospital or healthcare clinic,” is a false narrative. Cyberattacks against network servers in the healthcare sector rose 35% in 2020 and another 53% in 2021, according to Fortified Health Security reports. Bad actors are making sure that healthcare organizations either spend now on security defenses or pay later for ransoms, fines and lawsuits.

However, you don’t want to waste money. You need a plan that gives you the visibility and security you need with repeatable simplicity that aligns with security frameworks (like NIST and MITRE) and HIPAA regulations.

Make Network Security SMART

Due to rising geopolitical tensions – time is of the essence. An easy way to increase your security upgrades is to make them SMART (Specific, Measurable, Achievable, Relevant, and Time-Bound), just like employee initiatives. You can start the process with a three-point plan focused on prevention, detection, and vigilance.

Here are some focused recommendations from this three-point plan:

1. Deploy an inline security solution to reduce as many vulnerabilities within the network as possible
2. Hunt down intrusions to find and quickly remediate intrusions that are discovered in the network
3. Periodically test your defenses with breach and attack simulations (BAS) to make sure they are actually detecting and blocking threats

Inline security solutions are a high impact technique that address security threats, especially ransomware targeting healthcare networks. These solutions can eliminate 90% or more of incoming security threats before they even enter your network. An inline security solution includes both security appliances (like an intrusion prevention system (IPS), web application firewalls (WAF), TLS 1.3 decryption, etc.) and

infrastructure components like external bypass switches and network packet brokers to access and deliver complete data visibility. This allows for the examination of ALL suspect data entering the network.

Unfortunately, inline solutions cannot prevent everything. This is why you need a second level of defense that helps you actively search for threats. This part of the plan uses taps and network packet brokers to capture relevant packet data and then feed that data to purpose-built threat hunting tools to proactively look for indicators of compromise (IOC) within network components and Internet of Medical Things (IoMT) devices.

The third level of defense is to periodically validate that your security architecture is working as designed. This means using a BAS solution to safely check your defenses against real-world threats to find any holes before hackers find them for you.

Expect The Unexpected

A final step is to focus on cyber resiliency. Once a cyber-attack or breach has been launched, you obviously need to stop the threat. However, it is just as important to get back to normal operations as fast as possible to maintain business continuity and satisfy patient needs. The key to making cyber resiliency work safely is to engineer your security architecture with self-healing capabilities from the start.

Some examples of engineered cyber resilience include:

- External bypass switches that use heartbeat messaging. These devices can be set to Fail Open or Fail Closed, as you choose, and revert back to normal operation once a problem is resolved. This creates a self-healing architecture.
- The use of inline and out-of-band network packet brokers that have n+1 survivability functions for security applications. This increases network reliability and delivers additional inline security fail-over techniques.
- Clustered security appliance configurations for improved survivability
- Inline packet brokers with Active-Active processors that provide enhanced business continuity without loss of data. Active-Standby solutions lose data when the standby processor comes online.
- Use of network packet brokers that support integration to SIEMs. This allows your network to use automation to collect data faster and thwart security attacks as fast as possible.
- A BAS solution that supports a recommendation engine that quickly tells you where problems exist and how to fix them. Some BAS solutions can even communicate the necessary remediation to SIEMs to increase speed of reaction to security attacks.

Keysight Technologies and our technology partners can show you how to fortify your network against multiple threat vectors within your healthcare practice.

Learn more at: www.getnetworkvisibility.com/HealthcareSecured

Keysight sponsors GetNetworkVisibility.com, a thought leadership website dedicated to the importance of packet-based visibility to power security, performance, and network monitoring tools. For more information, contact us at:

www.getnetworkvisibility.com/contact-us/