Global Information Assurance Certification Paper

Version 1.4
CERT: A Valuable Team to Mitigate Computer Security Vulnerabilities in an Organization
Nancy L. Bell

Abstract

In the aftermath of the Morris Worm Incident, or the Internet Worm, in 1988, many computer experts were bustling around trying to anticipate the next occurrence of a virus, propagating Trojan horse, or other widespread attacks. As a result, one of several 24-hour emergency response teams that were established was the Computer Emergency Response Team, or CERT. This paper provides an overview of what a CERT is and what services, including types of alerts that it can provide to assist in the mitigation of computer security vulnerabilities. In addition, information of areas to consider to justify the need for an implementation of a CERT are included, as well as what preparations and interpersonal skills are required to ensure that a team is as efficient as possible.

Introduction

The Computer Emergency Response Team (CERT) was formed by the Defense Advanced Research Projects Agency (DARPA) in 1988. Centered at the Software Engineering Institute at Carnegie Mellon University, CERT is an assistance team that is comprised of technical experts from around the country who are responsible for receiving, reviewing, and responding to computer security incident reports and activity. Security incidents, defined as any related set of security events, ranging from a large-scale virus outbreak to much smaller ones, have risen nearly every year since CERT's founding in 1988.

It was during an outgrowth of the November 1988 Internet worm incident, which was managed and resolved by an informal network of Internet users and administrators, that CERT was established to provide the capability for more systematic and structured response; in particular, it was intended to facilitate communications during system emergencies.

Through practical experience dealing with attacks on systems, one role that has evolved since CERT's inception is communication with vendors regarding software weaknesses or vulnerabilities. CERT incorporates experience from system users and development communities, as well as coordinates efforts with the National Institute of Standards and Technology and the National Security Agency. Additionally, it sponsors workshops to involve its constituents in defining its role and to share information about perceived problems and issues (Pethia, 2000).

CERT's services are usually performed for customers that include corporations,

federal and state government agencies, and educational organizations. The CERT responds to computer security threats such as the recent self-replicating computer program virus, "I Love You" [CERT® Advisory CA-2000-04 Love Letter Worm] (Carnegie Mellon University, 2000), that invaded many defense and research computers.

According to Pollak (2002), "'CERT' and 'CERT Coordination Center' are registered with the U.S. Patent and Trademark office as service marks of Carnegie Mellon University." When referring to the CERT/CC in writing, use 'the CERT® Coordination Center' or 'the CERT®/CC'. Although 'CERT' should not be expanded into an acronym, it is appropriate to note in your writing that the CERT/CC was originally the Computer Emergency Response Team.

Services Performed by a CERT

The implementation of a CERT provides an organization with a dedicated team to receive, review and respond to computer security incidents and activities, such as those stated above. Through a series of services, this team can help to mitigate vulnerabilities that might otherwise be left wide open to intruders and address incidents should a system be penetrated. An overview of these services follows in the paragraphs below.

Vulnerability and Risk Analysis

Through the establishment of testing programs and procedures, the CERT can assist in identifying flaws in the design an implementation of systems and products. With such procedures in place, they can assist in developing methods to report technical vulnerabilities, suggest work-around solutions, and identify ways to issue necessary alerts. The CERT can also identify cyber-security needs as well as develop and implement improvement plans.

Intrusion Detection

The CERT will collect and analyze intrusion reports to identify patterns and trends and spot potential problems early. They will establish focal points for understanding and promoting the use of intrusion detection technologies, practices and services.

Incident Handling

This process for the CERT includes receiving request from various government agencies or organizations, responding to the incidents appropriately then analyzing, tracking and recording the appropriate data. They also verify the incident, including its magnitude and scope, protect the evidence, communicate with the management who are involved and recover programs and applications, including the restoration of data. During

this phase of the incident, some of the tasks and actions that are done by CERT Incident Handlers include:

- Analyzing reports, logs and files
- Researching site or host information
- Providing direct technical assistance
- Coordination and sharing information

Once this type of information is captured, it needs to be protected through a secure chain-of custody procedure that tracks who has been involved in handling the evidence and where it has been stored. Another good rule-of-thumb is labeling the data according to classification or sensitivity in order to help the investigation progress smoothly (West-Brown et al., 1998).

Once data has been gathered, the CERT will provide guidance on how to record and track all information associated with any type of activity that is reported. Some of the key points to handling this data include:

- Prioritizing incidents and action items
- Correlating incident activity reports
- Providing status updates to management
- What is the current workload
- Transferring the incident to someone else
- Prepare for possible legal action

The answers are only obtainable by evaluating and analyzing all of the available information. To identify the details of the incident, the CERT can identify what the nature of the incident was by answering the following questions:

- What technique was used to gain access?
- What system(s) and data were accessed by the intruder(s)?
- What did the intruder(s) do after obtaining access?
- What is or was an intruder doing before the compromised system was contained or eliminated?

In order for the CERT to deal with an intrusion effectively, they need to determine its scope, address possible impacts, and prioritize their intended actions. An intrusion can only be dealt with effectively once all collected information has been analyzed. Jumping to conclusions, without a thorough analysis, can result in false and inaccurate information and may be considered unprofessional.

Once an intrusion incident has been analyzed and addressed, the incident must be

closed. The CERT is responsible for establishing guidelines on how to properly close an incident, including the process of notifying the involved parties that the incident has been closed as well as determining any expectations should it need to be reopened.

Alerts and Announcements that CERT May Provide

In an effort to prevent possible intruder attacks, a CERT can be a central point for providing information on Alerts and Announcements. Announcements such as CERT Advisories [CA-2000-17] provide information on preventing threats that are generally discovered as the result of incident reports and cannot generally be created without use of the team's vulnerability service. Announcements can take on many forms, from those providing short-term information related to a specific type of ongoing activity to general long-term information for improving awareness and system security. Several types of announcements are briefly discussed in the paragraphs below.

Heads-up Announcement

A 'heads-up' announcement usually takes the form of a short message and is issued when detailed information is unavailable. The purpose of this type of message is to inform those who may be affected of something that is likely to be important in the near future.

Alerts

Alerts are short-term notices about critical developments containing information about recent attacks, succeeded break-ins or new vulnerabilities. Lanza (2001) provides an example of DOD CERT alert that was issued to address vulnerabilities in Microsoft's Internet Explorer:

> DOD CERT Alert 2001-A-0015 Multiple Vulnerabilities in Microsoft Internet Explorer
>
> Systems Affected
> IE 5.01 sp2 for Windows 2000, IE 5.5 sp1/sp2, IE 6.0
> IE versions prior to 5.01 sp2 are not supported by Microsoft, thus have not been tested and may be susceptible to this vulnerability.
>
> TECHNICAL OVERVIEW: In the File Execution Vulnerability HTML web pages and email messages usually contain HTML text, but other files types may also be included. When obtaining files from the web server or the attachments of an email message the MIME headers Content-Disposition and Content-Type determine the type of the file in question.

There is a problem with the way that the Content-Disposition and Content-Type MIME headers are handled in Internet Explorer. By constructing malicious web pages or email messages using these headers to misrepresent the file type, an attacker may be able to execute arbitrary code on a victim's system. This code would be executed as the user who viewed the web page or the email message. The only dialog boxes or warning that might allow a user to prevent the execution of the malicious code would be the download progress dialog box. Apply the appropriate Microsoft patch immediately.
http://www.microsoft.com/windows/ie/downloads/critical/q316059/default.asp

Advisories

Advisories provide mid- and long-term information about problems and solutions suitable to raise awareness and help avoid incidents. These advisories can be very beneficial to network administrators and application developers as the individuals can keep the information in mind, implement necessary patches to mitigate possible vulnerabilities and try to eliminate up front any security holes that might otherwise exist allowing an intruder to infiltrate a system. One example of a CERT Advisory is provided by Hernan (2002) and identifies vulnerabilities in Microsoft's Internet Information Server (IIS):

CERT® Advisory CA-2002-09 Multiple Vulnerabilities in Microsoft IIS:

Systems Affected
Microsoft IIS 4.0, 5.0, and 5.1
Overview
A variety of vulnerabilities exist in various versions of Microsoft IIS. Some of these vulnerabilities may allow an intruder to execute arbitrary code on vulnerable systems.

I. Description
There are a variety of vulnerabilities in Microsoft IIS. Many of these vulnerabilities are buffer overflows that could permit an intruder to execute arbitrary code on vulnerable systems.

We strongly encourage all sites running IIS to read Microsoft's advisory on these and other vulnerabilities and take appropriate action as soon as practical.
Microsoft's bulletin is available at
http://www.microsoft.com/technet/security/bulletin/MS02-018.asp

Technical Guidelines and Procedures

Technical guidelines have been developed and are available with technically detailed procedures in order to fix problems that may occur. Examples of some of these procedures can be found in the CERT Tech Tips. Once such procedure containing information on how to address problems with known "Sendmail" vulnerabilities is the CERT Advisory CA-95:05.sendmail.vulnerabilities (CERT/CC ,1995).

Considerations for Justifying a CERT

While a CERT may not be in the forefront of consideration of an organization, there are many considerations that may help to justify the development and implementation of a CERT. A few of the more prominent ones are discussed below.

Internet

With the advances in technology, the Internet has increasingly become a part of our every day lives. It is an international merging of cross-jurisdictional networks resulting in an explosion of use by government agencies, commercial industries and consumers. This increasing use has resulted in a large number of applications being placed on the Internet that may contain sensitive information. With millions of entry-points, the lack of central administrative control and the steady stream of new technologies it incorporates, the Internet is an easy target for intruders.

Opportunities for Intrusion

There are many changes in the way we use technology that have opened the doors for new opportunities for intrusions. Some of these changes include a rapid adoption usage of computers and networks, technology growth in government, and educational organizations, expansion of e-commerce and thousands of reported exploitable vulnerabilities in technology alone in 2001 (Carnegie Mellon University, 2002). With all of this in mind, it may bring forth a shortage of a lack of awareness regarding information security, a shortage of qualified system and network administrators and a lack of security regulations and means of enforcement.

Intruder (Hacker) Motives

Intruders conduct attacks for multiple reasons, including widespread disruption, espionage, money/profit incentives, competitive advantages, personal grievances, vengeance or as simple as a curiosity of new technical features.

Effects of an network attack

If an intruder, or hacker, succeeds in penetrating the software or system, there are a number of exploitations that may be taken advantage of. Some of the possible effects of an attack include denial of service, unauthorized use or misuse of computing systems, the loss or compromise of data or software, or the loss of trust in a computer or network system.

There are many possible attacks that an intruder may perform. One such attack is Internet Protocol (IP) spoofing. IP spoofing is a technique where the intruder "sends messages to a computer with an IP address indicating that the message is coming from a trusted host" (INT Media Group, Inc., 2002). Another attack, denial of service attack, essentially renders a network useless, as the intruders flood it with massive useless traffic. A type of attack that we're all familiar with is the virus that can take many forms, including a self-replicating, memory intensive version known as a worm. Intruders also pride themselves in other types of attacks including, but not limited to, web abuse, email bombing and attacks on routers.

Preparing a CERT

The value of a CERT can only have positive effects for an organization; however, a CERT can only be effective when it is properly prepared, when regular training and adequate education is provided and when timely access is granted for necessary information. It is also vital to set up proper policies and procedures to ensure the success of the team. These areas are expanded upon in the paragraphs that follow.

External Preparations

To ensure that a CERT is fully prepared, it is good practice to establish contacts with local law enforcement officials. It is also beneficial to have the CERT join a local chapter of InfraGard. InfraGard is a government and private sector alliance developed by FBI Cleveland in 1996 to help provide formal and informal channels for the exchange of information regarding infrastructure threats and vulnerabilities (InfraGard, 2002). It is also important during preparations to have Internet accessibility and the phone numbers and contacts for companies that have developed software that is installed on existing computer systems.

Participation in Continued Education

Continued education, in both current and upcoming technologies, provides learning opportunities and expands team knowledge on future information systems developments. There are many organizations and companies that provide this type of training, i.e. Carnegie Mellon Software Engineering Institute; System Administration, Networking and Security (SANS) Institute; CERT Organizations; Computer Security Institute; CERT and

Security User Groups. The threat is ever changing and certifications such as the Global Information Assurance Certification (GIAC) help to keep team members up-to-date with current technologies and issues.

Implementation of Staff Training Programs

To ensure that team members are kept apprised of new technologies, it is important to implement staff training and awareness programs for the team members. The CERT can provide information systems security training to managers and system administrators (Army Regulation 380-19, 1998, p.10). A CERT exchanges ideas and practices to enhance the sharing of security-related information and tool usage. For instance, the team can set up separate computer labs to test various known exploits and practice using CERT toolboxes. Other recommendations include implementing a reading library as well as joining various security-related groups and information security related listserv mailing lists.

Ensure Timely Access to Appropriate Information Resources

Information relating to computer security is ever changing and team members need to have the capability, knowledge, and necessary know-how to be able to look for updates on incidents that have occurred. One of the best resources available is having accessibility to various web sites, including http://www.cert.org, http://www.securityfocus.com and http://www.cert.mil.

Defining Policies and Procedures

A CERT's documented policies and procedures are vital to the success of the CERT. In order to offer guidance to the CERT, the policies and procedures must be well defined and clearly understood so that the staff can correctly implement procedures and fulfill their responsibilities. Procedures need to clearly indicate how policies, services and responsibilities are to be carried out as well as how to provide the necessary level of detail to ensure clarity of the mission. To remain effective, policies should undergo a regular review and updated cycle.

Interpersonal Skills Necessary for an Effective and Efficient CERT

While the CERT, as a whole, can work to reduce and address security vulnerabilities that may occur, it is critical to have a team that works as a cohesive unit. In order to achieve this type of dynamic team, there are certain interpersonal skills that a CERT member should possess, including common sense, good communication skills, discretion, integrity, and problem-solving techniques. These traits are expounded upon in the following paragraphs.

Common Sense

Team members need to have common sense in an effort to help make efficient and acceptable decisions whenever there is no clear ruling available, when a severe time crunch is a factor or when the situation results in a lot of stress.

Communication Skills

Members of a CERT must also have effective oral and written communication skills necessary to interact with other team members or personnel from various organizations.

Discretion

During an investigation of a computer incident, team members need to be discreet, where necessary, when dealing with various parties, i.e. the media.

Integrity

A CERT's reputation and solid foundations are built on members' integrity and trustworthiness when handling incidents.

Problem solving techniques

Each team member is as beneficial as the next, as each brings various skills to the table. As new incidents occur, problem solving can efficiently be handled when the team's members skills compliment each other's, resulting in a dynamic approach to the problem at hand.

Possible CERT Staffing Issues

A competent and skilled team is hard to find and the initial training process does take time. It is important to provide opportunities for professional development, career growth for each team member. If opportunities are not made available, one resulting side effect could be staff 'burn out." Instead, provide team members with the opportunity to excel and be an integral part of the "Team" and let them know that opportunities for training and learning will always be available.

Conclusion

The benefits of implementing a CERT are many. The purpose of a Computer Emergency Response Team is to promote research and develop techniques for information systems security and provide support mechanisms to coordinate activities of

experts in the Defense Advanced Research Projects Agency and associated communities. It provides a reliable, trusted, 24-hour, single point of contact for emergencies and has the capability to rapidly facilitate communication among experts working to solve security problems to the affected computer users and government authorities as appropriate. A CERT serves as a central point for identifying and correcting vulnerabilities in computer systems and maintains close ties with research activities and conduct research to improve the security of existing systems. Once a CERT has been formed and implemented, it is through proactive measures of ongoing training and education that an increased awareness and understanding of information security and computer security issues is obtained. As with biological viruses, the solutions must come from an organized group of experts who possess some very important interpersonal skills – a CERT can provide just that for computer security.

References

Army Regulation 380-19. (1998). Information Systems Security, HQ's Department of the Army, Washington, DC, 27 February 1998

Carnegie Mellon University. (2000). CERT® Advisory CA-2000-04 Love Letter Worm. Retrieved May 25, 2002 from the World Wide Web: http://www.cert.org/advisories/CA-2000-04.html

Carnegie Mellon University. (2002). CERT/CC Statistics 1988-2002. Retrieved May 25, 2002 from the World Wide Web: http://www.cert.org/stats/

CERT/CC (1995). CERT Advisory CA-95:05.sendmail.vulnerabilities, Retrieved May 18, 2002 from the World Wide Web: http://www.cctec.com/maillists/nanog/historical/9502/msg00046.html

Hernan, S.V. (2002). CERT® Advisory CA-2002-09 Multiple Vulnerabilities in Microsoft IIS. Retrieved May 17, 2002 from the World Wide Web: http://www.cert.org/advisories/CA-2002-09.html

InfraGard (2002). Frequently Asked Questions. Retrieved May 25, 2002 from the World Wide Web: http://www.infragard.net/faq.htm

INT Media Group, Inc. (2002). IP Spoofing. Webopedia. Retrieved May 29, 2002 from the World Wide Web: http://www.webopedia.com/TERM/I/IP_spoofing.html

Lanza, J.P. (2001). Multiple Vulnerabilities in Microsoft Internet Explorer. DOD CERT Alert 2001-A-0015. Retrieved May 18, 2002 from the World Wide Web: ftp://www.cert.mil/pub/bulletins/dodcert2001/2001-a-0015.htm

Pethia, R.D. (2000). Computer Security – testimony, Retrieved May 25, 2002 from the World Wide Web http://www.cert.org/congressional_testimony/Pethia_testimony_Mar9.html#Introduction

Pollak, B. (2002). Frequently Asked Questions About the CERT Coordination Center. Retrieved May 25, 2002 from the World Wide Web: http://www.sei.cmu.edu/about/press/CERT_faq.htm#3

West-Brown, M., Kossakowski, K., Stikvoort, D. (1998) Handbook for Computer Security Incident Response Teams (CSIRTs). December 1998 HANDBOOK CMU/ SEI-98- HB- 001 Pittsburgh, PA 15213- 3890

Web Resources:

http://www.cert.org

http://www.infragard.net

http://securityfocus.com

http://www.cert.mil