Homeland Security

NCCIC
National Cybersecurity and
Communications Integration Center

PREPARING FOR CYBER INCIDENT ANALYSIS

ICS-CERT

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provides guidance to critical infrastructure asset owners to assist in preparing their networks to handle and analyze a cyber incident.

Even the best cyber defense mechanisms cannot prevent all cyber incidents. The sheer volume of intrusions attempted against information technology systems every day creates the possibility that a cyber attack could penetrate the numerous defensive systems in place on many networks. In order to provide the swiftest incident response and recovery possible, preparation and planning are essential.

ESTABLISH SYSTEMS ANALYSIS CAPABILITY

The ability to identify the source of an incident and analyze the extent of the compromise is necessary to rapidly detect issues, minimize loss, mitigate exploited vulnerabilities, and restore computing services. Two comprehensive resources for developing an incident response capability are:

- Developing an Industrial Control Systems Cybersecurity Incident Response Capability, 2009
- Computer Security Incident Handling Guide, 2012

OPERATIONAL PREPARATION

Cyber incidents are tense, complicated, and not often part of routine operations. When properly maintained, operational preparedness measures can ensure the availability of information necessary to recover from an incident quickly while minimizing the impact.

A dedicated incident handling team should be led by a senior technical staff member who has the authority to make key decisions in a timely manner. In addition to the lead and forensics analysts, the team should have stakeholders from the following groups: Corporate IT (both network and host management), Control Systems Subject Matter Experts, Public Relations, Legal Counsel, Law Enforcement (if necessary).

The team should be trained in proper incident handling techniques and should practice using the tools to establish and maintain proficiency. Operating procedures should be developed to include:

- Identification of objectives and goals of response
- Internal and external communications policy
- Meeting and briefing schedules
- Reporting to all required regulatory agencies.

An overall incident preparedness checklist should be created and reviewed annually using a ‘table-top’ exercise. Documentation should be accessible to operations personnel to help facilitate analysis of the incident and identify priorities for recovery. At a minimum, documentation should include:

- An up-to-date network map to include IP ranges, hostnames, OS versions, and roles for servers, ingress and egress points between sub-networks, and wireless access points and modems
- Firewall and IPS rule sets
- Contact lists and escalation points for Internet Service Providers (ISPs), Computer Emergency Response Teams (CERTs), and service, software and hardware providers.

An incident response information gathering checklist should also be created. This checklist should identify the types of information that should be collected to aid analysis by external CERTs or partners. Examples of critical information may include:

- Affected IPs
- Method of detection
- Type of activity that has occurred or is occurring
- What processes are affected
- Timeline information; how long has the activity been going on and when it was detected
- Type of assistance needed
- Potential operational impact
- Points of contact.

It is important to establish an “out-of-band” communications policy. Any communications regarding an incident or potential incident should not go through the standard communication channels, e.g. corporate email, VoIP systems, as these may already be compromised and will tip off the adversary that you are aware of their presence in your network. In addition, any files relating to the incident or your handling policy should be stored off of the network under the control of the incident response team.

IMPORTANCE OF LOGGING

System and network device logs are essential to incident investigators. The types of logging that should be considered include Firewall, Proxy, DNS, DHCP, web app, A/V, IDS/ IPS and host and application logs. Additional logging to be considered is flow data from routers, switches, and packet captures.

Log integrity is essential during an incident investigation; therefore, logs should be continuously stored on a separate system, frequently backed-up, and cryptographically hashed to allow detection of log alterations.

PRESERVING FORENSIC DATA

Other critical components of incident response are forensic data collection, analysis, and reporting. These elements are essential to preserving important evidence. To avoid the loss of essential forensic data:

1. Keep detailed notes of why the forensic actions are needed, what is observed (including dates/times) mitigation steps taken/not taken, device logging enabled/disabled, and machine names for suspected compromised equipment. More information is generally better than less information.
2. Capture forensic images of the system memory before doing anything else to the system. Avoid running any antivirus software “after the fact” as the AV scan changes critical file dates and impedes discovery and analysis of suspected malicious files and timelines.
3. Avoid making any changes to the operating system or hardware, including updates and patches, as they will overwrite important information about the suspected malware.

Organizations should consult with trained forensic investigators for advice and assistance prior to implementing any recovery or forensic efforts. In addition, ICS-CERT subject matter experts are available to aid in incident response activities. Affected entities should not hesitate to contact ICS-CERT for assistance. Control system environments have special needs that should be evaluated when establishing a cyber forensic plan. The ICS-CERT recommends the following source on control system forensics:

Recommended Practice: Creating Cyber Forensics Plans for Control Systems, 2008

About ICS-CERT

ICS-CERT works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors.

https://ics-cert.us-cert.gov

About NCCIC

The National Cybersecurity and Communications Integration Center (NCCIC) is a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement.

http://www.dhs.gov/national-cybersecurity-communications-integration-center