NATIONAL SUPPLY CHAIN INTEGRITY MONTH

ENERGY

National Counterintelligence and Security Center Factsheet
April 2021

THREATS: Threats to energy sector supply chains often revolve around the disruption of reliable energy services to the consumer through the tampering or destruction of energy sector assets. Such threats include nation states, criminal organizations, and human errors within an energy sector organization. Nation-state actors often focus on espionage, theft of Intellectual Property, or the pre-positioning of malware to disrupt infrastructure or the energy supply chain in a time of crisis. Criminal organizations often direct their actions towards personal information and theft of data for profit. Human errors also pose threats to energy sector supply chains due to lack of training such as an employee failing to secure data or clicking on a spear-phishing email link. Whatever the threat may be, reducing risks to the energy sector requires an integrated risk reduction approach to protect and ensure a reliable and resilient energy supply chain.

Best Practices

- **Audit and review of vendor security practices**
  - Before contracting with a supplier, vendor, manufacturer, or any other third-party organization, it is essential to review their security practices. The third-party must have a supply chain risk management program as well as a robust risk-based approach to cybersecurity and supply chain security.
- **Implement endpoint detection, incident response, and Security Information and Event Management (SIEM) systems on devices to mitigate risk.**
  - Endpoint detection and response systems software detect irregularities on an endpoint device to mitigate threats that make it down the supply chain.
  - SIEM will collect information from across the network to normalize a level of function. The SIEM can alert a security team to abnormal events once a baseline has been established.
  - In concert, these systems guard against vulnerabilities that find their way into the supply chain.
- **Air gap critical systems involved in power generation, such as nuclear facility controllers.**
  - While connecting devices to the internet can increase efficiency within power facilities, certain systems should be kept offline due to criticality.
  - If a compromise of the system's integrity could result in loss of life or large-scale destruction, air gapping the system should be considered.
- **Restrict access to documents and systems.**
  - In general, having access control policies in place restricts access to the system and to documents that are not necessary for daily operations.
  - Access control policies limit the ability for insiders or intruders to tamper with outgoing products, manipulate updates, or infect the supply chain further down the line.
- **Identify responsible risk stewards over critical assets.**
  - A critical step of supply chain risk management is to identify who is responsible for risk associated with various parts of the supply chain. An organizational policy should be in place that clearly outlines the risk steward responsible for the asset in each phase of the supply chain.

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 in this product was prepared with the assistance of the 2021 Federal Virtual Intern Service