GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Incident Handling:
An Imperative Tool in the Battle Against Cyberterrorism

Kelly McCracken

GSEC Practical Option 1v 1.4b

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Abstract

Cyberterrorism has been the topic of discussion and worry for the past few years. The United States, in particular, has been contemplating how to deal with the situation. A solution: incident handling. Incident handling is the process of preparing for a cyber attack, and identifying, containing, eradicating, recovering, and following-up after the attack.

This paper suggests an outlined process for incident handling to help prepare an organization for a cyber attack on their system. A few of the most severe cyber attacks from the past are presented with information on how incident handling played a role in the recovery of each. A discussion of precautionary measures the U.S. has taken to protect against cyberterrorism is also included in this paper. This paper is designed to illustrate the role incident handling must take in order to protect the nation's computer systems from cyberterrorists.

Introduction

The need for computer security, in both the public and private sectors, has increased significantly and can be demonstrated through the Nimda worm. On September 17, 2001, the Federal Bureau of Investigation (F.B.I.) National Infrastructure Protection Center (NIPC) released Advisory 01-021 announcing potential Distributed Denial of Service Attacks (DDoS). Since there was known hacking activity in response to the September 11, 2001 terrorist attacks, the NIPC warned that the potential DDoS activity could be related. However, on September 18, 2001, the NIPC released Advisory 01-022 that announced a new Worm, called W32.Nimda.A@mm - also known as Nimda. Nimda exploits vulnerabilities in software that run on various versions of Microsoft Internet Explorer browser, Internet Information Server (IIS) and Office 2000 across various platforms of the Microsoft operating systems: Windows 95, Windows 98, Window ME, and Windows 2000. By disrupting many of the nation's computer systems, Nimda helped illustrate the importance of incident handling, a series of steps that will greatly aid organizations in dealing with cyberterrorism and minimizing its effects. Nimda demonstrated to many companies, and the U.S. Government, that incident handling is an essential part of an information security program

Incident handling has never been as important as it is today. With major daily activities such as commerce, communication, and security being conducted on a foundation supported by networks and powered by the Internet, a major cyber attack by terrorists is wholly plausible. A powerful "super" worm would cause significant damage, hurt companies financially, and possibly jeopardize companies' proprietary information. Although the world is divided into countries by borders, these borders do not exist on the Internet. Boundaries have been blurred by technology, at a pace that has left governments and regulatory agencies wondering how to best protect the public's interest, without invading their privacy. Governments have researched and developed methods to track cyberterrorists, but to date, no procedure has been developed that does not in some way impede

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

upon the right to freedom of speech. The F.B.I. uses a system called Carnivore that has the capability to intercept and collect internet traffic, which are the subject of the lawful order while ignoring those communications which they are not authorized to intercept. However, there remains much controversy over its connection to Internet Service Providers' (ISP) servers. The ISP industry has fought court orders allowing the F.B.I. to use Carnivore because it has the ability to surveil Internet traffic of their customers, a trait that is viewed by many as an invasion of privacy.

Despite spending millions of dollars on incident handling and related research, there is still no way to truly secure a system, similar to the notion that there is no way to truly protect against an act of physical terror. However, ensuring that a system's security features are up-to-date and installing the most recent technology can decrease the chance that a system will be jeopardized. Being prepared in the event that an attack on a system occurs can decrease the amount of damage and increase the chance of catching the intruder.

Cyberterrorism is a reality in today's world, but as more companies and the Government build stronger incident handling programs, the effects can be significantly decreased.

An Overview of Cyberterrorism

After the September 11th attacks, the definition of "terrorism" was viewed with an entirely new meaning. Although the attack took place on physical structures, each target carried great symbolism. One was synonymous with America's great financial freedom and dominance throughout the global economy. The other, which still stands, represents our political liberty and military strength. And while these buildings varied greatly in terms of the work their inhabitants performed, the two share much more in common than simply being on the receiving end of those terrible attacks. As a country, we were rudely awakened to the fact that, in creating an open and trusting society, we had simultaneously become vulnerable to both physical attacks, as happened on September 11, 2001, and a cyber attack in the form of a digital worm that spread in the week following those attacks. Another dose of shock treatment that proved Cyberterrorism is every bit as real of a threat as physical terrorism. And while its results may not be as severe in terms of loss of life, its effects on financial markets, productivity and other, more extensive forms of security have the potential to be far more reaching. So, although an attack would indeed cause problems, they would most likely be nothing that would threaten life.[1]

