

An Introduction to Incident Handling

Chad Cook 2000-11-29

An Introduction to Incident Handling

by *Chad Cook* (*ccook@illusive.org*)

last updated Nov. 29, 2000

Incident handling is a generalized term that refers to the response by a person or organization to an attack. An organized and careful reaction to an incident can mean the difference between complete recovery and total disaster. This paper will provide a logical approach to handling two common forms of attack - virus outbreak and system compromise. The method that this article will propose includes the following sequence of steps that should be followed in the case of all types of attack.

1) Preparation

Comprehensively addressing the issue of security includes methods to prevent attack as well as how to respond to a successful one. In order to minimize the potential damage from an attack, some level of preparation is needed. These practices include backup copies of all key data on a regular basis, monitoring and updating software on a regular basis, and creating and implementing a documented security policy. Regularly-scheduled backups minimize the potential loss of data should an attack occur. Monitoring vendors' and security web sites and mailing lists is a good way to keep up to date with the state of the software and patches. It is necessary to update software in order to patch vulnerabilities that are discovered. It is also vital to update anti-virus software in order to keep system protection up-to-date. A documented security policy that outlines the responses to incidents will prove helpful in the event of an attack, as a reliable set of instructions.

2) Identification of Attack

While preparation is vital for minimizing the effects of an attack, the first post-attack step in Incident handling is the identification of an incident. Identification of an incident becomes more difficult as the complexity of the attack grows. One needs to identify several characteristics of an attack before it can be properly contained: the fact that an attack is occurring, its effects on local and remote networks and systems and from where it originates.

3) Containment of Attack

Once an attack has been identified, steps must be taken to minimize the effects of the attack. Containment allows the user or administrator to protect other systems and networks from the attack and limit damage. The response phase details the methods used to stop the attack or virus outbreak. Once the attack has been contained, the final phases are recovery and analysis.

4) Recovery and Analysis

The recovery phase allows users to assess what damage has been incurred, what information has been lost and what the post-attack status of the system is. Once the user can be assured that the attack has been contained, it is helpful to conduct an analysis of the attack. Why did it happen? Was it handled promptly and properly? Could it have been handled better? The analysis phase allows the users and administrators to determine the reason the attack succeeded and the best course of action to protect against future attacks.

Incident Handling - Viruses

Preparation

Viruses can cause irreparable harm to important files and records. The home and small office user is at even higher risk than larger organizations because the user often works with one computer or stores important information in a single location. Unlike larger organizations that have data spread across many systems in several locations, a virus outbreak in a home or small office could permanently destroy important data. This puts greater emphasis on the need for creating backups of all information. Additionally, backup disks should be kept in a separate location, away from the computer. This ensures that in case of an incident such as fire or theft of hardware that a backup copy of all information is still available.

The second crucial step in preparing for an attack is to install anti-virus software. Anti-virus software is readily available, easy to install and operate and is affordable. New viruses are created frequently, so it is important to be diligent with anti-virus software maintenance. Almost all anti-virus vendors make updates available on their websites. Users should update their anti-virus software on a regular basis.

Identification of Virus Attack

Viruses are particularly potent and frightening because of their ability to spread quickly to 'friendly' computers. Just think of the public relations nightmare your company could endure if you're the address book in your e-mail program was used to spread a virus to all your suppliers' and your customers' computers.

Early identification of an incident is crucial to ensuring that the virus does not spread to other computers. It is crucial that users are familiar with the symptoms of a virus attack, such as mass e-mailing, file destruction or other malevolent actions the results of which can be seen immediately. Stealthy viruses require a bit more attention. The user should be aware that periodic anomalous behavior on a system is not always an indicator of a virus attack. Other factors may cause the erratic behaviour; however, for the sake of security, the user should scan the computer comprehensively to clearly identify the cause. Configuring the anti-virus software to do real-time scanning of files and to periodically do complete system scans helps to both prevent and identify viruses.

Containment

Containment of the virus is pivotal in limiting the effects. Many viruses spread themselves automatically. If a non-replicating virus infects a single computer, containing the virus is fairly straightforward. The administrator, or user, should disconnect network access including shared directories and other components that may allow the virus to infect files and programs on other machines. Anti-virus software often has a "rescue" component that allows an administrator to scan and clean a system by booting from a specialized floppy disk or CDROM. If available, these tools should be utilized to disinfect the system.

Should the anti-virus software fail to clean the system or lack the features necessary to do the cleansing, it is advisable to try other software packages that may provide more comprehensive coverage. If the system has been altered beyond repair, the last resort is to clear the system entirely and reinstall the operating system and software. If reinstalling, care should be taken to use software that is known to be uninfected and to completely reformat the hard drive to assure the eradication of the virus.

Recovery and Analysis

Viruses cause varying degrees of destruction- some exist merely to replicate; others attach to and destroy files and programs. Anti-virus programs can generally restore files to their original

state, but there are exceptions. If there is doubt to the reliability of the data held within a file, the user should compare the damaged file to a backup copy in order to assess whether or not damage has been sustained.

