TOP 5 CYBERSECURITY TRENDS FOR 2020

NAVIGATING TECHNOLOGY, SECURITY, AND COMPLIANCE

HC3 Advisors has released what it believes are the top 5 cybersecurity threats to the healthcare industry for 2020. Using cybersecurity intelligence to better understand how attacks have evolved and are continuing to evolve can help your organization better deploy your defenses to match the current threat and not last year's threat.

HEALING HEALTHCARE SECURITY

HC3 Advisors warns not to get too distracted by healthcare specific needs. Patching, monitoring and response protocols are the basics that can make the highest impact.

1. PHISHING ATTACKS CONTINUE TO RISE

Ransomware will continue to be a major security threat to healthcare in 2020.

Ransomware will continue to be a major information security threat to healthcare in 2020. Majority of ransomware will be propagated through various phishing methods that trick people and ultimately leads to the encryption and demand for payment to regain access to files and systems. Even then, paying the ransom doesn't guarantee that your systems will be restored. A variety of healthcare related facilities were struck by ransomware in 2019 and HC3 Advisors predicts that this number will only increase in 2020. Because Healthcare is a high value target, attackers are going to increase the frequency and sophistication of attacks with more targeted approaches. This will continue to be a nightmare for health systems that are unprepared across people, processes and technology spectrum.

Some of the reasons to the increase in ransomware attacks are that there is a significant increase in the availability of malicious code on the black market. Cyber criminals have made the source code more available, affordable, and easier to access. Ransomware as a service (RaaS) continues to be the best way for inexperienced cybercriminals to get started in ransomware, and underground forums are flooded with ads for different RaaS offerings at all price points. This code is then further modified by the purchaser to make certain that current security products that may have detected the original code will likely fail with the modified version. As a result of increased access to affordable code, HC3 Advisors predicts a steady increase in attacks over the course of 2020.

2. CONCERNS OVER CLOUDS SERVICES

As more and more of the healthcare industry moves to the cloud it is not without its own set of unique security challenges.

As more and more of the healthcare industry moves to the cloud, it is not without its own set of unique security challenges. As part of the appeal to moving to the cloud, the assumption was that data stored in the cloud must be as secure if not more secure than on premise solutions. The beauty of the cloud from an adversary perspective is that it greatly reduces the reconnaissance time looking at on-premises defenses for vulnerabilities. And contrary to what many might think, the main responsibility for protecting corporate data in the cloud lies not with the cloud service provider but with the cloud customer. The truth is the data you store in SaaS applications are not protected from attacks at your end which includes human error, malicious deletion requests, phishing, and more. With so much data going into the cloud and into public cloud services in particular, these resources become natural targets for hackers to exploit.

Cyber attackers are also targeting cloud backups and when they find backups stored in the cloud, they attempt to obtain the cloud storage credentials and then use them to restore the victim's data to servers under the attacker's control. Once they are able to gain access, they simply login to the cloud services and download it from your server, fully invisible to your data breach detection software. As the attackers are restoring the data, it won't raise any warnings for the victim as their servers appear to be operating normally.

As healthcare continues its transition to cloud services, enterprises are starting to question if any particular cloud service provider is more ‘secure’ than others. Cloud services offer a lot of benefits and security is a big issue and the key is to do proper due diligence with your cloud providers and really understand their security safeguards and responsibilities.

3. VULNERABILITY OF HEALTHCARE SUPPLY CHAINS

Healthcare organizations often overlook the supply chain, which many security researchers say is where they are the most vulnerable.

Healthcare organizations often overlook the supply chain, which many security researchers say is their most vulnerable asset. Healthcare systems have been adopting automated supply chains with the goal of greater efficiency and lowering costs. When prescription drugs, medical devices, and other medical supplies are in an optimized supply chain, healthcare providers see their costs lowered, their revenues enhanced, and, most importantly, their quality of care improved. These supply chains leverage Internet of Things (IoT) automation, robotics and big data that form these smart supply chains that track where a product or its components can be located at any time. Nevertheless, smart supply chains are dynamic and efficient, but are also prone to cyberattacks. When one element is compromised there can be cascading effects up and down the supply chain. As an example, the WannaCry virus may not have specifically targeted the healthcare industry but the ransomware impact left its mark by blocking National Health Service (NHS) to trust hospitals from accessing patient records and forcing doctors to reschedule appointments and surgeries. The profound effect on the healthcare industry prompted researchers to investigate the healthcare network and specifically how supply chain cyberthreats, and exposed connected medical systems and devices, affected organizations' security posture.

4. MEDICAL IOT DEVICES ARE SPREADING FASTER THAN THEY CAN BE SECURED

The trend towards owning a medical device increases the risk of an Internet health crisis.

The healthcare sector relies heavily on its connected devices, including medical device IoT, to ensure seamless patient care. However, many of those devices operate on outdated systems that leave these vulnerable endpoints open to attackers. Medical IoT devices have some of the highest rates of legacy Windows 7, XP and other legacy OS versions and unfortunately, a high percentage of these devices are now connected to networks, giving healthcare some of the biggest exposures.

The challenge lies in the shelf life of these devices already operating within the healthcare organization. Some devices cost millions of dollars to replace and it is simply not feasible from a capital standpoint to replace them. Instead, some organizations choose not to patch even with known security risks, as devices may not support newer versions. However, the risk these vulnerable devices pose will significantly increase as time goes on and by failing to patch them will only heighten the risk of exposure.

Healthcare organizations will move up the cybersecurity maturity model in 2020, and those that do not effectively address their IoT exposure particularly small to medium size healthcare organizations, will continue to face devastating cybersecurity threats, HC3 Advisors predicts.

5. ARTIFICIAL INTELLIGENCE (AI) THE NEW WEAPON

Artificial Intelligence (AI) is the new technology arms race.

Artificial Intelligence (AI) is the new technology arms race where both sides are looking to it for an advantage. Just as AI can “learn” to spot patterns that could signal an attack, it can also learn to adapt and disguise the same behavior to maneuver its way around your security defenses.

Many organizations acknowledged they could not respond to critical cyber threats without the help of AI technology. It can detect patterns, then give alerts if network traffic shifts or a person uses a product different from their norm. This can also lead to false positives which can waste the better part of a security analyst’s day but having an Artificial Intelligence program smart enough to recognize what is a real threat and what is just background noise will be critical in fending off hackers and malware.

Cyber hackers using AI in their tool arsenal are becoming a very real threat that companies need to prepare for. Hackers have started equipping themselves with their own machine learning algorithms that will help them attack companies and users in a way that escapes detection. In order to counteract these advances on the adversarial side, cybersecurity teams need to be armed with the best defensive tools possible.

As the industry shifts from supervised AI models towards autonomous AI systems, it will mark the beginning of a much more technologically forward decade. The tug of war between hacker and security team will go on with more advanced cyber weapons and defense methods, but the real test will be parsing through all of the misinformation and false marketing claims of ‘Artificial Intelligence’ that isn’t intelligent at all, and finding the programs that actually work.