Cyberterrorism is defined as using the cyber-infrastructure to directly inflict fear upon the victim. In today's society, a cyber attack would cause great chaos all over our world: a world connected by wires that shoot information around the planet in nanoseconds. As Ed Skoudis once said, "A snow storm can shut down a city for a day or two, but it is not Armageddon…the same goes for the Internet."[2]

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

An Overview of Incident Handling

In today's world, it is imperative for an organization to have a strong incident handling plan in place. One devastating incident could cost a company millions of dollars not only in hardware and software, but also in the loss of proprietary information, company time, and productivity. Many corporate executives overlook the need to have a strong incident handling procedure in place because of the lack of knowledge about computer security. Incident handling indeed has significant costs associated with it (i.e., equipment purchases, employee training, etc.), but the benefits far outweigh the costs. In order to prevent a system from being completely compromised, it is advised that a company follow the six phases of incident handling: preparation, identification, containment, eradication, recovery, and follow-up.

Preparation

Preparation is the most crucial step in incident handling. If a system is not initially prepared for an attack, it is extremely vulnerable and if attacked, the potential destruction will be greater. In order to help prevent an intrusion, it is necessary that a company plans and prepares for any possible intrusion. This includes creating a security plan and policy, developing an emergency communication plan, selecting and training incident handling team members, providing easy reporting facilities, and routinely practicing and improving upon the incident response plan.[3]

Ensuring that security policies are in place is not the only precautionary step in preparing a system. This initial phase in the incident handling process also includes preparing your systems by layering protective measures. It is important to have multiple security controls in place, but the security of a system should be built upon the foundation of the business. For example, an intrusion detection system should be installed to help detect an attack (this will be discussed in more detail in the identification phase). As with many protective measures, the quality of the security must be paramount to the quantity – more money spent on security systems does not equate to more secure systems. Security controls should only be used for what the business requires. In other words, build a system that allows the company to access their business needs and then eliminate anything else.[4]

What are probably the two easiest ways to protect a system? Install antivirus software and apply all security patches. Installing antivirus software after a clean reboot, or even better, as part of the first installation, can help protect your system against viruses. However, the only way the antivirus software can truly protect a system is by ensuring it is kept up-to-date by using the online updates. Although when software is released, the developers believe it is secure, but this is not always the case. After software is released, usually vulnerabilities are found. When this occurs, the vendor is notified and then tries to develop a patch for the vulnerability. Once a security patch is developed and released, organizations should test the patch for quality assurance before it is applied to the system. Without applying the current patches to your system, you run a greater risk of

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

being attacked. Security patches can be found at websites that develop the product that requires the patch, such as Microsoft's website for all of its products.

Identification

Noticing something unusual on a system is usually the first step to identification. Identification involves perpetual monitoring, which will help determine whether an event has really occurred, and the nature of this event. Examining the system logs regularly will help a system administrator be more aware of an intrusion or some unusual activity. The system log can show denied access messages, messages referring to old vulnerabilities, and blocked accesses to specific services.[3]

During the identification phase, a person should be assigned the responsibility for leading the incident response, enabling the incident handling process to continue in an organized fashion. A "need to know" policy should go into affect to ensure that the intruder does not realize he is being monitored because of a significant change in the system's processes. If the whole organization is notified of the intrusion, it could cause chaos and the intruder might catch on, making it difficult to catch them. Coordination with the organization's network services should be established in the event that a system has to be pulled off the network or the ISP needs to be notified. However, it should be kept in mind that only secure communication channels should be used to prevent the intruder from overhearing the communication.[3]

