Homeland Security

Incident Handling

Preparing for Incident Analysis

You have the best firewalls configured and managed by a well-trained staff. You have the most recent antivirus systems watching email, workstations, and servers. You have managed web proxies configured with good policies. You have a solid network architecture designed from the ground up with security in mind and with an excellent user education program in place - and you still get hacked. Even with the best cyber defense mechanisms in place, cyber incidents will likely occur. Are you prepared to properly identify what went wrong and how to recover? A little planning and preparation now will be invaluable if and when your systems are compromised.

ICS-CERT

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provides guidance to critical infrastructure asset owners on how to prepare your network to handle and analyze a cyber incident. The following paragraphs outline recommended practices for developing incident response capabilities necessary to collect data and perform follow-on actions to restore your systems to normal operations.

Establish Systems Analysis Capability

Not all cyber incidents can be prevented; therefore, the ability to identify the source and analyze the extent of the compromise is necessary for rapidly detecting incidents, minimizing loss, mitigating the weaknesses that were exploited, and restoring computing services. Two comprehensive resources for developing an incident response capability are:

1) *Developing an Industrial Control Systems Cybersecurity Incident Response Capability, 2009*
http://www.us-cert.gov/control_systems/csdocuments.html

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

Operational Preparation

Operational preparedness measures should be maintained to ensure availability of adequate data to recover from an incident. In particular, an overall incident preparedness checklist should be created and reviewed regularly. Contact lists and escalation points should also be maintained, printed, and stored to include ISPs, CERTs, service/software/hardware providers, internal team leads, etc. System 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:

- IP ranges and hostnames
- DNS information
- Software and Operating System names, versions, and patch levels, etc.
- User and computer roles
- Ingress and Egress points between networks.

An incident response information gathering “checklist” should also be created to make sure the type of information which might aid external CERTs or partners is gathered as soon as possible. The checklist should include information such as:

- Affected IPs
- Method of detection
- Type of incident
- Type of assistance needed
- Potential operational impact
- Points of contact.

Homeland Security

Incident Handling
Preparing for Incident Analysis

Importance of Logging

System and network device logs are essential to incident investigators. The following types of logging should be considered:

- Firewall logs
- Proxy logs
- DNS logs
- IDS logs
- Flow data from routers and switches
- Packet captures
- Host and Application logs.

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 in an incident investigation. System auditing features, log retention durations, and time synchronization should be properly managed.

Log integrity is essential in 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, the following activities should be conducted:

- 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 machine from the network you suspect is compromised.
- 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.

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

http://www.uscert.gov/control_systems/pdf/Forensics_RP.pdf

Contact the ICS-CERT

To learn more about control systems-related cyber vulnerabilities, training, standards, and references, visit: http://www.ics-cert.org

CSSP and ICS-CERT encourage you to report suspicious cyber activity, incidents, and vulnerabilities affecting critical infrastructure control systems.

ICS-CERT Watch Floor: 1-877-776-7585

E-mail: ics-cert@dhs.gov