QI EXPRESS

HEALTH TECH
ACCESS ALLIANCE

Current Vulnerabilities and Threats Affecting Healthcare

Week of October 28, 2019

Health Sector- Data Breach

There were 19,000 patients and 3,000 volunteers from six Prisma Health-Midlands hospitals in South Carolina affected by a data breach. An employee’s login credentials were compromised which provided unauthorized access to patient pre-registration and volunteer registration information forms. Patient information that was exposed included names, addresses, date of birth, social security numbers and health insurance information. Hospitals and healthcare providers must take action to enhance their security measures as data breaches continue to affect the healthcare industry. The vast majority include a human element in which risk could be reduced through training and policy oversight.

Ransomware

In 2019, ransomware has increasingly been targeting healthcare organizations. Attackers are spending time gathering their victims’ information to ensure they can inflict maximum disruptions. Ransomware generates over $25 million in revenue for hackers each year. According to Cyber Security Ventures, an organization will fall victim to ransomware every 14 seconds in 2019, and every 11 seconds by 2021. Even the FBI has softened its stance on paying ransoms as it now acknowledges that organizations need to evaluate options to protect their customers and employees.

Adobe Exposed

On October 19, 2019, Adobe reported that 7.5 million records which contained Creative Cloud customer information were exposed due to a misconfiguration. The cause of the exposure was identified as an unprotected Elasticsearch database which was accessible without a password. The database stored Creative Cloud customer information such as email addresses, subscription status, member ID, payment status, and other account information. This leak could cause Adobe Creative Cloud users to be targeted through phishing emails and scams in the future. Organization of all sizes must be diligent.

Pharmaceutical Sector

Digital transformation and the increased use of automated control systems to manage drug formulations and product quality are creating new security risks for pharmaceutical companies as they adopt IoT technology. In June 2017, the pharmaceutical sector and many other industries were targeted by the Wannacry ransomware and were forced to halt operations upon discovering vulnerabilities. As a result, there is an urgency for protecting pharmaceutical Operation Technology networks from external attacks, insider threats, and human error. This requires a deep awareness of the state, configurations and changes made to each device. If unintended changes occur, they should be logged in real-time and should include the user who logged in, what processes were running, the code download initiated, as well as all changes in the environment. Maintaining this detailed audit trail will enable faster incident response and allow pharmaceutical manufacturers to demonstrate compliance with organizational security policies.

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