www.pipelinepub.com
Volume 19, Issue 3

Protecting the Healthcare Sector from Supply Chain Security Attacks

By: **Dennis Mattoon**

With a cyberattack occurring every 39 seconds, not only are they becoming more frequent, they are becoming more sophisticated and premeditated. Attackers have begun targeting supply chains, which is especially worrying as one attack can create a chain reaction and compromise a network of providers.

With many stages and companies involved, hackers are benefiting from the lack of sufficient security by infiltrating systems with malicious codes, compromising the code shipped into hardware components and gaining access to data. This is particularly concerning for the healthcare sector when the patient's health depends on having secure equipment and services provided to them. To overcome these challenges on a global scale, security must be at the top of every organization's agenda to boost protection and bolster personal safety.

Supply chain security in the healthcare sector

Cyberattacks on vulnerable supply chains are making it difficult to implement successful security practices, which poses a challenge to the healthcare sector. Modern manufacturing is a highly complex process, which requires components to comply with safety and health regulations. Owing to the magnitude of cyber threats, it is also important to check that every stage of the supply chain is cyber secure and cannot be accessed by hackers. One of the most significant issues is the ability for malware to go undetected, which can inflict damage without anyone noticing for a long time by targeting these large organizations from one single entry point. With hackers able to stay hidden, hardware, software, and IT networks risk being compromised, and this can have devastating consequences for patients in hospitals.

If hackers gained access into hospital systems, they would be able to gain access into patients' confidential records, which they may hold hostage for financial gain, or be able to affect the sensors within vital machinery, leading to life-threatening risks. In the US, there have been several cases in which attackers have caused significant disruptions to operations, leading to a delay in chemotherapy treatments. In 2019, a newborn suffered fatal brain damage due to a heart monitor failure as a result of a ransomware attack, while ambulances in San Diego were diverted away from emergency rooms because of frozen computer systems. As recently as October 2022, the digital tools used by medical professionals at Des Moines Hospital to accurately prescribe doses of medicine were corrupted as a result of a cyberattack, leading to a three-year-old child receiving five times the required amount. When putting together medical equipment within the supply chain, it is important to check that it meets the safety regulations, but as mentioned earlier, it is also essential to check it hasn't been tampered with or hacked into, or this can lead to significant consequences for any patients found at the end of the chain.

One of the reasons that supply chain hacks have become more common is the increased digitization brought by the pandemic, with more providers switching to telehealth to connect with patients. Telehealth leverages digital communication technologies to allow patients and other users to remotely access any relevant medical services to help manage their health care. Devices such as tablets and smartphones are commonly used to access these services, while nurses or other healthcare professionals can provide these services from a medical office or mobile van if the patient resides in a rural area. doesn't even factor

This can affect the supply chain because if hackers can access any device used for communication between the patient and the healthcare professional, they can quickly gain access to any personal, sensitive data. This can cause significant financial damage to any hospital or clinic that falls victim to an attack. In 2016, a successful ransomware attack led the Hollywood Presbyterian Medical Center to pay $17,000in Bitcoin in order to regain access to its files and records. This cost in the reputational damage such an attack can cause to an organization, and as such, there needs to be better risk management in order to safeguard the patients under a hospital's care. Yet all too often the security measures currently in place within the healthcare industry are not designed to overcome the rise of such new and sophisticated attacks.

Supply chain attacks are dangerous for those affected but are also immensely costly, especially for healthcare organizations where the main objectives are to improve health and save lives; they don't want to be spending money on procuring new equipment as a result of malicious tampering. This further demonstrates the need for the healthcare sector to strengthen its cyber security measures to alleviate these challenges.

Mitigating the risks of cyber attacks

Although security measures are in place, most rely on human intervention, such as visual inspection within the supply chain. This includes monitoring the alignment of labels, verifying the authenticity of serial numbers, and checking the shape of markings. However, these tasks are very costly and require copious amounts of time, which many organizations simply do not have. Some systems may also not be completely up to date with security protections and updating these needs to become a priority for the industry.

To mitigate the risks of hacking, organizations should adhere to the principles of trusted computing—and so should every other user, company or supplier in the supply chain. If one stage or process has insufficient security, the entire supply chain will be more susceptible to hackers and can create huge amounts of risk and challenges. To address this, the Trusted Computing Group (TCG) has developed the Firmware Integrity Measurement (FIM) specification, which acts as a way to determine the security status of multiple endpoints with a network by providing guidelines to review the integrity of a device at the manufacturing stage and offering a baseline measurement that allows for security result comparisons throughout.

The FIM specification verifies that an endpoint device has been received by the end user and matches what they had ordered. The FIM can then be measured and compared to the Reference Integrity Measurement (RIM) to detect if the hardware has been compromised. Thus, at any point of a supply chain, manufacturers can determine the integrity of a device.

TCG’s aim is to reduce the risk of cyberattacks to zero, by using cybersecurity professionals to educate and make cybersecurity top of the agenda, so that industries such as the healthcare sector will be protected from threats. Adhering to the measures provided by TCG will help minimize these risks and prevent the attacks from occurring by ensuring verification of the different stages of the supply chain before the equipment physically arrives at the hospital. Organizations must actively put measures in place to utilize the tools and technologies to detect malware, so that cybersecurity does not become a bigger issue. Thus, it is of the utmost importance for each player in the supply chain to do their part and take a security-first approach.

Keeping supply chain security measures up to date

Over time, hackers will keep evolving and becoming more sophisticated as more people rely on the Internet and digital technology. Therefore, it is critical to keep security measures up to date in all sectors, but especially the healthcare sector—where lives are at stake. Organizations and individuals working along the supply chain should continuously monitor the components, technologies, and practices as supply chains become increasingly more complex.