Once the system or systems have been returned to full operation, analysis should be done to determine where the defenses failed. Does fault lie in the anti-virus software, or the frequency and reliability of updates? Or did some user behaviour - such as opening files from an unknown or untrusted source - allow the system to become infected? Once the attack was identified, were appropriate and sufficient steps taken to minimize the damage that the system sustained? Analysis of the incident allows the user to learn from the unfortunate incident and ensure that it does not happen again.

System Compromise

Preparation

System compromise is an attack in which an intruder breaks into a computer and, either sitting directly in front of it or from a remote network, is able to use that computer. The attacker typically has total access to a system and all information contained therein including files, applications and potentially any other system connected to it.

Managing system compromise is more daunting than managing virus outbreaks. The basic steps to help prepare in case of system compromise are basically the same as are used in preparation for virus outbreaks. All vital information should be backed up on a regular basis. Software updates are also crucial. System compromise often arises due to security vulnerabilities in common software, particularly in operating system software. Users and administrators should be sure to maintain current software patches in order to protect against attacks. Patches are available through vendors' websites. Users can learn about the latest patches by monitoring vendors' web sites, mailing lists and user forums related to the software and to security.

In order to prevent against unauthorized intrusion into a system, users should implement firewalls. Just as anti-virus software is the cornerstone of a virus prevention strategy, firewalls are extremely important in preventing unauthorized individuals from accessing network services and resources. Like anti-virus software, firewalls are relatively affordable and easy to use - they not only protect against intrusion, but some can be configured to notify the user if an intrusion

is being attempted.

Identification

Systems compromise attacks are often indicated by missing or modified files, changes to the system configuration and services, greater memory and disk usage and unidentified network connections. Attackers will often seek to hide any indication of the intrusion by replacing files and programs with versions that protect the attacker. Programs that act normally on one occasion and strangely the next, as well as files and programs that have their time, date or size information modified may be indicative of an unauthorized intrusion. Comparison against backup copies may reveal changes to files.

Users and systems administrators can identify potential systems compromise attacks by monitoring network traffic and processes. The new wave of Intrusion Detection Systems (IDS) is extremely helpful in allowing for the monitoring of systems. By actively monitoring the network for known signs of attack and other anomalous conditions, an IDS notifies users as soon as it detects the event. IDS are useful in complex networked environments and where minimal technical staffing is available. By automatically monitoring and notifying users, an IDS can offload some responsibility from an overburdened administrator, making them invaluable resources for users and administrators in small offices and home offices.

Containment

Containment of an intrusion involves some effort on the part of the administrator. First, the administrator should freeze the current system as soon as an intrusion is suspected. This includes disconnecting the system from the network, stopping the operating system and disallowing anyone to use the system. As an operating system runs and people use the system files are naturally modified and updated depending on what they are doing. This normal functionality often erases important information that can be used to detect and trace an intrusion, therefore it is very important to stop the system as soon as possible after an attack is discovered. If possible, it is advisable to duplicate the hard disk of the system. This allows the administrator to begin the cleanup process on one disk and to give the other to an expert to determine the exact source and cause of the intrusion.

Recovery and Analysis

The most devastating but least-effort method of cleaning up a compromised system is to wipe the hard disk clean and re-install the operating system and software allowing a faster return to normal operation. A more painstaking approach is to compare each individual file and program against a copy known to be original in order to determine if any modifications have been made. It is important to do a minimal level of analysis in order to determine the cause of the intrusion. Once a cause is determined, changes to the environment should be made to avoid future attacks by that method. This includes updating affected software, access control methods that allow only certain users, systems and networks to use the services, firewalls and intrusion detection systems. A combination of these changes can provide a safer and more secure working environment.

Analysis of the attack provides several benefits. The user and administrator can determine the shortcomings in existing security policies, installation methods and configurations that allow attacks to succeed. Users and administrators should periodically review existing installations, configurations and security policies. New attacks and security vulnerabilities are found often and updating the existing environment can minimize the threats of future attack.

Conclusion

This paper provides a short overview and several guidelines to handle incidents with regards to three of the most common attacks - viruses, system compromise and denial of service. There are several general philosophies that foster security-minded thought and analysis. Forethought towards installation, configuration and the associated usage policies is important to the security of an organization. Rational and logical reactions to unnerving incidents help minimize the potential damage of attacks. Preparations such as backups, regular software updates and monitoring help an organization better deal with an incident and return to normal functionality as soon as possible after an attack. A high level of security within an organization can be provided with a bit of proactive consideration and planning, thereby avoiding reflexive responses that can prove disastrous.

Relevant Links

For more information on incident handling, please visit [SecurityFocus.com's Incident Handling focus area](#)

[Moment's Notice: The Immediate Steps of Incident Handling](#)

By Ben Malisow

[Computer Security Incident Handling: Step-by-Step](#)

From SANS Institute

[Computer Security Incident Handling](#)

Roger W. Baker

[Privacy Statement](#)

Copyright 2006, SecurityFocus