aruba
a Hewlett Packard Enterprise company

AT A GLANCE

MODERNIZING CYBER SECURITY IN HEALTHCARE

Healthcare is one of the most targeted and breached industries by cybercriminals. Stolen electronic medical health records are highly lucrative as they give a comprehensive and multi-faceted profile of an individual from which to launch personal identity theft scams as well as phishing and a variety of other cyberattacks to gain access to company networks.

BROAD ATTACK SURFACE

Healthcare network infrastructures are complex. The physical facility is open to a constantly changing array of new visitors who access guest networks with personal devices or can even connect into unsecured wired ports. The network supports many different types of Internet connected IoT devices and sensors in addition to staff computers, tablets and handhelds - both company owned and BYOD. And with the expected useful life of biomedical devices at 10+ years, IT and security teams also have to deal with older, outdated connectivity and security standards. All this widens the attack surface and makes the infrastructure more difficult to secure.

CLOSING THE GAPS

Although healthcare organizations are investing in cybersecurity, recent breach statics suggest there are opportunities for improvement to stay ahead of threats. Most traditional security solutions focus on securing the perimeter by detecting "known" malware by their patterns or signatures. Yet, advanced targeted attacks, "new" never before seen threats or variations of known malware that don't match known patterns easily bypass these types of traditional solutions.

There has been an upward trend in data breaches over the past 9 years. Healthcare data breaches are now being reported at a rate of more than 1 per day.[1]

Healthcare breaches of 500+ records during 2009-2017[1]:

- 2,181 breaches
- Theft/exposure of 176.7M patient records
- 54% of US population

- HIPAA Journal

On the black market, the going rate for your social security number is 10 cents. Your credit card number is worth 25 cents. But your electronic medical health record (EHR) could be worth hundreds or even thousands of dollars[2]

- Forbes

Reference Sources:
[1] https://www.hipaajournal.com/healthcare-data-breach-statistics/
[2] https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#4257843850cf

Let's investigate how two modern security solutions from Aruba that focus on detecting advanced attacks and preventing unauthorized network access can help healthcare organizations better:

- Ensure that the appropriate IT access policies are applied to users and devices
- Detect and investigate attacks by malicious, negligent and compromised insiders
- Secure and profile inherently insecure IoT devices and sensors

ACCESS CONTROLS

Security starts with visibility of who and what is connected to your network and what they are doing on the network at all times.

- **"Zero Trust" Access to the Network**
  Aruba ClearPass NAC (Network Access Control) delivers discovery, profiling, authentication and authorization of users, their devices and IoT devices before letting them on the network or giving them access to IT resources. These pre-admission controls are critical because cybercriminals are adept at quickly advancing and moving laterally within seconds after gaining access to a network.
- **Precise Control of Access to IT Resources and Assets**
  ClearPass provides adaptive, granular policy-based access controls by user, device, role and location, including for applications. These controls ensure that each user, device or IoT only has access to the network and IT resources and assets they are approved for.

SECURE ON THE INSIDE

Protecting against advanced attacks that are active on the inside of a network is critical.

- **"Adaptive Trust" with Continuous Activity Monitoring**
  Aruba IntroSpect UEBA (User and Entity Behavior Analytics) uses machine learning and analytics to continuously monitor behavior of users and "entities" (i.e, anything with an IP address such as a user device, server or IoT device) looking for indicators of unusual activity that indicates a gestating attack.
- **Advanced Attack Detection**
  Using a combination of self-learning and trained machine learning models, IntroSpect detects stealthy hidden attacks that traditional perimeter based security solutions have missed.
- **Accelerated Incident Investigation, Prioritization and Response.**
  IntroSpect uses "Risk Scoring" to prioritize risk into a single number and comprehensive "Risk Profiles" to dramatically accelerate investigation. Incident response is orchestrated within IntroSpect and/or with third party solutions such as ClearPass, SIEMs and other security solutions.

NEXT STEPS FOR A HEALTHIER SECURITY POSTURE

With advanced access controls and security that addresses hidden attacks from the inside, and interoperability with over 140 multi-vendor network and security solutions, you can rest assured with the visibility and confidence that your security posture is in a much healthier state.

LEARN MORE

- https://www.networkworld.com/article/3327211/internet/802-11ax-means-more-iot-now-how-do-i-secure-it.html
- https://www.arubanetworks.com/solutions/healthcare/
- https://www.arubanetworks.com/solutions/security/
- https://connect.arubanetworks.com/ponemonsecurityreport
- https://connect.arubanetworks.com/carta

aruba
a Hewlett Packard Enterprise company

AAG_SecurityInHealthcare_032019 a00065994enw