NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Security Guideline for the Electricity Sector - Supply Chain

Vendor Identified Incident Response Measures

The objective of the reliability guidelines is to distribute key practices and information on specific issues critical to promote and maintain a highly reliable and secure bulk power system (BPS). Reliability guidelines are not binding norms or parameters to the level that compliance to NERC's Reliability Standards is monitored or enforced. Rather, their incorporation into industry practices is strictly voluntary.

Introduction

The Supply Chain Cybersecurity Risk Management Plan ("Risk Management Plan") addresses, among others, risks that originate with vendors. The procurement process should include agreement on a risk management plan, inclusive of cyber-incident response elements such as identification, notification, mitigation, remediation, and recovery.

Defining a Vendor-Identified Incident

The definition of a vendor-identified incident and criteria of what poses a risk to the Bulk Electric System (BES) could differ from vendor to vendor and entity to entity. Discuss this definition with the vendor during procurement evaluation, to ensure there is a common, documented understanding of what both parties define as a vendor-identified incident.

Potential Incidents

Supply chain security measures protect a NERC entity's Bulk Electric System (BES) components from incidents that originate within the entity's supply chain. These incidents could occur outside the control or visibility of an entity's security program, but could still pose a risk to the products or services that support the BES. This in turn could compromise a vendor's development process, ongoing support of delivered systems, trusted connections between vendor and entity network(s), trusted communications channels, or vendor employees. Incidents could be attempts to gain access to or adversely affect an entity's BES systems, including, but not limited to:

System integrity compromises:

- Of the vendor code for patches, updates, software, installation or configuration files, used on a BES Cyber System at any point in the software development lifecycle
- Of vendor hardware such as malicious chip or board level implants or modifications, or malicious factory configuration
- Of manufacturing specifications or proprietary information that could be used by a malicious actor to exploit physical or cyber vulnerabilities

- Discovery of a back door or other potential for unauthorized electronic access to a BES Cyber System
- Vendor software (known or active exploitation of a software vulnerability by a malicious actor)

Vendor network compromises:

- To a vendor's computer network used for access to an entity's BES Cyber System(s)
- Of a vendor's trusted communication channels that may have been used to transmit malicious messages to an entity, such as postal shipped items, compromised file transfer systems or social engineering methods e.g. (phishing or vishing)
- Of a vendor's authorized remote access to an entity's network by a malicious actor

Vendor employee compromises:

- Vendor employee or anyone acting on behalf of vendor perpetrating a cybercrime or physical crime that indicate an increased risk to their customers, such as a violation of the Computer Fraud and Abuse Act[1], computer espionage, theft, trespassing, or acts of violence
- Vendor employee linked to terrorist organization, or organizations that promote attacks against the electric power industry

Coordination of Responses to Vendor-Identified Incidents

When a vendor becomes aware of an actual or potential incident (e.g., notification by a third party, public disclosure), the vendor should implement its notification process in a mutually agreed upon time and method. Notifications should include circumstantial and technical details, remedial steps being undertaken, recommended mitigations, and the method and timing for sharing updated information.

Based on the size and scope of the incident, direct communication with the entity might not be viable as the initial means of notification. Vendors may disclose incidents publicly or through an advisory organization such as the Electricity Information Sharing Analysis Center (E-ISAC), Department of Homeland Security, or Federal Bureau of Investigation. If disclosures occur in this manner, the vendor should notify entities with updated information throughout the incident investigation through established communications channels.

Establish mutual points of contact (or roles) with the vendor, in order to assure there are no single points of failure in the incident response process. Both parties should ensure that the established notification method(s) remain viable by testing the established process at an agreed-upon frequency.

Incident Response Lifecycle Considerations

Be prepared to activate an established incident response plan upon notification from a vendor of a cybersecurity incident. If an incident is discovered internally, determine the size and scope of the incident and respond accordingly, as defined by the entity's plan.

[1] https://www.nacdl.org/Landing/ComputerFraudandAbuseAct

Establish ongoing communication methods between the vendor and the entity. This may take the form of public notices published by the vendor. However communicated, vendor notifications about the incident should establish the method and frequency for additional information regarding the incident.

During the procurement process, establish a mutually agreed upon approach to submitting and receiving responses to specific questions from the vendor about incidents.

Design incident action plans in accordance with the type of incident, impact, and stage of detection to support the response plan. Incident action plans establish standard response measures based on the stage and potential impact of the affected system or service.

Be specific in reports and notifications to E-ISAC as to observations of the incident and attach information that the vendor has already released. Reporting specific observations and technical details supports the collecting analyst's ability to determine the full size and scope of all the reporting parties, allowing them to assess and share actionable intelligence.

After the incident, conduct a post mortem review with the vendor, focusing on the interaction, coordination, and communication that took place throughout the detection, notification, and response process. Identify security control improvements and establish target dates for implementation of the improvements. Update the Incident Response Plan as needed.

Security Control Improvement

After completing the vendor-identified incident investigation and determining its root cause, evaluate the associated security controls and improvements that were identified during the post mortem to help prevent future incidents. The vendor should provide documented evidence of the implemented changes.

Unfortunately, there is always the possibility that the vendor will fail to perform some or all of what was expected. In that case, possible actions include:

- Apply internal mitigating security controls to reduce the risk
- Document and communicate issues which were not addressed
  - Engage management and/or senior leadership of the vendor as needed, emphasizing the importance of the control(s) or mitigation(s) and the need to implement appropriate measures
  - Communicate to the vendor that unresolved issues may impact future scoring or evaluation of new purchases of products or services or renewal of existing product and service contracts
- Evaluate terminating the relationship with the vendor
- If appropriate, take legal action

Additional topics and guidance for Supply Chain Security can be found at the Supply Chain Risk Mitigation Program page.[2]

[2] https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx