5 Cyberattack Vectors for MSSP to Mitigate in Healthcare

July 11, 2018 / in BYOD and Mobile Security / by Joe Velderman

It's no secret that healthcare continues to be one of the most targeted industries for cybercriminals. Healthcare providers store and maintain some of the most valuable data and the appetite for fraudulent claims or fake prescription medications is insatiable.

Despite all of the regulations, there are still fewer watchdogs overseeing healthcare. For many providers, cyber security hasn't been a priority until very recently.

With more and more organizations reaching out to cyber security experts for assistance, it's more important than ever that managed security services providers (MSSPs) understand the healthcare industry so that they can tailor solutions aimed at improving the security posture of healthcare providers.

Inside Users Present the Greatest Threat

According to a 2018 survey of cyber security professionals conducted by HIMSS, over 60 percent of threat actors are internal users within a healthcare organization. Email phishing and spear-phishing attempts are aimed at tricking users into providing credentials or access to information for cybercriminals. Negligent insiders, who have access to trusted information, can facilitate data breaches or cyber incidents while trying to be helpful.

In addition to systematically monitoring and protecting infrastructure components, MSSPs need to consider a multi-faceted campaign that creates a cyber security awareness culture within healthcare organizations. This campaign should include template policies and procedures for organizations to adopt, regular and routine training efforts, and human penetration-testing.

From a systematic perspective, it's important to have tools that will do everything possible to mitigate cyberattacks. Tools like next-generation email security to block potential phishing or spear phishing attempts; endpoint security solutions to monitor behavior through heuristic-based techniques; and internal network routing through a next-generation firewall to perform deep packet inspection (DPI) on any information transgressing the network — especially if it's encrypted.

Mobile Devices Open Large Attack Surfaces

Mobile devices have changed the way that we do just about everything. And the same is true for the manner in which healthcare conducts business.

To enable mobility and on-demand access, many electronic health record (EHR) applications have specific apps that create avenues for mobile devices to access portions of the EHR software. The widespread adoption of mobile devices and BYOD trends are pushing healthcare to adapt new business models and workflows. Cyber risk mitigation must be a priority as momentum continues to build.

MSSPs need to pay very careful attention to the access that mobile devices have to the EHR application, whether hosted on-premise or in the cloud. For more protection, implement a mobile device management (MDM) solution if the organization doesn't already have one.

IoT Leaves Many Healthcare Providers at Risk

The Internet of Things (IoT) is bringing connectivity and statistical information to providers in near real-time while offering incredible convenience to the patient. Even wearable devices have immense capabilities to monitor chronic illnesses, such as heart disease, diabetes and hypertension. With these devices comes an incredible opportunity for hackers and immense threat for healthcare providers.

IoT devices tend to have weaker protections than typical computers. Many IoT devices do not receive software or firmware updates in any sort of regular cadence even though all of them are connected to the internet. There are so many manufacturers of IoT devices, and they are distributed through so many channels. There are no standards or controls regarding passwords, encryption or chain of command tracking capabilities to see who has handled the device.

If it's feasible for the organization, totally isolate any IoT-connected devices to a secure inside network not connected to the internet (i.e., air gapped).

Encryption for Data at Rest Is Critical

For healthcare providers, it's equally important to have a strong encryption for both data at rest and data in transit. Encryption for data at rest includes ensuring the software managing PHI doesn't have a really weak single key that could unlock everyone's PHI. If at all possible, records should be encrypted with unique keys so that a potentially exposed key doesn't open the door to everyone's information.

Attacks Are Hiding within Encrypted Traffic

MSSPs serving healthcare organizations need to realize that there is not one layer of defense that they should rely on. That said, perhaps the most important layer is the firewall.

A next-generation firewall, with DPI capabilities, is a critical component to securing a healthcare network. Even internal traffic transgressing the network should be routed through the firewall to prevent any potential malicious traffic from proliferating the entire LAN and to log transactions.

As much as possible, isolate medical devices and software applications that host PHI inside a secure network zone and protect that zone with an internal DPI-capable firewall that will only allow access to authorized services and IP addresses.

About ProviNET

ProviNET is a SonicWall SecureFirst Gold Partner. For nearly three decades, ProviNET has delivered trusted technology solutions for healthcare organizations. Whether it's a single project or full-time onsite work, ProviNET designs and implements customized solutions so healthcare organizations can focus on core services.

ProviNET's tight-knit group of experienced, industry-certified personnel are focused on customer satisfaction. They are a reputable organization, fulfilling immediate IT needs and helping plan for tomorrow. They are ready to put their extensive knowledge to work for healthcare, developing strategies and solving challenges with the latest technology.

To learn more about ProviNET, please visit **www.provinet.com**.

JOE VELDERMAN

Director of Consulting Services | ProviNET Solutions

Joe Velderman has extensive experience providing advisory services to the senior living and long-term, post-acute care industry. ProviNET Solutions is a full-service technology consulting partner that was born out of a senior living provider and aims to help organizations be successful with technology. Joe developed a passion for ensuring healthcare organizations maintain regulatory compliance, but also mitigate cybersecurity risks. He routinely contributes thought leadership on this topic through whitepapers, blog posts, educational webinars and speaking engagements.

Tags: Cyber Security, Encrypted Traffic, IoT, MSSP, next generation firewalls