An intrusion detection system (IDS) is a tool that can aid in the identification and detection of activities of an attack. The system should be installed as a part of the preparation activities as a supporting infrastructure component to the incident response capability with in an organization. The IDS's one purpose is to detect an attack by a hacker by monitoring incoming traffic while the attack is actually occurring.[5] By using a host-based intrusion detection tool, you can prevent a worm from infecting your system by blocking it from entering the system. An IDS can be placed as a central IDS that monitors traffic from the Internet, and/or it can be placed on every computer to also monitor internal threats. The IDS first analyzes the data that originates in system event logs. The IDS then compares the operations on the log to the pre-exiting database. There are two types of pre-existing databases that an IDS can use: one that has what the system will allow; and one that contains what the system will not allow. The pre-existing database then directs the IDS as to what to do about the attack. If there is an obvious violation, the IDS will sound an alarm and alert the system administrator.[5]

Containment

In order to keep the magnitude of the incident to a minimum, it is important that the problem is contained. In order to contain the incident, there are a few steps that should be followed to make sure the problem does not expand. First, an on-site team should survey the incident and secure the area, if possible, while making sure to keep the system in the exact state that it was found. Securing the area

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

includes isolating the compromised system and keeping all non-essential persons away from the system. It is important to make this process efficient and inconspicuous; otherwise the chance of catching the attacker is slim. Another important step is to back up the system using new media. However, before it is backed up, the original information should be write-protected to prevent it from being changed. This backup should then be stored in a safe place to prevent tampering. If the evidence is altered and/or tainted it loses its validity as evidence in the event that the intruder is taken to court. It is also important to keep all the log files containing information regarding the intrusion to use as a reference in an investigation. Throughout the whole incident handling process, chain of custody should be maintained in order to have verifiable documentation of everyone that has had access to the compromised system. The final step in containment is determining whether the organization should continue operating in the compromised situation. [3]

Eradication

Once an incident has occurred, it is important to make sure it is not repeated. In order to do this, the problem needs to be eradicated. To eradicate the problem, the cause needs to be identified in order to improve the system's defenses. A vulnerability analysis should take place to search for any additional vulnerability on the system and prevent any future incidents of the same nature. The final step in eradication is to locate the most recent backup before the intrusion so that the system can be restored back to its original state.

Recovery

The first reaction, once the recovery stage has been reached, will be to restore the system. However, the system will require analysis to determine how the system can be improved so that the same kind of attack does not reoccur. The system may need to have its antivirus software updated, or the IDS updated with new policies. Documents should be copied in order to overwrite and reformat the system. Once the system is operating, the root password and all other passwords should be changed.

Another security measure that should be taken to prevent the intruder from entering the system again is a step that is taken in the preparation phase also: the application of security patches. The best approach would be to reload the system from clean sources of locally compiled applications.[3]

Follow-up

When the incident is under control, it is important to look back and reflect on how the incident occurred, and how effective the ensuing handling of the situation was. If the organization does not reflect on the intrusion and try to improve its security, the incident will continue to occur. Improvement of the security is not the only step that should take place; actions taken during the incident handling should also be assessed. During the follow-up stage, strategy meetings should be held, analytical reports should be written, and IT security-related policies should be updated.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Within three to five working days following the investigation of the incident, a meeting should be held with all involved parties. The meeting should discuss what needs to be improved in the system's security, as well as what can be improved with regards to the incident handling process. Important points to consider are whether to change the placement of firewalls, move the compromised system to a more secure location, change the IP address of the compromised system, or update the routers and firewalls.[3]

To document the incident, a report should be written contemporaneously with the investigation to ensure that all details are recorded. This document should include what worked well and what did not, which policies need to be updated, and which incident handling processes need to be improved. The document should also include any forms that were used during the incident handling process.[3]

After the meeting has occurred and the follow-up report has been prepared, the security policies, plan, and procedures will most likely require updates. These documents should be updated with all the suggestions that were mentioned during the report and meeting. The management groups should then be brought up to speed on all the changes.

Previous Cyber Attacks: Lessons Learned in Incident Handling

Cyberterrorism has had a major impact on the United States and the rest of the world. Some of the attacks have been more damaging than others, but each attack finds room for improvement in computer security, especially in incident handling. The statistics of the past are enough to make many in the IT field cringe, but our ever-increasing use of, and reliance upon, networks, email, and the Internet is enough to make everyone more aware of the crippling effects that a large-scale cyber attack could have.

