

Security Guidelines for the Electricity Sector: Control System Cyber Security Incident Response Planning

| | |
|------------------------------------|--|
| Effective Date: May 2, 2007 | Version: 1.0 |
| | Approved by Board of Trustees: May 2007 |

Preamble

This guideline addresses the potential risks that can impact some electricity sector organizations and provides practices that can help mitigate the risks. Each organization decides the risk it can accept and the practices it deems appropriate to manage its risk.

Introduction

The Control System Cyber Security Incident Response Planning Security Guideline provides the North American electricity sector organizations with actions they should consider when responding to cyber security incidents. The guideline is a framework for developing an incident response plan for internal use by the organization.

Purpose

The purpose of this guideline is to provide suggestions for creating and deploying an effective incident response plan for control systems. A well-formed incident response plan will help minimize possible impacts of cyber security incidents and assist in the identification, classification, response, and reporting of cyber security incidents related to critical cyber assets.

Applicability

This guideline is applicable to any entity that owns and/or manages control systems that support the bulk electric system.

A control system is as critical as its most critical component, and is as vulnerable as its most vulnerable component. In the case of a cyber security incident, timely detection, response and reporting of the incident are paramount to the continued production and protection of the bulk electric system. Each entity must define and outline their own cyber security incident response plan to effectively manage and mitigate the incidents when they occur. This guideline is intended to address cyber security incident response as outlined in CIP-008-1. Incident reporting is outlined by both the Electricity Sector Information Sharing and Analysis Center (ES ISAC) and the Department of Homeland Security's Indications, Analysis and Warnings program, and is not the focus of this particular guideline.

Background

The current threat environment and increased awareness of and vigilance against malicious activity has influenced how electricity sector organizations operate their facilities today. The increased awareness and the emergence of the NERC Critical Infrastructure Protection (CIP) standards have given rise to the need for formalized methods, teams, and protocols for managing cyber security incidents.

Control System Cyber Security Incident Response Guideline

Version 1.0: Effective May 2, 2007

Having an incident response plan does not guarantee the ability to eliminate damage from a cyber security incident. However, having a comprehensive incident response plan for managing and escalating countermeasures and the communication of those plans demonstrates the commitment of an entity to minimize the occurrence and potential impact of future malicious intrusions.

Definitions

This guideline addresses cyber security incidents as defined in the NERC glossary.

Cyber security incident response team

A group of subject matter experts established within an entity for the purpose of assisting in response to computer security-related incidents; also called a computer incident response team (CIRT) or a computer incident response center (CIRC) (or computer incident response capability).

Guideline Statement

To be successful, a sound incident response plan includes several fundamental features that include:

- Sound planning
 - Team members
 - Communication paths
 - Response times
- Clear escalation of responsibility and communication
- Thoroughly defined team
- Detailed response timelines and guidelines

Guideline Detail

Before an entity starts to develop its incident response plan; the entity should make certain decisions about how to manage the incidents. The plan should consider the merits of immediate response by blockage of a detected intruder as well as a delayed response that allows tracking the intruder access up to a certain point. The delayed response view purports to allow an entity time to assess the intruder's entrance strategy, tactics and possible installations, scope of attack, and how to utilize the current incident for future prevention. Entities must weigh the pros and cons of both options when first embarking on the development of an incident response plan and delineating decisions. However, the entity must recognize that the actions put forth in the second view exposes the critical cyber systems to prolonged risk during the monitoring and assessment activity.

Control System Cyber Security Incident Response Guideline Version 1.0: Effective May 2, 2007

For example, a 30-minute time frame from detection to correction may be too short or too long depending on the size and complexity of your organization and of the skill set and timely communication of your incident response team. An entity must also establish at the beginning of this plan a clear and concise order of action and communication as well as leadership for decision making during an incident so that there is no potential confusion during an incident.

Additional decisions and discussions will need to address the tradeoff between rapid system restoration and collection of evidence required for law enforcement proceedings (e.g., by chain of custody and quality of collection processes, tools, and proper documentation).

Other planning decisions that need to be made in developing an incident response plan include the proposed skill set of your response team or Cyber Security Incident Response Team (CSIRT). For a full discussion of recommended technical and interpersonal communication skills, refer to the U.S Computer Emergency Readiness Team (CERT) website (see Related Documents section). It is recommended an electricity sector organization also staff its response teams with individuals that possess the following skills:

- a. Power Systems Operations
- b. Control Room/Dispatching
- c. Generation and Substation operations, engineering, and maintenance

An electricity sector organization may also wish to establish a cyber security incident support relationship with their vendors to provide system-specific expertise to the CSIRT.

A well-balanced cyber security incident response plan itself will include a number of functions, including preparation, response, and follow up, which are discussed below.

Preparation

Preparation requires entities to develop definitions, determine and delegate responsibilities, and train and test the CSIRT.

Definitions

Definitions of what constitutes a reportable cyber security incident are required to distinguish between cyber security incidents that can be dealt with internally and those that must be reported to the appropriate authority as required by R1.1 of the CIP-008-1 standard. It is recommended that electricity sector organizations develop the definitions in tandem with a checklist of conditions consistent with CIP-008-1 requirements. Characteristics of a reportable incident should be consistent with those defined in CIP-008-1 and the Reporting Procedures Guideline.

Control System Cyber Security Incident Response Guideline

Version 1.0: Effective May 2, 2007

Delegation

As part of its response plan, entities should consider determining and delegating the roles and responsibility that will be instituted in the event of a cyber security incident (CIP-008-1, R 1.2) prior to the occurrence of an incident. Issues to be addressed should include: technical knowledge and experience of the operations staff to deal with a cyber security incident, and the person responsible for initiating response when an incident occurs.

Training and Exercises

The creation of a CSIRT is the recommended practice and will address most issues. A CSIRT with a greater knowledge of the systems and the training to effectively mitigate most threats can respond quickly and efficiently to incidents.

The primary responsibility of a CSIRT is to manage the response to a cyber security incident. This includes forming lines of communication and organizing resources to best deal with the cyber security incident. The CSIRT should also maintain the cyber security plan as well as review and test it annually (as required by R.4, R.5, and R.6 of CIP-008-1).

Those with the requisite knowledge of the systems and its connectivity should be part of the response team. Once the CSIRT team is established, a member of the response team should either be on shift or on call at all times.

As noted earlier, the Incident Response Plan should be tested at least annually. (See CIP-008-1 language.) Testing involves defining scenarios and assembling the incident response team to step through the scenarios and record how the team members would respond. The key to a successful test is the adequacy of the scenarios and the test objectives, as well as a comprehensive exploration of the issues and documentation of appropriate responses.

Scenarios

There are two primary dimensions to the scenarios that should be developed: threat and technical impact.

The possible threats to the environment should be described. Threats include, but are not limited to, virus/worm, sabotage, and intrusion. The possible technical impacts should also be listed that include the compromise of a single demilitarized zone device, the compromise of a single interior device, and widespread compromise of the control system environment that impacts business functionality. Scenarios should be developed for all possible intersections of the two lists.

Test Objectives

The test objectives should be determined and documented prior to the start of the test. While each company's objectives will be different, a list for consideration includes:

- The first responders must be pre-authorized for specific actions that must be taken, and must equally be clearly informed of forbidden actions.
- It must be clear who is authorized to take specific actions, such as escalating the incident, turning off devices, disconnecting the network, contacting management, etc.
- Backups must be adequate and available for all scenarios. For example, age of backups, location of backups, ability to detect malicious code in backups, ability to determine the integrity of backups, etc., should be included in the plan.
- The team members must have all the skills necessary to respond to all scenarios identified. Team members should have immediate access to any additional external resources.

Response

Once an event is detected through monitoring and is identified as a possible cyber security incident, the event will be evaluated by the designated personnel, whether a CSIRT member or otherwise.

The following represents a sequence of events an entity can use to respond to a cyber security incident:

1. Analyze the Incident

If the event meets any of the criteria outlined in the definition stage of your program setup, then the CSIRT team should be involved and begin to analyze the incident. If there are multiple symptoms or potential causes/sources, then the events need to be "triaged" or ranked by critical importance regarding escalation and remediation. The National Institute of Standards and Technology special publication SP800-61 contains guidance on how to triage multiple-event scenarios.

2. Respond to the Incident

Regardless of the method chosen to respond to incidents (i.e., rapid restoration or collection of evidence), at this stage an effective Incident Response Plan should endeavor to:

- a. Ensure no further damage can/will be done
- b. Contain and compartmentalize existing problem/intrusion
- c. Keep records of actions taken to aid in learning, reporting, and prosecuting
- d. Save and archive logs from impacted systems, IDSs (Intrusion Detection System) and firewalls

3. Escalate as Appropriate

If after initial implementation of the solution the incident is not contained, a pre-determined escalation plan should be invoked to augment the people and resources used to combat the issue. This escalation plan, or authority to enable escalation, should be decided upon prior to active handling of incidents.

4. Communicate

When the analysis phase determines that there is a reportable incident, then the communication channels must be opened. However, depending on the level of severity of the incident, different communication paths and plans may be appropriate for different situations. Further communication as the situation develops may be necessary, and in any case a summary report once the cyber security incident is resolved should be provided to all individuals at all levels involved in the escalation. Communication outside of the CSIRT group could include representatives of departments such as: legal, Human Resources, Marketing, Public Relations, Business Managers, existing security groups, such as physical security, audit or risk management departments, IT and any other employees or team members affected by the cyber security incident or its investigation. Clearly pre-determine who is authorized to release information about the incident to external entities.

5. Resolve the Incident

Resolve the threat agent and negate the vulnerability. At this point a post-cyber security incident report should be developed. The report itself should include information, such as:

- Incidence reference number
- Report author and contact information
- Summary of systems or assets involved
- Description of activity
- Supporting documentation or logs of activity
- Description of resolution
- Lessons learned

Documentation of the cyber security incident that can be reported will be kept for three calendar years as required by R2 of CIP-008-1. Contents of the report should include:

- How the cyber security incident was contained
- The cause and source of the compromise
- Elapsed time from compromise to detection
- Elapsed time from detection to containment of the threat
- Costs associated with the cyber security incident
- How much (if any) down time was caused

Control System Cyber Security Incident Response Guideline Version 1.0: Effective May 2, 2007

- How future similar cyber security incidents will be prevented
- Team members involved in remediation of the cyber security incident
- Policies that will be revised as a result of the incident resolution

6. Monitor for Possible Future Occurrences

After incident resolution is complete, and operations has returned to normal, the entity should continue monitoring the system at a higher level for a period of time, to insure no residual effects remain in the system, and that the corrective actions to not introduce any unintended consequences.

Follow up

Disclosure

Section R1.3 of CIP-008-1 requires that the responsible entity have a process for disclosing reportable cyber security incidents to the ES ISAC. This process should include:

- Contact information for the ES ISAC
- A designated person or persons responsible for reporting, and who will serve as the contact for the duration
- A document outlining all information that should be given to the ES ISAC and to law enforcement (e.g., local, state/provincial, FBI/RCMP)

Exceptions

None

Related Documents

Suggested CSIRT Team Skills:

<http://www.cert.org/csirts/csirt-staffing.html>

ES ISAC Reporting:

http://www.esisac.com/publicdocs/Guides/secguide_ThrIncReporting_final.pdf

Indications, Analysis and Warnings Program:

<http://www.esisac.com/IAW.htm>

DOE 417 Form and instructions:

<http://www.eia.doe.gov/oss/forms.html#OE-417>

NIST SP800-61

<http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>

Control System Cyber Security Incident Response Guideline
Version 1.0: Effective May 2, 2007

NERC Cyber Security Standards

http://www.nerc.com/~filez/standards/Reliability_Standards.html#Critical_Infrastructure_Protection

Revision History

| Date | Version Number | Reason/Comments |
|-------------|-----------------------|------------------------|
| 3/22/07 | Version 1.0 | Approved by CIPC |