NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Reliability Guideline

Cyber Intrusion Guide for System Operators

Preamble

It is in the public interest for the North American Electric Reliability Corporation (NERC) to develop guidelines that are useful for maintaining or enhancing the reliability of the Bulk Electric System (BES). Per their charters, the Technical Committees of NERC; the Operating Committee (OC), the Planning Committee (PC) and the Critical Infrastructure Protection Committee (CIPC) are authorized by the NERC Board of Trustees (Board) to develop Reliability (OC and PC) and Security (CIPC) Guidelines. Guidelines establish voluntary codes of practice for consideration and use by BES users, owners, and operators. These guidelines are developed by technical committees and include the collective experience, expertise and judgment of the industry. Reliability guidelines are not to be used to provide binding norms or create parameters by which compliance to standards is monitored or enforced. While the incorporation and use of guideline practices is strictly voluntary, the review, revision, and development of a program using these practices is highly encouraged to promote and achieve the highest levels of reliability for the BES.

This Cyber Intrusion Guide was created for electric System Operators, but the priciples within are applicable to any operators or support staff engaged in maintaining Reliable Operation of the BES.

Section 1: Background

The OC has tasked its Operating Reliability Subcommittee (ORS) to create a high level guideline to assist System Operators in detecting and responding to potential Cyber Security Incidents. The ORS recognizes not all organizations are the same, so this guidance is general and is based on the assumption that each entity has an approved Cyber Security Incident response and reporting process in place to follow any time a Cyber Security Incident has been identified, assessed, and confirmed.

The following guideline will assist System Operators in recognizing events that may be an indicator of a cyber-attack, and how and when to share information with others.

This document is intended to be used as a guide only. It is not intended to detract or conflict with an entity's Cyber Security Incident response plan. Rather, the guide should highlight the Plans to operators so that they can understand their role and what their company expects them to do. Developers of Cyber Security Incident response plans are encouraged to consider operators' perspective when creating their organization's plans.

As noted above, Reliability Guidelines are not to be used to provide binding norms or create parameters by which compliance to standards is monitored or enforced.

Section 2: Are we under attack? Recognizing an attack or an attempt to attack

System Operators are uniquely positioned to recognize cyber threats to the BES. Through direct access to Cyber Assets, and direct contact with field personnel, Operators may be the first to recognize real-time threats to system security. They may also be targets of social engineering attempts[1]. Operators are potentially the first and last line of defence to potential threats.

As threats to Cyber Assets are continually evolving, it is difficult to provide a comprehensive list of anomalies that may require a response. Rather, an operator's awareness and questioning attitude likely provide the greatest value. Real-time operating staff should be vigilant in asking themselves why their Cyber Assets are responding unusually. The System Operator should be asking their IT support to investigate any strange, unusual behavior, whenever it is detected. Similar to physical security concerns, operators should be encouraged to "say something when they see something." It is understood that increased vigilance may result in false positive reports. However, it is better to "play it safe" when Cyber Assets are behaving unusually.

Examples of anomalies that may require attention:

- Workstation unexpectedly locked out and/or receive a message indicates password has been changed
- Pointer or mouse cursor moving by itself
- Files / messages flashing / suspicious pop-ups appear on the screen
- New icons appear on desktop or in start menu
- System is unusually slow or unresponsive
  - Simultaneous loss of operational support systems (e.g., HVAC, Fire Suppression, phone/communications)
- Observing unusual system activity or alarms from Cyber Assets. For example:
  - Simultaneous loss of multiple components of the EMS/SCADA system
  - Multiple breaker operations during a non-storm event
  - Any unexplainable manual operations
  - Multiple perceived suspicious readings
  - Requests for information about the system (social engineering attempts)
  - Unexpected system shutdown or reboot
  - Complete loss of SCADA capabilities that support Real-time operations.

[1] For an overview of Social Engineering and Phishing attacks, please refer to US-CERT Security Tip.

- Erratic EMS/SCADA system equipment behaviour, messages/alarms, or degradation of performance, especially when more than one device exhibits the same behaviour
- Anti-malware application alerts on operator Human Machine Interface(s)
- Unexpected user account authentication lockouts or change in user privileges
- Calls from data partners (other Entities who see your data) to verify suspicious data being received via communication associations/exchange

Section 3: Initial Actions and Internal Notification Response

When unusual system behavior is observed, take any immediate steps outlined in your Cyber Security Incident response plan. As soon as possible, contact your cyber security team and follow their instructions. When describing issue, include details on the impact(s) of problem. This will help responders to follow best protocol to safe resolution, containment, and preservation of evidence. Depending on an entity's Cyber Security Incident response plan, this may require an operator to:

- Contact Energy Management System(EMS), Operational Technology (OT), Information Technology (IT), and cyber security personnel
- Notify the other operators on duty

Section 4: External Response

Once an attack attempt has been confirmed, follow the reporting instructions of your organization's Cyber Security Incident reponse plan (if available). This may involve:

- Notifying other control centers – adjacent, distribution via Reliability Coordinator Information System (RCIS), etc.
- Cyber Security Staff assuming responsibility for confidential communications related to Cyber event.
- Cyber Security Staff isolating certain equipment for containment, forensic analysis, evidence retention, and/or recovery.
- Law Enforcement Personnel taking control of an area or confiscating equipment. Reliable Operations should be maintained through a coordinated response between Law Enforcement, operations, and an entity's physical/cyber security teams.

Summary

Due to their unique role in operating the BES, System Operators may be the first to observe unusual behavior. To ensure that entities are able to respond effectively, it is important that Operators maintain a questioning attitude to assist in identifying something that requires further investigation. Further, electric operators should understand their important role in recognizing strange and unusual cyber security behavior and notifying the right people consistent with their incident response plan.