Current Vulnerabilities and Threats Affecting Healthcare

Week of November 18, 2019

Substance Abuse Facilities

A misconfigured Amazon Simple Storage Service exposed 93 million billing files that contained patient information from three drug and alcohol addiction facilities. These facilities located in San Juan Capistrano California, San Clemente California, and Bastrop Texas had left their data open and accessible. Exposed data consisted of names, email addresses, phone numbers, payment card numbers with CVV codes and health insurance information. Even though the database was made private after reporting of the incident, the data was still not secure as the files were still accessible without any password being required.

Google's Attempt at Acquiring Health Data

Google is working with Ascension, one of the largest healthcare systems in the country, to access sensitive personal health information of millions of Americans for their plan to acquire Fitbit. This is prompting lawmakers to take action on reforming competition law as Google may be cornering the market on health data. If Google acquires Fitbit, the sheer quantity of health data that they will own and what they plan to do with it is the topic of concern. Even though we have privacy laws in place, HIPAA policies only apply to specific "covered entities" –like hospitals—and their business associates; Google and Fitbit would not be applicable entities for this law.

Critical Flaws on Medical Devices

According to the Department of Homeland Security, recently patched vulnerabilities in the MedTronic Valleylab devices were allowing attackers to overwrite files and to achieve remote code execution. Even though the devices used the Descrypt algorithm for OS password hashing, and the network-based logons were disabled, attackers could use other vulnerabilities to get local shell access and obtain these hashes. The vulnerable devices should either be immediately disconnected from IP networks or the networks should be segregated to ensure none of the devices are accessible from an unsecured or untrusted network.

Malware Attacks on Hospitals

Over the course of this year, there has been a significant rise in trojan malware attacks targeting hospitals and the healthcare industry. Hackers view the healthcare industry as an easy target for stealing sensitive personal data. There has been a 60% increase in trojan malware detections in the first nine months of 2019. Two forms of trojan malware that are targeting healthcare industry the most are Emotet and Trickbot. Both forms are known for dropping ransomware onto compromised systems. Ransomware is not only affecting healthcare providers, but also patients themselves as hospitals store large amounts of personal data which can be used by hackers to commit fraud.

Our mailing address is:
11140 Rockville Pike, Suite 400
Rockville, MD 20851
301-200-9776