NATIONAL SUPPLY CHAIN INTEGRITY MONTH

HEALTH CARE

National Counterintelligence and Security Center Factsheet

April 2021

THREATS

Phishing Attacks - the practice of sending fraudulent communications disguised as information from a reputable source to gain access to a victim's machine to steal sensitive data or plant harmful malware.

- Over the past year, reports have shown a drastic increase in phishing attacks targeting the health care industry, causing data breaches and delays in critical medical functions. Cybercriminals have employed phishing campaigns to send fraudulent emails to health care administrators posing urgent messages related to Personal Protective Equipment information or vaccine schedules that hold malware links that, once clicked, allow access to the entire IT system. Phishing incidents are often used to steal patient financial and personal medical records.

Ransomware Attacks - installing a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable until the demands of the attackers are met.

- Ransomware attacks cause medical facilities dangerous setbacks. If the computer systems are not functional, critical patient care services can be interrupted. Other severe consequences of hospital ransomware attacks include diversion of emergency ambulances, delays in treatment, and inaccessible patient records. Hospitals often use public networks on due to limited resources, exposing them to cyber vulnerabilities.

COVID-19 Vaccine Attacks - represent important threats to a specifically vulnerable sub-sector of the health care supply chain.

- There are countless threats to COVID-19 supply chains. Reagents, chemical compounds, and other required ingredients needed for the vaccine mixtures are prime targets. Potential threats also can emerge through the information and communication technology utilized. Additionally, the need for COVID-19 vaccines to be stored at cold temperatures requires specialized storage units often powered by a connection to a public network system. Such exposure may allow the storage units to be disabled, rendering the vaccine supply useless.

BEST PRACTICES

Establish a Cyber Supply Chain Risk Management (C-SCRM) program across the health care organization

- Identify roles and responsibilities for each member of the C-SCRM program management team, including those in enterprise risk management, supply chain, cybersecurity, IT, business contracts, and legal.
- Develop guidance for each business unit detailing specific C-SCRM activities, consistent with roles and responsibilities.
- Provide organization-wide training for all executive stakeholders within the organization, such as supply chain, legal, IT, health administrators, and procurement.
- Integrate a formal training program for all personnel on cybersecurity strategies to improve detection and awareness of potential fraudulent emails.
- Institute protocols for securely terminating supplier relationships which ensure that all hardware containing data has been properly disposed of thus limiting the risks of data leakage.

Incorporate Supply Chain Security Protections

- Assess supply chain for potential disruptions and incorporate security measures to reduce risks.
- Identify alternative sources of critical components to ensure uninterrupted production and delivery of products and simultaneously grow indigenous sources of production to have parallel supply chain avenues.
- Determine if critical systems need to be connected to the internet at all times.
- Keep clear communication with all suppliers at each phase of the supply chain lifecycle.
- Implement guidance on securing data stored on hardware devices, even during disposal, that may contain regulated data (e.g., personally identifiable information [PII] or protected health information [PHI]) or otherwise sensitive information (e.g., intellectual property).
- Maintain offline encrypted backups of sensitive patient, personnel, financial, and administrative data.

NOTE: Information contained herein was gathered from the most reliable sources found in the public domain on supply chain risk management, including information from the Department of Homeland Security, the National Institute of Science and Technology, the Federal Bureau of Investigation, and the National Counterintelligence and Security Center.

The information on this product was prepared with the assistance of the 2021 Federal Virtual Intern Service.