Cyber attacks have caused great distress to organizations and individuals. However, once a cyber attack occurs, efforts must be exerted to improve incident handling and computer security. Three of the worst cyber attacks are discussed below with a detailed description of how each led to the improvement of incident handling either by procedures or by use of security tools. A proactive approach to incident handling is the key to preventing cyber attacks and minimizing their effects on systems. In the coming years, the severity and frequency of cyber attacks will increase. The only thing that can reduce the threat of these attacks is to use what is learned from the past and apply it to the systems and incident handling procedures of today.

Distributed Denial of Service Attacks (DDoS)

Shortly after the arrival of the millennium, a series of DDoS attacks crippled some of the Internet's most popular sites: Yahoo!, CNN, Amazon.com, E*Trade, ZDNet,

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

and Buy.com. The purpose of a DDoS is to cause a flood of data packets to target servers, which in turn, causes them to crash or block legitimate access to the server by using up all the available bandwidth. According to the trade magazine ***Information Security***, this attack increased awareness of the vulnerability of the Internet. [2]

There are multiple tools hackers can use to send out a DDoS. These tools use technology to create large networks or hosts that have the capability to launch large coordinated packet flooding denial of service attacks.[6] Two tools that will be discussed in this paper are the Trinoo (trin00) and the Tribe Flood Network (TFN). Each specific tool carries out the attack in a different way. Trinoo launches an attack from many sources by using User Datagram Protocol (UDP) denial of service attacks. UDP is a connectionless protocol that runs on top of IP networks that offers a direct way to send and receive datagrams over an IP network.[7] Although UDP is usually used to broadcast messages over a network, Trinoo uses it to send a flood of messages over the network causing a denial of service attack. A DDoS attack is carried out by an intruder using a Trinoo network to connect to a Trinoo master and instructing it to launch a denial of service (DoS) attack against more than one IP address. The Trinoo master then instructs the daemons to attack the IP addresses for a specified amount of time.[6]

A Tribe Flood Network (TFN) is a distributed tool that launches a coordinated DoS attack from many sources against one or more targets. TFN is similar to Trinoo since it too can generate a UDP flood attack. Along with UDP flood, TFN can also generate a TCP SYN flood, ICMP echo request flood, and an ICMP directed broadcast DoS attack. An intruder, using a command line, instructs a client (master) to send attack instructions to a list of TFN servers (daemons). The master uses ICMP echo reply packets with 16-bit binary values embedded in the ID field to communicate with the daemon. The binary values are what represent the instructions sent from the masters to the daemons. The daemons can then generate a specified type of DDoS attack against target IP addresses. In order to use the TFN master, the intruder must provide a list of IP addresses for the daemons. The list of daemon IP addresses can be concealed using blowfish encryption. TFN daemons tend to be installed on systems under the filename "tp."[6]

The DDoS attacks accentuated the necessity of having anti-spoofing filters. This will cause the firewalls to drop the spoofed traffic if the web server starts spewing packets using unknown sources. This attack also made incident response teams more aware of the need to coordinate with their ISPs to block packet floods using an anti-spoofing filter as part of the eradication phase of incident handling. Anti-spoofing filters set up "rules" of what is allowed in and out of the server. For instance, an ISP can set up a requirement to not allow anything in or out of their server that does not have the ISP's source address. Other rules, such as the one mentioned, can be used to prevent DDoS attacks.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

So what else can an organization do to protect its systems from a DDoS attack? As mentioned throughout this paper, following the steps of incident handling, beginning with the preparation stage of applying patches to operating systems and software and ensuring they are up-to-date, is the number one thing in preventing DDoS attacks. Another thing an organization can implement to protect their systems is the deployment of an IDS, which is also part of the preparation stage. Using the IDS, an organization can have it look for patterns that may indicate Trinoo or TFN activity is taking place based on the communication between the master and daemon portions of the tool. [8] Another preparation procedure an organization should take is to ensure their security policy includes an emergency contact plan in the case that the Internet is unable to be used because of the attack and network operators and the emergency response teams need to be contacted.

During the eradication stage of incident handling for a DDoS attack, an organization should try to capture a packet sample for analysis and preserve it as evidence. To capture a packet sample, it is recommended that an organization use a SUN workstation or a Linux box (as long as it is on a fast Pentium machine). The tcp dump program should be used for capturing a data with the command syntax:

```
tcp dump –i interface –s 1500 –w capture_file
```

The evidence should then be preserved in a secure location.[8]

If an organization finds a distributed attack tool on their system, they should first determine the type of tool that has been installed. The tool that is found can possibly provide information to help locate the other parts of the distributed attack, which then can be disabled. Determining the type of tool and locating the other parts are part of the identification and eradication stage of incident handling.

Code Red

Code Red, a worm that caused a buffer overflow in Microsoft's Internet Information Server (IIS), occurred in July 2001. Code Red demonstrated to the IT community that the IIS web server may not be obvious to the everyday user because of being used as personal web servers on an intranet, which the everyday user does not realize is still connected to the Internet. [9] Code Red has been used as an example as a possible terrorist attack, showing how fast our systems could be possibly taken down.

Code Red could have been prevented using the preparation phase of incident handling by keeping patches up-to-date. A patch for IIS was released by Microsoft a month before the attack to fix this vulnerability, but many companies did not install the patch due to a lack of publicity.[2] Microsoft's IIS is embedded in the Internet Explorer browser and the Windows operating systems, Windows 2000 and XP. The IIS requires the installation of numerous patches to keep the server secure. A patch is released almost every week for IIS on Microsoft's website.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Personal computers running the Internet Explorer browser, IIS Web servers, or Outlook Express must install every patch and service pack as soon as they are released.[9] System Administrators often use the auto install option provided with the service pack and or updates, which will not always apply to their servers, it is highly recommended that they manually go to the Microsoft site to download and install patches that apply directly to their systems. It is imperative that security patches are kept up-to-date, tested, and applied immediately after their release. Code Red led the IT industry to release patches faster, without compromising the quality of the patch.[2]

More than 250,000 Web servers were affected by Code Red in less than nine hours.[2] Code Red propagates itself over TCP/IP connections. It randomly picks IP addresses and then checks to see if those systems have Microsoft's IIS. If the system has an unpatched and unprotected Microsoft IIS, it will embed itself in the system. The worm is controlled by the system's date. From the 1st to the 20th of the month, the worm spreads, and then from the 20th to the 27th, the worm directs PCs to launch a Denial of Service (DOS) on the U.S. White House's website. Hackers have been known to use the Code Red worm to identify computers that have vulnerabilities in their IIS. Once the hacker has determined they system is vulnerable using the worm, he then can obtain control over the system.[10]

A possible solution of mitigating the risk of viruses such as Code Red is to place honeypots in the server infrastructure. A honey pot is a computer system on the Internet that is expressly set up to attract and "trap" people who attempt to penetrate other people's computer systems [11] Honeypots are not a solution to protecting a system, but they are a tool to help mitigate risk, and should be implemented in the preparation or follow-up phase of incident handling (the particular phase depends on whether an attack has already occurred). They are a good tool to use because they do not require a lot of bandwidth since they only collect data that comes to them. However, the data they do collect is very valuable. They are especially valuable for capturing information from automated attacks. System administrators can use the information that is collected from honeypots to reduce the vulnerability of their system. Honeypots can be as complex as desired, but the more the honeypot can do, the more risk that is accepted.[12]

Many important security lessons were learned from the Code Red attack. Along with the importance of keeping security patches up-to-date and using honeypots for research, the need for coordinated response was demonstrated. As part of the identification phase of incident handling, communication lines and reporting capabilities should be in place to prevent any delay in broadcasting that an attack has occurred. As mentioned later in this paper, there are organizations that post alerts and have information on how to report an incident. Although many lessons have been learned from Code Red, the worm will continue to attack until all the vulnerabilities in Microsoft's IIS are patched.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Nimda

Nimda, a multi-exploit worm, occurred in September 2001, only one week after 9/11. Nimda attacked Windows environments by attacking the Unicode Directory Transversal vulnerability of Microsoft's IIS, and the Multipurpose Internet Mail Extensions (MIME) vulnerability of Microsoft's Outlook, Outlook Express, and Internet Explorer. The worm adds JavaScript to web pages served by infected servers. When visitors go to the infected page, Nimda is automatically downloaded to their computers as an embedded Microsoft Outlook file called "readme.eml." This .eml file will cause the Internet Explorer browser to view the message, which will cause the readme.exe file to execute. The virus will then spread by email as an attachment called "readme.exe".[13] If the receiver of that email uses an Internet Explorer based email client, Microsoft Outlook, or Outlook Express, it will automatically execute the attachment "readme.exe" of the unusual MIME type "audio/x-wav" to infect the system.[14]

Nimda affects a system in a few different ways. It opens the system to outside access making the system very vulnerable to attacks. Nimda also modifies the boot sequence to include the worm. This means the worm is executed every time the system is booted up. A third affect of the system is that it opens network shares. Nimda will create or activate "Guest" accounts with administrative rights.[14] Once a guest account is created with administrative rights, it gives access to hackers who then have the ability to do whatever they want to the system.

