Establishing Incident Handling Procedures

By Karen Russo

SANS Security Essentials GSEC Practical Assignment Version 1.2f

INTRODUCTION

Computer systems and the information they store are valuable resources that need to be protected. Computer threats are on the rise and are becoming much more complex. Threats including system and network intruders, computer viruses, and network worms can exploit a variety of weaknesses in computer systems and cause significant damage.

Establishing incident handling policies and procedures will ensure thorough and comprehensive documentation for the appropriate personnel and possibly the authorities. It will provide a plan of action in a panicked situation, which can aid in minimizing the potential damage.

The procedures established should provide thorough guidelines on what to do if a security incident is discovered. An incident can be any irregular or adverse event that occurs on any part of the organization, which can include, but is not limited to, a virus or worm, the compromise or disclosure of sensitive information, and denial of service. There are many different types of incidents, and it would be helpful for procedures to be written for each specific type, which may include, but not be limited to, malicious code attacks, probes and network mapping, denial of service, espionage, hoaxes and system and network intruders. In addition, the procedures should comprise of role responsibilities, who to contact and when to contact someone.

Define the reporting and escalation hierarchy. Select a central point of contact such as the Information Security Officer. There should be several authorized contacts assigned with different areas of expertise as necessary, but a central point of contact should be identified for notification of the incident. In addition, the central contact will be the coordinator of the overall assignment of tasks and the response process. The central contact will assign authorization to enforce any actions required. Describe a primary and alternate means for contacting each member in the notification tree. List telephone, FAX, and E-mail information for each member of the tree. Also include in the procedures reasonable timeframes for responding to the incident depending on the level of the incident. If the first person on the call list to be notified cannot respond within a reasonable timeframe, then the second person must be called in addition to the first. It will be the responsibility of the people on the notification tree to determine if they can respond within an acceptable timeframe.

The organization may at some point also have the responsibility to inform other sites about an incident, which may affect them. It is important to have control over the information and notification so it does not get into the wrong hands. Assigned personnel such as the central contact should authorize the release of any information. Any information released must be explicit and factual.

Documentation of information is critical in situations that may eventually involve federal authorities and the possibility of a criminal trial. The implications from each security incident are not always known at the beginning of, or even during, the course of an incident. Therefore, documentation must be maintained and secured for all security incidents that are under investigation. Include as much information in the documentation as possible, such as vulnerability, dates and times of discovery of the incident and phone calls or conversations regarding the incident, required actions, contact information, systems affected, and date system was cleaned.

Establish backup procedures for every system. Having backups eliminates much of the threat of even a severe incident, since backups preclude serious data loss.

Finally, all employees must be made aware of the policy and procedures, and a test of the procedures should be performed for adjustments or enhancements. The testing of the procedures will also provide the essential training for increased skills and efficiency.

The steps included in handling a security are to identify the problem, provide protection/containment from the problem, eliminate the problem, recover from the incident and perform a follow-up analysis. These steps are outlined in more detail below in this document.

INCIDENT HANDLING STEPS

Identify The Problem

The team of experts will perform an initial investigation to determine if there was truly an incident and they will assess the severity of it.

If it is clear that an incident has occurred, create an image backup of the affected hard drives. An image backup will contain information that is not accessible from file systems, such as deleted files. Unix includes the dump device (dd) command, and commercial products are available for Windows NT and 2000, which will make image backups.

If an image backup is not feasible, check for suspicious activity in audit trails and logs, network traces, any change dates on files and directories, changes to startup files or the registry, new users or groups or members added to groups. Usually the Windows system and security log files can be found in the \winnt\system32\config directory and in the /usr/adm directory for Unix.

Examples in researching suspicious activity specific to Unix and Windows NT are outlined below:

UNIX:

- System crashes
- New user accounts, or high activity on an account that has had no activity previously.
- New files with strange file names.

- Last log files (usually wtmp and wtmpx viewed by the last command): These logs record all login connections including the originating address. Check the originating address and user combinations for users that should not be accessing your system. Maintain a list of known hacker addresses. Pay close attention to the originating address listed for each user connection. If the originating address does not fall within your IP range, check with the user. If the user cannot account for the address, or activity related to that IP address, you may have identified a compromised account. You should check that user's directories for any malicious files that may have been left by a hacker. Look for "hidden" directories such as "...", "._", ".tcsh", etc.
- Sulog: This log records every time the "su" command was used and by whom. Usually the "su" is from a user to root, but you may also see an "su" from one user to another. Check to see if users that shouldn't be switching to root have been successful in getting super user privileges.
- System logs: Various logs files (depending on the operating system) including syslog (or SYSLOG), messages, mailinfo, and warnings. Look for any wrapper messages (if TCP wrappers has been installed) that indicate login attempts from unknown sources. Look in FTP logs if FTP logging has been activated. Look for messages that may indicate a segmentation fault (this could indicate that a buffer overflow exploit may have occurred).
- Web server logs: If you think you have been compromised by a vulnerability, look for occurrences of "/etc/passwd" in your web server access log file. If you find any, check (usually) the first three digit number after "/etc/passwd". If it is "200", the exploit was successful and the password file has been displayed in the hacker's web browser.
- Sniffer Logs: If you find sniffer files (e.g., 198.17.244.10.1076-168.143.0.187.23, tcp.log, etc.), send them to your Information Security Officer for analysis.

