Global Information Assurance Certification Paper

Computer Security: Protection, Detection & Preparation

Amy Wilmeth
GSEC Practical Version 1.3

Abstract

The best way to prepare for a computer security incident is by doing everything possible to prevent it from happening, but no amount of protection will leave your system completely safe from an attacker. This paper will discuss ways to protect your systems from attackers, ways to detect an attack, and how to prepare to respond to a reported incident. This is a guide to help companies by giving them a point to begin implementation of computer security within different environments, and is therefore a general overview of these topics.

The paper begins by covering some general areas where companies and organizations need to implement and enforce security standards, policies, and procedures to ensure a high level of security to begin with. Then it moves on to detection mechanisms that can be used to detect an intruder on your system. It closes with an introduction to building an Incident Response Procedure, which includes forming a Computer Security Incident Response Team (CSIRT.) Building computer security on part if not all items covered in these three areas will give a company a good basis for computer security.

Security Awareness and Best Practices

The first step in preventing security incidents is to instill security awareness among the users on your company computer systems. If users know what is expected of them, they are less likely to inadvertently cause a security incident. Setting up company specific security best practices can be key to protecting valuable information from an intruder. Setting up security policy for all users to follow can accomplish this goal. The SANS resource site has many policy templates to use to build your own company policies from at http://www.sans.org/newlook/resources/policies/policies.htm#template.

This section will cover some key areas where standards and policies should be put into place in any company.

Strong and Protected Password Standards

Password requirements vary from company to company, so you will have to decide on a specific set of rules or standards for your company. Password

policies should stress the need for strong passwords, as well as protected passwords. Strong passwords that are just left lying around on a piece of paper do not provide adequate security.

Some common password requirements are as follows:

- A minimum of eight alphanumeric characters with at least one special character,
- Upper and lower case letters,
- Not written down or recorded online in any form,
- Not shared with anybody,
- Not words, or combinations of words, found in dictionaries, spelling lists, or other lists of words, even if combined with other alphanumeric and special characters,
- Not a user ID in any form, and
- Not information easily obtained about the user.

Program Loading/Software Download Standards

If there are no limitations to what software is loaded or programs are downloaded from the Internet to company computers, you can easily have users loading malicious code to their computers located on your company networks. Users may also be running programs that interfere with system processes. One way to control the software loaded and programs downloaded onto your network is to have the help desk or your support team load any software or programs users need onto their computers for them. You may also be able to limit the rights of the users to not allow downloads or installations. This will allow you to keep malicious code and potential attackers out of your network.

Patch and Update Procedure

Your company should let users know how software on their workstations and servers will be kept up to date. New patches and updates can contain serious vulnerabilities that could leave your company open to attack. You can either let users update their own software or again have the help desk or support team download and apply any updates or patches to the proper systems. Taking the decision out of user hands will help to avoid confusion among the users as to which patches they need to apply and when updates are available for download.

Lock Workstation Standards

It is best to have users lock their workstations anytime they are away from their desks. Anyone walking by can easily sit down at a workstation and have access to the entire company network. Someone with access to the company

network can easily steal information, make changes to documents or systems, or execute malicious programs that can be very destructive to a company's internal network. Any of these malicious uses of access can devastate a company.

Antivirus Program Standards

You should have a company-wide virus detection system set up to check incoming traffic as well as individual workstations. The workstation antiviral programs need to be properly configured by your setup or support team when installed on the system. You also need to ensure that individual users are not able to turn off virus protection software on their workstations. Antivirus programs also need to be updated periodically to detect new viruses as they are written and released into the wild. About.com's website http://antivirus.about.com/cs/antivirusvendors/ gives a list of virus protection software available.

Social Engineering Prevention Standards

Users should also be trained *not* to give out passwords or network information to unknown individuals over the phone or in person. An attacker may call up and pose as a support worker that needs to have your password to change permissions on a file. One possible alternate way to implement this is to have a support account on each workstation that is used for any changes or upgrades computer support workers need to perform. This eliminates the need for a user to give out his or her password to anyone at anytime.

Physical Security Standards

Physical security of your network is also very important. If you have your system completely safeguarded against an attacker's penetration, and an attacker is able to walk into your building, sit down at a workstation or server, and log on or power it down, all that work is for nothing. Access to server farms and servers should be restricted to system administrators and others you authorize to have access. Restricting access to workstation areas is also a good idea. Make sure to keep a record of all guests that come into or out of workstation or server areas. Train users to keep their eyes open for suspicious activity from visitors or unidentified persons. It is a good idea to ask a visitor for identification and a reason for being there if you do not know them. These steps will help secure the area where your workstations and servers are located from possible attacks.