The attack of Nimda is what brought public awareness to containment phase of incident handling. Without incident handling, the spread of this attack could have caused severe problems. The need for strong and navigable links between incident handling capabilities and network management personnel became apparent during Nimda. The link is important because once a worm is discovered filters need to be deployed throughout the Wide-Area Network (WAN) to prevent the worm from spreading to other servers and users as part of the containment phase of incident handling. A full security audit should then be done to check for any other security vulnerabilities, as part of the follow-up phase.[2]

U.S. Government's Role in Preventing Cyberterrorism

Although an attack on the Government's systems is not as likely as an attack on the private sector, there is not much the Government can do to protect the nation against a cyberterrorist. In fact, regulatory agencies, both public and private, find themselves in a precarious situation. Because of the severely global nature of the Internet, international regulations are hard to develop. Hence, governments are forced to take a more reactive, as opposed to pro-active, role in network security systems. While the government understands the importance of the preparation stage of incident handling, and invests heavily in it, lawmakers also realize the necessity of the following five steps that take action after an attack has occurred.

Before, but especially after, the September 11th attacks, the need to protect both private and public sector computer systems against terrorism became apparent.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The Government created a National Advisory Panel to Assess Domestic Response Capabilities for Terrorism to approach this issue. In September 2001, Chairman James Gilmore stated that the U.S. Government would have difficulty enforcing laws regarding the Internet because of its global nature. It is also argued that enforcing regulation of the Internet would also impede on the civil rights of the American citizens. [15]

Currently the Federal Bureau of Investigation (F.B.I.) uses a system called Carnivore (subsequently renamed "DCS1000") that monitors Internet communication. This system uses a combination of hardware and software that connects to an Internet Service Provider's (ISP) network to track all the communication on that network. This system is able to single out electronic traffic of one person who is under investigation. It then can listen to every word passing through the ISP. Carnivore can also be used as a sniffer for surveillance. However, in order to use the system, the F.B.I. must have court orders and proof that the person needs to be under investigation. Many ISPs fight court orders allowing Carnivore to be connected to their servers because it violates their customers' privacy for the benefit of catching only one person. Since it does violate a civil right of U.S. citizens, the Government is hesitant to use a system of this nature.[16]

The U.S. has spent billions of dollars on protecting its systems. After September 11th, President Bush allocated a record amount of money to help improve and protect not only the Government's systems, but also to educate the private sector on how to protect their systems. Although the money has been allocated, it will still take a few years to get the systems up to speed to the point that attacks will not be as devastating. Recently, the government released "The National Strategy to Secure Cyberspace" to "engage and empower Americans" to secure their part of the Internet which they control, operate, or interact with. The Government believes that in order to secure the cyberspace that the country uses, a coordinated effort is necessary.[17]

An organization sponsored by the National Information Protection Center, which is part of the F.B.I, called InfraGard has been formed for federal agencies to help companies that have come under a cyber attack. It provides a forum to exchange information on computer crime, a service that is beneficial to both the identification and follow-up phases of incident handling. [18] The goal of the organization is "to provide better protection for all of corporate America and our critical information infrastructure".[15] This organization started in 1996 and continues to grow. It was an important step for the Government to take due to many Government systems' interconnection with private systems. A partnership of the private sector and Government helps both parties fight against cyber attacks. On the InfraGard website, www.infragard.net, agencies and companies have the ability to report an incident. If the incident could possibly occur on many systems, an alert can be distributed to inform other members of InfraGard. This organization was definitely

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

a step in the right direction for the Government and private industry to help fight cyberterrorism.[17]

Conclusion

Incident handling was a security procedure many company executives overlooked, but not anymore. Companies are beginning to realize what is at stake, not just financially, but also in proprietary information, if an attack were to occur on their systems. Security policies are beginning to be kept up-to-date, system inventories are being made, and incident response teams are being formed. Companies are beginning to protect their systems from the ground up and are keeping their systems up-to-date under the principles of incident handling.

