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
www.us-cert.gov/control_systems/csdocuments.html

Computer Security Incident Handling Guide, 2008
http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

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 regularly. Documentation should be accessible to operations personnel to help facilitate analysis of the incident and indentify priorities for recovery. At a minimum, documentation should include:

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

Homeland Security

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 occurred
- Whether activity is continuing
- Timeline information
- Evidence of compromise
- Type of assistance needed
- Potential operational impact
- Impact to control systems
- 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 or at the very least protected using strong encryption and proper key management.

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.

During an incident investigation, network administrators should be able to identify which internal hosts have communicated with which IP addresses and what type of traffic was generated. DNS queries, proxy activity, and unusual network activity (such as port scanning) are also important data that may be required during an incident investigation. Packet captures may help identify any data that was exfiltrated. System auditing features, log retention durations, and time synchronization should be managed properly.

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:

- Keep detailed notes of 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.
- When possible, capture live system data (i.e., current network connections and open processes) prior to disconnecting a compromised machine from the network.
- Capture forensic images of the system memory and hard drive prior to powering down 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.
- 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. Additionally, 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, Department of Homeland Security, 2008
www.uscert.gov/control_systems/pdf/Forensics_RP.pdf

ABOUT CSSP

DHS created the National Cyber Security Division's CSSP to reduce industrial control system risks within and across all critical infrastructure and key resource sectors.

For more information, visit www.us-cert.gov/control_systems.