Workstation and Server System Build Procedures

Workstation and system build procedures should be written to provide an environment that is as secure as possible. This includes turning off or uninstalling unneeded services on servers and workstations. This could also include restricting access to certain services in order to lock down a system from possible misuse. It is good to have these procedures written down so that anyone can see the requirements at anytime, and there is no confusion as to which services users are allowed to have running on their workstations or servers.

Regular Backups of Critical Systems

Any system or document that is required for company day-to-day operation and cannot be easily restored should be backed up regularly. In the event of an incident that compromises a server, restoring the server from the backup image may be much more efficient than building everything from scratch and reloading all programs, information, and updates necessary to get the system back online. You should always be sure that the backup is not compromised before putting it back online. Otherwise you may be right back where you started a few minutes later.

When all precautions have been taken to prevent a security incident, it's time to think about detecting and responding to incidents that are able to penetrate your defenses.

Detection Mechanisms

One way to detect intrusions is to set up an Intrusion Detection System, IDS, to monitor the traffic coming into and going out of your network. Setting up sensors at strategic points throughout your network will help you detect any unusual or suspicious activity on the network. Most network Intrusion Detection Systems match signatures against packet information and traits to determine if the packet looks like an attack or part of an attack. These signatures are updated periodically to identify new attacks as they are discovered. Talisker's Network Security Tools lists most Intrusion Detection Systems available today at http://www.networkintrusion.co.uk/ids.htm.

Another simple way to detect intrusions is to turn on and review audit logs on key systems regularly, such as firewalls and servers. These logs can show changes in activity or failed attempts that indicate someone is trying to do something wrong. These logs can also be used to correlate information or to identify false positive alerts from IDS logs.

Another way to detect intrusions is to have administrators and users report any activity that is out of the ordinary. Some attacks may be so new that an IDS may not have a signature to match against the attack. So if unusual activity is reported and investigated, an incident may be discovered and averted. If unsure as to whether something should be reported, go ahead and report it. It's always better to be safe than to end up sorry for not reporting something that was important.

If you have the time and the resources, a honeypot or honeynet may be another option to consider. According to Robert Lemos, a honeypot is "a software application that pretends to be a helpless server on the Internet." [1] A honeynet is "a network of standard computers that is watched closely by a combination of surveillance technologies."[1] A honeynet consists of two or more honeypots used to lure unsuspecting attackers. A honeypot or honeynet may distract an attacker from your real systems and allow you to gather valuable information about the attacks being attempted. This may allow you to update or protect your systems from an attack you may be vulnerable to otherwise. Talisker's Network Security Tools list also has information on available honeypot technology at http://www.networkintrusion.co.uk/ids.htm.

Finally, a vulnerability scan of your systems can reveal any potential problem areas that can allow an attacker to gain access or cause damage to a system. A vulnerability scan can be set up to test for weak passwords, unpatched systems, or unnecessary running programs, among other things. This knowledge can help system administrators make the necessary changes to protect their systems from known attacks. There is an extensive list of available vulnerability scanners at Talisker's Network Security Tools located at http://www.networkintrusion.co.uk/scanners.htm.

Now that we know how to prevent incidents and how to detect an attack, it's time to discuss how to prepare to respond to an incident. It's only a matter of time in today's world before your company will have to deal with an incident. Having a plan to deal with that incident can mean the difference between a minor incident and a major incident.

Preparation for an Incident

Logically when an incident or possible incident is discovered, a response method must be in place to deal with the situation. The first step to responding to an incident is writing a company specific Incident Response Procedure document.

An excellent guide to follow when writing your Incident Response Procedure document is the SANS Institute's Computer Security Incident Handling: Step-by-Step[13] guide. It gives detailed actions to take over six phases of dealing with an incident: Preparation, Identification, Containment, Eradication, Recovery and Follow-up. We will only cover the first phase, Preparation, in this document.

Your company's Incident Response Procedure document must have the support of individuals in upper management positions in order to have the authority needed to enforce the procedures outlined. It is best to have key individuals sign off on the final version of the Incident Response Procedure document.

Establishing a CSIRT in your Company

An Incident Response Procedure can only be carried out completely with a Computer Security Incident Response Team (CSIRT.) The individuals selected for this CSIRT must be given the authority needed to carry out the job they are entrusted to perform, which is why the Incident Response Procedure document is so important. The limits of the decisions the CSIRT are allowed to make should be outlined in the Incident Response Procedure document. For example, if the CSIRT is allowed to tell a system administrator to take a server offline in the midst of an incident, this will meet less resistance if a signed document can be shown that gives them the authority to do that.

The most ideal CSIRT solution is to have a team of dedicated individuals whose sole task is to work with computer security and incident handling situations. With this as the primary task of the individuals, they should be given adequate time to keep up to date on the latest news and advancements in computer security. This team can also perform the necessary vulnerability assessments on company systems, serve as the central area to report incidents or possible incidents, investigate any incidents reported and take appropriate action. This team can also serve in other areas such as computer security awareness training for users and system administrators within the company, monitoring an IDS, writing security policy and procedures, and serving as consultants on company projects requiring a computer security aspect.

While it may not be feasible for some companies to finance such a team of individuals fully devoted to computer security, the tasks of the CSIRT may be divided up and assigned to appropriate individuals within the company. Most system administrators are required to keep up to date on security issues to properly protect their systems from attackers, so it would be easy for each of them to be responsible for a different, specific aspect of the Incident Response Procedure.

Next you face the job of deciding what tasks need to be done in the case of a specific security incident within your company. These tasks should be outlined in the company Incident Response Procedure document mentioned earlier. The Incident Response Procedure must be organized into a set of guidelines to be followed by the members of the CSIRT in case of an incident.

The first step is to set up a notification procedure. All users need to know who to contact when they see anything they might consider an incident. If you have a dedicated security team, it's logical to have all incidents reported directly to that team. If not, it might be easier to have incidents reported to your help desk personnel and passed along to the proper CSIRT contact if the help desk personnel are unable to help or deem the problem CSIRT necessary. In order to do this, help desk personnel must be informed which types of minor incidents they are allowed to handle without CSIRT assistance and which incidents require notification of your company CSIRT. Whichever method your company uses, be sure that all users know who to report to in case of a security breach or possible incident. This will allow the incident to be reported quickly and allow the team to begin responding to the incident promptly.

When notified of an incident, the CSIRT takes over and decides what to do with the information received. The CSIRT will gather as much information on the incident as possible to allow them to calculate the best procedure to take in dealing with the incident. CSIRT may need to enlist the help of server administrators and others within the company while researching a security incident.

Another way that the CSIRT can prepare to respond to an incident is by having the proper knowledge and contacts needed to investigate an incident. The team needs to know how the company network is set up and which machines belong to which administrators in order to make informed decisions. A list of names and contacts should be compiled and distributed to each member of the CSIRT. Without a list of contacts, the team may be left scrambling to identify and locate the administrator of a compromised system. This can leave company information open to the attacker longer than is absolutely necessary.

CSIRT Member Assignments

With the CSIRT members chosen and contact information shared, tasks must be assigned to each member. One person should be designated as the head of the team. This person will be responsible for making final decisions pertaining to shutting down systems or removing them from the Internet or network. This person must be given the authority over all company systems to make these

types of decisions and have them carried out by others in the company.

The other members of CSIRT may be given specific tasks, or they may be assigned tasks when incidents arise. The leader of the team should know the strengths and areas of expertise of the members and assign tasks accordingly.

There should also be an alternate person chosen for each position within CSIRT. If one person is on vacation or not working the time of day the incident is reported and cannot be reached, an alternate person needs to be ready to step in and perform these necessary tasks.

Logging

The CSIRT also needs to have a logging system worked out. All actions performed by the team in response to an incident need to be documented for future reference. It's easy to perform many tasks quickly and not recall all of the details afterward.

The team may want to set up a basic template or Incident Response Form of all the information needed about an incident. This will allow the team to gather the required information as quickly as possible under the time pressure of the situation. This can be used to summarize the important information from an incident. Having all of this information from the beginning will help expedite the incident response procedure.

Some key information you want to be sure to include in your Incident Response Form includes the following:

- Source and destination IP numbers and port numbers
- Owners/Administrators of IP numbers involved
- Contact information
- Dates and Times of incidents and discoveries
- Information on any contact (email, phone, in person) made and what information was obtained

This is by no means the only logging required for an incident. A detailed log should be kept that answers the basic questions who, what, when, where, why, and how about that particular incident and any actions taken to research and resolve the situation. Having a log of all these details can be useful for training new team members or learning from past mistakes and not making them again when dealing with future incidents. The solution can also be applied to similar incidents in the future for a quick return to normal operation.