Cyberterrorism is real and the only way to prevent the attacks from being catastrophic is to have an effective and well-rehearsed incident handling procedure in place. With the tumultuous political and financial state of the world today, it is inevitable that attacks on cyberspace will continue, but with preparation and effective incident response, hopefully attacks will not be as devastating as in the past.

Previous cyber attacks have provided information on how to protect from future attacks, and in each instance, incident handling has proven useful. Although the IT community has learned from these previous attacks, many security professionals believe the attacks of the future are going to be worse. However, taking what a company learns from handling an incident will continue to make systems stronger and in turn, help fight cyberterrorism.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

List of References

1. Author Unknown. "Deception and Perception Management in Cyber-Terrorism". Fred Cohen & Associates. Date Unknown.
   URL: http://www.all.net/journal/ntb/terror-pm.html

2. Skoudis, Ed. "Infosec's Worst Nightmares". Information Security. November 2002: 38-49

3. Allen, Julia. CERT Guide to System and Network Security Practices. Boston: Addison-Wesley, 2001.

4. Horgan, Daniel. "Five Thoughts About Cyberterrorism". CNN.com. October 30, 2001.
   URL:
   http://www.cnn.com/2001/TECH/internet/10/30/cyberterror.thoughts.idg/index.html

5. Fogie, Seth and Cyrus Peikari. Windows Internet Security. Upper Saddle River: Prentice Hall, 2002.

6. Unknown Author. "Distributed Denial of Service Tool." CERT Incident Note IN-99-07. January 15, 2001.
   URL: http://www.cert.org/incident_notes/IN-99-07.html

7. Unknown Author. "User Datagram Protocol." Webopedia. December 10, 2002.
   URL: http://www.webopedia.com/TERM/U/User_Datagram_Protocol.html

8. Dittrich, Dave. "The Distributed DoS Attacks." Washington University website. July 22, 2000.
   URL: http://staff.washington.edu/dittrich/talks/sec2000/how.html

9. Prescator, John. "Commentary: Another worm, more patches." Gartner Viewpoint. September 20, 2001.
   URL: http://news.com.com/2009-1001-273288.html?legacy=cnet&tag=nbs

10. Author Unknown. Untitled. Frisk Software International. August 7, 2001.
    URL: http://www.f-prot.com/virusinfo/redcode.html

11. Author Unknown. "Honeypot." SearchSecurity.com. April 6, 2002.
    URL:
    http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci551721,00.html

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

12. Sptizner, Lance. "Honeypots and Value of Honeypots." May 17, 2002.
URL: http://www.spitzner.net/honeypot.html

13. Heng, Christopher. "Nimda Worm/Virus: What are Cmd.exe, Readme.exe, and Root.exe?" September 26, 2001.
URL: http://www.thesitewizard.com/news/Nimdaworm.shtml

14. Mackie, Andrew, Roculan, Jensenne, Russel, Ryan, and Van Velsen, Mario. Nimda Worm Analysis. 21 Sept 2001. Attack Registry & Intelligence Service.
URL: http://aris.securityfocus.com/alerts/nimda/010919-Analysis-Nimda.pdf

15. Garretson, Cara. "US Commission Examines Cyberterrorism". CNN.com. September 18, 2001.
URL: http://www.cnn.com/2001/TECH/industry/09/18/cyberterrorism.idg/index.html

16. Wingfield, Nick and Don Clark. "ISPs Bite Back at Carnivore". The Wall Street Journal Online. July 11, 2000.
URL: http://zdnet.com.com/2100-11-522107.html

17. Author Unknown. "The National Strategy to Secure Cyberspace." White House Online. February 2003.
URL: http://www.whitehouse.gov/pcipb

18. Author Unknown. "About Infragard". Infragard Website. January 19, 2003.
URL: http://www.infragard.net

© SANS Institute 2003, Author retains full rights.

Last Updated: April 28th, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS