Current Vulnerabilities and Threats Affecting Healthcare

Week of December 16, 2019

Ransomware

In 2019, nearly 1,000 US government agencies, educational establishments, and healthcare providers have been hit by ransomware attacks. The healthcare sector continues to be the largest group hit by the attacks, resulting in cancelled operations, interruptions to 911 services, and delays to surgical procedures. In a 2019 report issued by the State Auditor of Mississippi, it stated that there continued to be a disregard for cybersecurity in all departments in state governments. This report found that many states do not have a security policy plan or disaster recovery plan in place. Government agencies, and related healthcare organizations must perform risk assessments regularly to make sure they are not encrypting sensitive information.

Breaches

Cheyenne Regional Medical Center (CRMC) located in Wyoming had a data breach in April that exposed patients' personal information, including dates of birth and social security numbers. The hacker appeared to be interested in payroll information but also accessed several employee email accounts that put 16,000 patient records in jeopardy. Although CRMC policies stated that patient information must be securely stored in the hospital's database, some information was exchanged via email for administrative purposes. Since the breach, CRMC has implemented further security measures surrounding internal network applications and has mandated continuous review and monitoring of its security processes.

Breach Impacts

The Phoenix-based healthcare delivery system, Banner Health, has agreed to pay up to $6 million to settle consolidated class-action lawsuits against their massive 2016 data breach. The hackers gained access to systems containing patient information and exfiltrated the protected health information of approximately 2.9 million patients. Malware installed in the food and beverage outlets in the facility had also managed to exfiltrate credit card numbers of 30,000 patients over a period of 2 weeks. The lawsuit alleges that Banner Health failed to implement appropriate safeguards such as multi-factor authentication, data encryption, and firewalls that would protect them against cyberattacks.

Dangerous Phishing Campaign

A phishing campaign was discovered in which access was gained through the recipient's Microsoft Office 365 account and data was accessed through the Microsoft OAuth API. This attack method is unique as it targets a victim's Office 365 account instead of directly stealing user's login name and password. OAuth is an open authentication and permission standard that is used to give third-parties access to user's account and perform actions on their behalves. Attackers display a "Permissions requested" dialog which allows them to access all of the user's data and services from their own servers. This method bypasses traditional defensive measures and is difficult to detect and remove. Strong security measures to authorize and manage external/remote access must be in place to protect user data and privacy.

Our mailing address is:
11140 Rockville Pike, Suite 400
Rockville, MD 20851