Other considerations

In preparing the Incident Response Procedure for your company's CSIRT to follow, you will also want to consider of the following items:

- Preserving evidence – You will need to preserve a copy of any compromised system for use in cases of legal action. The legal department in your company should be contacted to coordinate this effort. A copy is also useful in analysis when a system needs to be back online as soon as possible. You can keep a backup copy to analyze further while system administrators can get the system up and running if a backup machine is unavailable for use. A complete system rebuild is usually recommended to prevent any backdoors from staying on the compromised system. In some cases it may be safe to "disinfect" the system in the case of a viral infection with a removal program.

- Contacting Sources of Attacks – Your company will need to implement a policy for contacting ISPs and other offending sources of an attack. You may want to make up a template of information you want to initially give to an attacking IP number's abuse contact. In case the person that receives the information is part of the attack, you do not want to give away too much information pertaining to your network and the level of penetration of the attack. It is usually best to initially only give them information that can easily be obtained from outside your network. Including dates and times of the incident should allow them to be able to look into the matter from their side.

- Blocking IP numbers from your Network – Your company will also need to decide when it is permissible to block an attacking IP number or IP block if there is no other way to stop the attacker. This could potentially block customers and users from reaching your site. It may be best to temporarily block an IP number or group of IP numbers until your systems are prepared to stand up to the attack.

All of these items should be considered when writing your Incident Handling Procedure document and forming a CSIRT to handle incidents in your company. For more information on forming a CSIRT for your company, see CERT Coordination Center's CSIRT development site at http://www.cert.org/csirts.

Conclusion

This has been an overview of how to begin securing a network of computer systems, detecting intrusions on those systems, and responding to security incidents that occur. After implementing a security policy, which covers all

aspects of computer security, your computer systems should be as well protected as possible. An attacker can still break into even the most protected systems, so it is important to have detection mechanisms in place to see when security breaches occur. After a security breach is discovered, the policies and procedures must be in place to allow a group of individuals to respond to that incident and repair any damage done enabling operation to continue as normal.

References

1. Lemos, Robert. “Honeynet Project sweetens hacker bait.“ 13 July 2001.
URL: http://news.com.com/2100-1001-269900.html?legacy=cnet (3 April 2002).

2. The Honeynet Project.
URL: http://project.honeynet.org/ (3 April 2002).

3. Theunissen, David. “Corporate Incident Handling Guidelines” 14 November 2001.
URL: http://rr.sans.org/incident/corp_guide.php (3 April 2002).

4. “NAS Security Incident Handling Procedures.” 4 March 1998.
URL: http://www.sans.org/newlook/resources/policies/item7.pdf (3 April 2002).

5. “State of Vermont Incident Handling Procedures.”
URL: http://www.cio.state.vt.us/pdfs/sov_intrusion_procedures.pdf (3 April 2002).

6. BSI (Bundesamt fur Sicherheit in der Informationstechnik). “IT Baseline Protection Manual: S 6.58 Establishment of a management system for handling security incidents.” January 2000.
URL: http://www.bsi.de/gshb/english/s/s6058.htm (3 April 2002).

7. Scalet, Sarah D. “How to Plan for the Inevitable.” 15 March 2002.
URL: http://www.cio.com/archive/031502/plan.html (3 April 2002).

8. Kossakowski, Klaus-Peter, et al. “Responding to Intrusions.” February 1999.
URL: http://www.cert.org/security-improvement/modules/m06.html (3 April 2002).

9. Ford, Paul Mason. “Incident Reporting & Automation.” 9 March 2001.
URL: http://rr.sans.org/incident/automation.php (3 April 2002).

10. Talisker’s Network Security Tools list: IDS list.
URL: http://www.networkintrusion.co.uk/ids.htm (3 April 2002).

11. Talisker’s Network Security Tools list: Vulnerability Scanners list.
URL: http://www.networkintrusion.co.uk/scanners.htm (3 April 2002).

12. About.com. Antivirus Software list.
URL: http://antivirus.about.com/cs/antivirusvendors/ (3 April 2002).

13. SANS Institute publications. Excerpt from Computer Security Incident Handling: Step-by-Step.
URL: http://www.sans.org/newlook/publications/incident_handling.htm (3 April 2002).

14. CERT Coordination Center. “Incident Reporting Guidelines. 30 July 2001.
URL: http://www.cert.org/tech_tips/incident_reporting.html#IV (3 April 2002).

15. SANS Institute resources. “The SANS Security Policy Project”.
URL: http://www.sans.org/newlook/resources/policies/policies.htm#template (3 April 2002).

16. CERT Coordination Center. CSIRT development.
URL: http://www.cert.org/csirts/ (3 April 2002).

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor