Global Information Assurance Certification Paper

Thomas Davis

GIAC Security Essentials Certification Practical Assignment
Version 1.4b, Option 1

A Manager's Guide to Understanding and Utilizing the Variety of Available Security and Advisory Sites

Abstract

The networking aspect of the internet has fostered the development of worms, viruses, and other exploits that are targeted to impact certain systems and applications. The internet community responded to these threats by organizing information and developing internet security sites that were designed to be accessible repositories of information about threats. The proliferation of threats has led to more and more information that people both need and want. The increase in the number of these security sites has led to a mass of information that can be confusing and overlapping. A brief discussion about these sites is given and is followed by a brief history. Those sections are followed by a description of the information that sites have evolved into carrying. Included is an explanation about the introduction of sector specific information and advisory sites (ISACs), as well as recent changes to the Department of Homeland Security.

The advisory or security sites are a necessary tool for all mangers to use, yet there is no simple answer as to how to best use them. By understanding the history of the sites and the types of information available, guidelines can be given to assist in obtaining the most effective information.

1. Introduction

The internet provides connectivity throughout the world. Along with the connectivity, comes many capabilities. The internet has become the de facto tool for both personal and business use throughout the world. The internet is now the standard medium to distribute and share information.

Those desirable characteristics of connectivity and data sharing are the same characteristics that allow malicious code to be easily propagated. Typical of these sorts of code are viruses, worms, and other exploits. The increase in the rate of new incidents is tremendous as shown by CERT's statistics concerning reported incidents.

1988-1989

Year	1988	1989
Incidents	6	132

1990-1999

Year	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999
Incidents	252	406	773	1,334	2,340	2,412	2,573	2,134	3,734	9,859

2000-2003

Year	2000	2001	2002	1Q-2Q 2003
Incidents	21,756	52,658	82,094	76,404

Total incidents reported (1988-2Q 2003): **258,867**

Please note that an incident may involve one site or hundreds (or even thousands) of sites. Also, some incidents may involve ongoing activity for long periods of time. (www.cert.org/stats/)

The intent of the malicious code varies tremendously, ranging from nuisance issues to national security issues. The dollar costs of just cleaning up the nuisance exploits are tremendous. The actual Dollar impact of the result of the exploits is also tremendous.

A Cnet News Article in January of this year outlined the cost of the cleaning up some of the more recent exploits.

> On Thursday, London-based market intelligence firm Mi2g said that the worm caused between $950 million and $1.2 billion in lost productivity in its first five days worldwide. That puts the worm at No. 9 on the company's list of the most costly malicious code, behind the likes of the Code Red worm, with its average of $2.6 billion in productivity loss; the LoveLetter virus, with $8.8 billion; and the Klez virus, with $9.0 billion. (Lemos,news.com.com/2100-1001-982955.html)

The problem grew to become significant enough that security focused organizations were formed and internet security sites were developed to help manage the problems

created by exploitive code. Today there are many organizations and their focus may vary depending of their goals. In general, there seem to be interest groups that grow into organizations and the organizations then use the advantages of the internet to share information and to promote the particular organizations. Some sites are designed to assist particular industry sectors, while others are targeted to assist general automation interests. Many sites targeting many unique interests are now available.

Raising the internet security stakes further, is the wide spread use of the internet by infrastructure providers whose services are vital to maintaining the stability of the operation of this and other countries. In a recent announcement of a new division, Secretary Ridge of the Department of Homeland Defense highlighted the critical nature of providing cyber security, noting that it can not be separated from the delivery of critical infrastructure.

> Cyber security cuts across all aspects of critical infrastructure protection. Most businesses in this country are unable to segregate the cyber operations from the physical aspects of their business because they operate interdependently," said Secretary Ridge. "This new division will be focused on the vitally important task of protecting the nation's cyber assets so that we may best protect the nation's critical infrastructure assets.(http://www.dhs.gov/dhspublic/display?content=915).

Clearly security is important and today it is impossible to have secure internet connected computer systems without devoting resources to security. The security situation is very dynamic and the internet security sites offer the best and most timely information about security. They are mandatory tools for people at different levels in automation sections. The sites and information are no longer limited to the “techies”, as the sites also provide a wealth of useful management and guidance information.

The key is to understand the types of security information that are available and then in selecting and using the most effective sites. Sector specific sites or vendor specific sites may not be your best choice. This paper will provide guidance in working through the information by presenting a brief history of the development of the sites, an evolution of the security information that has become available, and finally some recommendations on how to best use the available information.

2. History

Writing code came with computers, and it was clearly an intellectual exercise in problem solving. Through intellectual exercises, challenges, and informal games, exploration of self replicating code and other coding exploits evolved. Some of these exploits were later used for malicious purposes and interconnected systems became the tool to propagate these exploits.

The internet originated as an outgrowth of the networking efforts of a research wing of

the military community in the US around 1969. The expansion of the concept was supported through a number of schools and other educational and research groups. The concept continued to spread and resulted in growth at an exponential rate. The number of hosts on the network broke 1000 in 1984, 10,000 in 1987, 100,000 in 1989 and 1,000,000 in 1992.

The growing capabilities as well as the interconnectivity of the internet made it a very attractive medium for distributing and sharing all types of information by all types of users. Exploits were developed in the 80's and were propagated by file sharing on some of the bulletin board systems. Compilations of known problem files were created and shared. As the internet grew, it provided a richer environment than the BBSs for the spreading of exploits.

> In 1986, the first well-publicized international security incident was identified by Cliff Stoll, then of Lawrence Berkeley National Laboratory in northern California. A simple accounting error in the computer records of systems connected to the ARPANET led Stoll to uncover an international effort, using the network, to connect to computers in the United States and copy information from them. These U.S. computers were not only at universities, but at military and government sites all over the country. (Longstaff).

"In November 1988, a computer security incident known as the "Internet worm" brought major portions of the Internet to its knees. Reaction to this incident was isolated and uncoordinated, resulting in much duplicated effort, and in conflicting solutions. Weeks later, the CERT Coordination Center was formed". (http://www.first.org/about/first-description.html).

Early the following year, through the efforts of people in the Department of Energy, CIAC, The Computer Incident Advisory Capability was formed "to assist their sites with events, such as hackers, viruses, and worms, for both classified and unclassified computer systems". (www.ciac.org/ciac/ciac_timeline.html).

These organizations were focus points for the sharing of information about new exploits and for coordinating a team response to problems.

Initially, coding exploits were seen as an annoyance, yet the risk to the systems on the internet was recognized and response systems developed.

3. Evolution of Organizations, Sites, and the Information they carry

The early advisory sites started as a response to a threat. In response to the increases in the variety and types of threats, the newer sites that have since developed, offer a much broader range of information. Today the sites are sponsored by a variety of providers and the sites tend to offer information that track the sponsors interests. Some sites are provided by commercial providers, some by government, and some by interest groups.

It is import to understand the offerings in order to make the best use of the information that is available. The offerings include information about response teams, vulnerabilities, hoaxes, virus information, general and specific advisory information, best practices, general practices, resources, training, and statistics. The sites, while being independent, tend to have some of the same information but organized in different fashions.

Virus Information

Viruses are rampant and cause a tremendous amount of damage every year. Viruses vary in the speed that they spread, the types of systems they infect, the amount of damage they do, the methods to fix them and their impact to the internet itself. Viable Anti-Virus software vendors support and maintain sites to assist their customers. Generally, detailed information is also available to the public about particular viruses. Anti-virus software updates are often available for downloading, although most sites that have an anti-virus program automatically receive updates.

Response Team Information

A response team is a group of people that work together to resolve some sort of incident. Typically, these groups are called CSIRTs (Computer Security Incident Response Team). The organizational structure and duties of a team are determined by the sponsoring entity. State and larger local governments, larger companies, and educational facilities may have organized teams. Some teams are only activated when necessary, while a larger organization may have a full time, dedicated team. Advisory sites are great sources of information for starting and managing teams. The value of this information is less dynamic than much of the other information on these sites.

Training Information

It became apparent that internet security issues were complex enough and that the base of knowledgeable people was so low, that organizations began offering training. Virtually every security site offers courses or at least some information about training. Again, while this information is valuable, it is less dynamic than other information on these sites.

Vulnerabilities information

Applications, operating systems and computer hardware are very complex items. While a lot of testing of software occurs, it is often released with problems. Those problems are often recognized by earnest users or they maybe even be exploited by malicious coder writers. Many sites offer a running list of currently known vulnerabilities, as well as archives of past vulnerabilities.

Fixes, Patches, Releases Information

When companies recognize problems with their software, they will often develop fixes for those problems. These fixes are often incorporated into the next version of their software. Sometimes problems are exploited by writers of malicious code, and a software developer is forced to quickly develop patches or fixes to resolve vulnerabilities. Many advisory sites offer a running list of patches, fixes or releases of particular software applications and operating systems.

Hoax Information

Hoaxes are spread via the internet, typically via email, and advisory sites have either developed or have devoted space on their sites to share information about hoaxes. These sites are repositories for specifics about hoaxes and also give information about dealing with hoaxes.

Best Practices Information

Over the years guidelines for minimizing risk to systems and data have been developed. These have been compiled and are available at some sites and are typically known as “best practices”.

Advisories, Bulletins, Reports, and Alerts Information

This group of offerings is on many sites, and can mean many different things. In general, they offer information about “late breaking” situations that might include any sort of threat or fixes for threats. This group tends to present “current events” type information and is less focused on particular types of threats. Some security sites have more granular breakdowns of events and issues based on the time sensitivity of the event. In other words, a fast spreading virus would be on their highest importance section.

Statistical Information

Advisory / security sites have evolved into gathering statistical information. The information gathered includes such areas as the number of viruses, the speed of the spread of particular exploits, internet traffic measurements, internet speed measurements, most attacked ports, types of attacks by continents, top attackers, the percentage of dropped packets, and the list goes on. Selected information is sometimes combined to show things such as the impact the spread of a particular virus has on the traffic on the internet.

Distributed Intrusion Detection Information

In general, intrusion detection is a process to detect unauthorized attempts to access

the resources within your system. Often a pattern matching process is used to recognize the attempt. One security site receives data from distributed clients about the unauthorized access attempts, and then compiles, analyzes and presents the data.

Wireless Information

Wireless is a relatively new technology for accessing the internet. The use of wireless raises the risk of having your system exploited by uninvited guests. Security issues concerning wireless access are evolving quickly and special interest sites are a great source for up-to-date information.

Sector Specific Information

In 1996 The President's Commission on Critical Infrastructure Protection recognized the critical nature of the infrastructures that this country relies on. Their report recognized that responsibility for reliable operations lay with both the public and private sector. Their report formed the basis for the Presidential Decision Directive – 63 (PDD-63) which recognized that sectors of the economy were critical for the country and that each of the eight named sectors should form information sharing and advisory centers (ISACs). This was further extended by President Bush in a later executive order. The named sectors somewhat coincided with the main Federal Government agencies, and encompassed commerce, finance, transportation, water, law enforcement, fire services, health, and energy. Sub sectors within each of the main sectors were also allowed to form ISACs. As an example, both aviation and surface transportation have ISACs and they both fall under one of the named main sectors, transportation which coincides with a Federal Agency.

After September 11th

As has been shown, since the formation of CERT and CIAC the information and the availability of information about exploits has dramatically increased. Further the increase in the critical dependence on the internet has been recognized by government and political leaders. The critical dependence issue and the vulnerability to exploits were brought to a head by the terrorist attacks in 2001. Since that time the Federal Government has been reorganizing to better respond to terrorism and terrorism issues; eventually culminating in the formation of the Department of Homeland Security. This reorganization and consolidation of departments has also affected the security and advisory sites that were and are being made available. In June of this year, a new division was created within the Department of Homeland Defense called the National Cyber Security Division (NCSD). This division is charged with identifying threats and vulnerabilities, along with sharing information about and coordinating responses to threats. The Division is to be a consolidation of resources and responsibilities. It appears that the new division will continue to work through the sector structure that was established earlier on.

4. Recommendations

I have outlined some of the basic offerings by security / advisory sites that are ready and willing to share information. I have also outlined the processes that resulted in the sector specific ISACs that have and are being created. I also touched on the changes in the government that continue to affect the sector specific ISACs. The dynamic information that is available from these security / advisory sites is necessary for anyone that has vital resources connected to the internet. These internet security / advisory sites offer the most practical approach to obtaining accurate information in a timely manner.

The goal is to insure that staff has accurate, timely information available to them. It is the manager's job to insure that the goal is met. In simple terms, know your company in depth, know the information that is available, and get the people and the information together. Obviously this is not magic, but it takes an investment of time and effort.

In broad terms, the majority of the available information is Information Technology (IT) specific and of little interest to upper management, so it makes sense to start there. The general approach is to 1.) Require your staff to obtain information from different security sites, and 2.) Assure yourself that they truly know about the sources of information. One way to do this is by sitting down with staff and getting them to explain the information they find, and where they find it. On the one hand this approach may seem simplistic and on the other it may seem awkward for larger companies with very structured organizations. For the more structured organizations the principle still needs to be met and can be accomplished in other ways. For smaller, less structured organizations, the manager sitting down with working staff is always good.

An anti-virus program in some form is a necessary part of automation. There seems to be no way to avoid viruses, so entities need to be proactive. Your anti-virus program manager needs to use the available sites to keep abreast of viruses. Additionally, the sites should be used to obtain detailed reference information about particular viruses, but beware that all sites do not agree and good information can be found by using multiple sites. Do two things: 1.) the next time a virus issue crops up, ask your person to get you the procedure to fix the problem from two different sites, and 2.) sit down with them and ask them to explain the process, the differences in the processes, and where the information was obtained. The Symantec site, www.symantec.com and the McAfee site, www.mcafee.com are good places to start when looking for anti-virus information.

Staying current with software patches, fixes, and new releases is consider by some to be the primary method to avoid security problems. Others consider a more measured approach of reviewing the impact and purpose of patches, fixes, and new releases. Regardless of the merits of either approach, somebody in your business or agency should be given the responsibility to keep current on the products used at your sites. Again, sit down with the appropriate staff and discuss strategies and sources of information. Are they notified when vulnerabilities are discovered? Are they working with lead vendors? What release are you at? What is your patch strategy? Who and

how are people notified of fixes and patches? For this category, your staff should have access to the vendor supported sites. Lacking specific vendor information, the Info system security web site, www.infosyssec.com, lists a number of sites for information from particular vendors.

Hoaxes while not obviously damaging are in fact a problem. Users run into hoaxes everyday and waste both personal and corporate time and resources in responding to hoaxes. The advisory sites are useful tools for either the users or the staff that end up responding to the concerned user. This should be handled via assigning it as a staff responsibility and by user education. The hoax section on the CIAC site, hoaxbusters.ciac.org, is a good place to start when looking for information about hoaxes.

Evolving technologies like wireless security can be difficult to track and targeted sites can provide a wealth of information. Sites with information about evolving technologies should be routinely accessed by systems people. Sites with information concerning best practices should also be routinely used by systems people. Again, you need to insure the information is getting to the appropriate staff. The Computer Security Institute

You as a manager need to stay current with the sector specific information. Sector or industry specific advisory sites are useful in a variety of ways. They can be used as educational tools for showing upper management the need for investing in security, and they can show how competitors are also taking security seriously. Technical staff can also benefit from sharing knowledge with like institutions. Some upper management may want to receive routine security advisories from sector specific sites. Providers of critical infrastructure that should be participating in sharing with like sector providers, need to stay current the Department of Homeland Security changes. In addition, they need to be aware of the sites that are specializing in their sector. Seek information about sector specific sites from counterparts in other organizations and from industry web sites. The Department of Homeland Security site, www.dhs.gov , and the New York State Cyber Security and Critical Infrastructure Coordination site, www.cscic.state.ny.us/related.htm are good places to start when looking for sector specific information.

Training resources and incidence response team information is not as dynamic as the other types of information that I have covered, but the security sites are very good resources for information. The security sites should be reviewed before making decisions in this area. The SANS site, www.sans.org and the CERT site, www.cert.org are good places to start when looking for training and response team information.

Statistical information is useful for both management and IT staff. The statistics can be used to support program needs as well as help in determining expenditures. It is better to spend money on the most frequent exploits than the least frequent. It is also educational information for IT staff. The SANS site, isc.sans.org, and the Internet Traffic Report site, www.internettrafficreport.com/main.htm, and the Dshield site,

www.dshield.org, are all places to start when looking for statistical information.

Remember there is no real magic, rather it is a matter of learning what is available and then applying good basic management practices. In summary;

A. Understand the information that is available
B. Insure that responsibilities are defined
C. Insure that the responsible staff is aware of the information
D. Insure that the responsible staff effectively use the information
E. Insure that upper management is aware of useful information

References:

Carnegie Mellon University, "CERT/CC Statistics 1988-2003" July 15, 2003
URL: http://www.cert.org/stats (07/18/2003)

Robert Lemos, "Counting the cost of Slammer" CNET News, January 31, 2003.
URL: http://news.com.com/2100-1001-982955.html (07/18/2003)

Office of the Press Secretary, U.S. Dept. of Homeland Defense, "Ridge Creates New Division to Combat Cyber Threats", June 6, 2003
URL:http://www.dhs.gov/dhspublic/display?content=915 (07/18/2003)

Robert Zakon, Hobbes' Internet Timeline v6.0"
URL:http://www.zakon.org/robert/internet/timeline/ (07/18/2003)

Sarah Gordon, David M. Chase, "Where there's Smoke, There's Mirrors: The Truth about Trojan Horses on the Internet", October 1998
http://www.badguys.org/smoke.htm (07/15/2003)

Thomas A. Longstaff. James T. Ellis, Shawn V. Hernan, Howard F. Lipson, Robert D. McMillan, Linda Hutz Pesante, Derek Simmel, "Security of the Internet"
URL:http://interactive.sei.cmu.edu/Features/1998/December/Background/background_dec98.pdf (07/18/2003)

Unattributed, CIAC Forum of Incident Response and Security Teams", May 7, 2002
http://www.first.org/about/first-description.html (07/15/2003)

James R. Lindley, "A Short Narrow Look at the History and Purpose of Information Sharing and Analysis Centers" January 10, 2000
https://www.it-isac.org/isacinfowhtppr.php (07/16/2003)

David Schwoegler, LLNL “Ten Years of CIAC” 1999
http://www.ciac.org/ciac/ciac_timeline.html (07/18/2003)

Unattributed, “History”, National Infrastructure Protection Center
http://www.nipc.gov/about/about3.htm (07/18/2003)