<u>NT:</u>

- System crashes
- New user accounts, or high activity on an account that has had no activity previously.
- Event Viewer - contains system logs, security logs, and application logs. The event viewer can be found by going to Programs, Administrative Tools, then Event Viewer.
- Suspicious Files: look for recently created *.dll, *.exe, and *.drv files and verify that they should have been created/updated.
- Web server logs: Review connections to RDS, FrontPage, ColdFusion, and iissample files. Confirm that the connecting hosts are legitimate.

Viruses and worms have the potential to spread quickly so early identification is critical. Virus software should always be kept up to date and configured to scan files in real-time with periodic complete system scans.

With a system compromise, an intruder will break into the computer (remotely or physically), and have complete control over it and potentially any other computer on the network. Implementation of firewalls will assist in the prevention of unauthorized access to a computer or network and can be configured with real-time alerts.

Once the initial analysis is complete, it is time to review the steps taken and plan the additional steps necessary.

*** Document all actions.**

Protection/Containment From The Problem

After the initial analysis is complete, you must protect the system by physically disconnecting from the network and shutting down the operation system to minimize the effects of the attack and to allow for the examination of the system. (Although in some instances it may be worthwhile to risk having some damage to a system that is not sensitive or classified by keeping the system online, which allows you to identify the intruder.) Notify all employees to change their passwords immediately.

Specific containment strategies should be developed for each type of incident, but the objective should be to provide a reasonable security solution until sufficient information has been gathered to take more appropriate actions to address the vulnerabilities exploited during the incident.

*** Document all actions.**

Eliminate the problem

A decision for the best course of action to take must be made. Anti-virus software usually has a boot disk or a "rescue disk" that allows you to boot and clean the system. If the virus software will not clean the system, it must be completely reformatted and rebuilt.

There should be a process in place to evaluate fixes or patches identified to secure the system prior to implementation. It would also be helpful to test the patches to confirm the fix or patch had the desired effect on securing the system. If the testing indicates that the fix or patch is not securing the system from the known attack, notify the source of the patch or fix.

*** Document all actions.**

Recover From The Incident

The objective in recovering from the incident is to return the systems to normal. If you choose to restore files to their original state by running anti-virus software, they should be compared to a backup copy to determine if any damage was done. The quickest and cleanest recovery from a system compromise would be to reformat and reinstall the operating system.

In the case of a network-based attack, it is important to install patches for any operating system vulnerability that was exploited. Before restoring connectivity, be sure to verify that all affected areas have successfully eliminated the problem and cleaned their systems, and then notify all involved that the systems will be put back online.

*** Document all actions.**

Follow Up Analysis

After an incident has been fully handled and all systems are restored to a normal mode of operation, a follow-up analysis should be performed as soon as possible. The follow-up stage is one of the most important stages for handling a security incident. All involved parties should meet and discuss actions that were taken and the lessons learned. Determine how well those involved performed. All existing procedures should be evaluated and modified, if necessary. If applicable, a set of recommendations should be presented to the appropriate management levels to make changes to the environment to avoid future attacks.

A security incident report should be written and distributed to all appropriate personnel. The report can provide a reference to be used in case of other similar incidents. It is also important to obtain a monetary estimate of the amount of damage the incident caused in terms of any loss of software and files, hardware damage, and manpower costs to restore altered files, reconfigure affected systems, and so forth. This estimate may become the basis for subsequent prosecution activity by federal authorities.

CONCLUSION

Too often little attention is given to the preparation of handling attacks. Not having policies and procedures can result in risk to human life, inadequate security of the confidential information, rushed decision-making, difficulty in collecting evidence, and delays in recovering the systems.

Also, many organizations spend more time reacting to recurring incidents, which results in lost productivity. Develop safeguards like firewalls and good computer security practices to prevent people from even trying to cause harm to your systems. Being proactive and able to quickly detect and handle the incident by using trained experts is what organizations need.

RESOURCES:

Kwok, Eddie C.S. "A Matrix Checklist Model For Cooperative Incident Handling."
http://wwwtools.cityu.edu.hk/ct1995/kwok.htm

Farrow, Rik. "Incident Handling. A Little Planning Goes a Long Way When Handling Computer Breakins" January 1, 2000.
http://www.networkmagazine.com/article/NMG20000515S0109/2

Bull, Jon. "An Introduction to Incident Response and Handling in a Microsoft Environment: A Primer for the Unprepared Administrator." March 2001
http://www.labmice.net/articles/incident_response.htm

Center for Information Technology. "Incident Handling Guidelines."
http://irm.cit.nih.gov/security/ih_guidelines.html

Arizona State University. "ASU Incident Handling."
http://www.asu.edu/it/ac/uncel/documents/incident.htm