Global Information Assurance Certification Paper

Bricks In The Security Wall

Edward Moe

May 1, 2003

INTRODUCTION

Turn on your television or the car radio, browse your favorite paper or Web site, and you're likely to hear or read about a new virus, or a computer system break-in. The importance of Information Security was brought to our attention once again with recent attacks on the E-commerce and E-banking/finance community within the United States. "The Federal Bureau of Investigation (FBI) disclosed that it has launched investigations into alleged hacking incidents by Eastern European organized crime groups in 20 states. These groups are believed to have stolen more than 1 million credit card numbers from E-commerce and E-banking/finance Web sites using Windows NT servers".

These attacks on the computing community should not come as a surprise. Instead they have now become a daily occurrence. A recent survey by The Computer Security Institute (CSI), " 2001 Computer Crime and Security Survey " shows us some interesting facts. Of the 538 responses:

85% - (primarily large corporations and government agencies) detected computer security breaches within the last twelve months.
64% - acknowledged financial losses due to computer breaches.
40% - detected system penetration from the outside (only 25% reported system penetration in 2000).
70% - cited their Internet connection as a frequent point of attack as compared to 31% for their internal systems.

These are just a few of the findings, the rest of the survey can be view at their Web site (http://www.gocsi.com/). Even the few specifics listed above should have anyone responsible for computer system security thinking about a few very big questions. The first one being, not, will the computer system be attacked or compromised? But, when will, or has the computer system been attacked or compromised? Somewhere, somehow, you can probably count on the computer system being attacked. The attack may not come from the outside by an Eastern European crime group, but maybe from the inside by a disgruntled employee of the company. Let us not forget about those nasty viruses that make their way around the company E-Mail system. I don't know of anyone who loved the "I Love You" virus. The other questions deal with two parts of information security, protection and detection. What can be done to help protect the computer system? Also, What can you do to detect if the computer system has been compromised? The answer to last two questions is a never-ending, always learning, 24 / 7, 365-day job. If you happen to be new at this, it's like

staring at a 10-foot brick wall with no way around, and no ladder in sight. So in all reality the biggest question of all is, Where do you begin?

THE LADDER

With the different Operating Systems (OS) and all the different aspects of protecting a computer system, there is no way to present all of the information here. That is not to say computer systems cannot be protected, they can be and should be. You wouldn't leave your car unlocked with a note on the windshield saying the keys are inside would you? The hope is in providing information to get you thinking about or started in Information Security, or finding the ladder.

No matter what kind of computer system you are responsible for, you need to gather information. The old adage knowledge is power is true. You can be sure the bad guys are gathering all the information they can, and you need to do the same. Not only will gathering all this information keep you abreast of what is happening in the computing community, hopefully it will also make your job a little easier. Okay, now you are probably asking how can you go about finding all of this useful information right? With all the information that is available at the click of a mouse button or a few keys stokes, the Internet is a good place to start. Go to your favorite search engine and do a search on the type of OS you have and don't be surprised at the results, there are hundreds of Web sites to pick from. So what kind of information should you be looking for? Try and locate some sites that will provide information on what kind of exploits are being attacked, or if new exploits have been discovered. You also need to learn what kinds of viruses are being introduced into the computing community. If you don't know where the holes are in the operating system, or what kinds of programs are being used to enter these holes, and which new viruses are making their way around the network, how can you expect to protect yourself against them?

There are a lot of good Web sites out on the Internet dealing with security issues. Locate the sites that can supply you with the information you need and visit them frequently. A few that come to mind are SANS, Windows IT Security, Ntbugtraq and CERT a center of Internet security expertise. Many of these sites offer bulletins, and/or news stories and other related security information. Subscribe to the security bulletins, or newsletters, maybe join a discussion forum, the more knowledge you can gain is certainly a plus for you. There are some other sites you might want to checkout also. Why not visit the same Web sites the people causing all these problems visit. You have probably heard about a hacker Web site or two, go take a look, it can be a real eye opener.

Along with gathering all this information on what the bad guys are doing, you also need to keep informed about security information being offered by your software vendors. Remember, when you are being attacked they to are also being attacked. They should be working just as hard to bring you a secured product as you are at securing their product. These sites are a good place to pickup how to information on securing their software. When a new exploit is

discovered or a virus makes its' way around the network, software company Web sites are a good first place to look. Sometimes the software vendors can provide a wealth of information on a fix or help with a virus or security breach. They may also offer patches or software upgrades to close the holes found in their software.

The Internet is not the only resource you have available to find the information you need. Let's not forget there are a lot of good books and magazines out in the market place. Learning all you can about what is taking place in the computing community is only a small part in protecting your computer system, and it is a part that should not be over looked.

MONITORING YOUR WORLD

Now that you have seen all of the disastrous events taking place out in the computing world, you will need to monitor your computer system to see if the same events are or have been taking place in your computing world. A White paper from Microsoft entitled "Monitoring and Auditing for End Systems" states, "The general goal of monitoring is to detect suspicious behavior by external users or employees, or malfunctions. An organization can do this directly, such as by monitoring for specific events, or indirectly, such as by watching the state of the server over time and investigating anomalous behavior". The first part of that statement is what you should focus on, do not think of it as an option, you need to monitor your computer system. Usually the operating system generates log files of system activity, and the best way to observe any suspicious activity is to review these log files on a daily basis. Notice I didn't say weekly or monthly, the quickest way for you to squash an attack or discover any unwanted activity on your computer system is to make viewing the system logs part of your daily routine.

Windows NT has three different kinds of event logs in which it records any significant event that does not require immediate attention. They are the system log, the security log, and the application log. You can pretty much tell what type of events the log file collects by its name. System component events, like the failure of a driver to load are logged in the system log. The application log of course, logs events related to the system applications. The security log is the log that should draw most of your attention. Events recorded in this log deal with security issues such as user logons and resource usage such as creating, opening and deleting of files. This is the place to look for any unwarranted system activity like unusual logon hours, or a large number of invalid password events possibly indicating a password cracking program might have been ran on the computer system. Now all this does not just happen by magic, in Windows NT, event logging does start automatically each time you start the machine, but "by default, security logging is turned off and must be enabled". This means that the system logs will have to be configured and must also be managed.

Configuring the system logs could be as simple as making sure that event logging is active, and setting up which events you would like to be recorded in the system logs. Perhaps unsuccessful logon attempts to see who is trying to on

the system or maybe successful logon attempts to see exactly who did log on the system. File and/or directory auditing may need to be enabled, to see if someone is trying to view the CEO's files, or maybe they are trying to find out the salaries of all the employees that happen to be stored in the Accounting directory. These are just some of the issues, and should be evaluated on a company-by-company basis and must be setup or enabled to have events such as these recorded. Securing the system logs is also just as important as viewing them. Keeping records of system events does no good if someone can delete the log files. Along with making sure the log files cannot be deleted, only the appropriate personnel should have access to view the files. Another aspect of managing the log files is archiving them. The reasoning behind archiving the log files is twofold. First it gets the files off the system, once again this is protect the files from unwarranted access. Along with this, keeping the log files on the system takes up disk space. Log files can grow to be quite big, even in this day of large hard drives we still seem to run out of room. The second reason for archiving the log files is for research. The day may come when you need to go back to discover when and how an attack begun on the system, or maybe to research a company policy/legal issue.

JUST IN CASE

Most people carry insurance to ease their burden when life decides to throw a little disaster in their path. Just as in life, every organization knows they should carry insurance for when that little computing disaster is thrown in their path, and that form of insurance is of course called a backup. Having a current system backup has eased a countless number of burdens in the computing community. Backups offer you a form of protection not by securing a particular resource, but by hopefully giving you the ability to restore your computer system to a working state after a malicious attack or maybe a wayward user has render the system unstable. When performing backups, you must be aware of what is being backed up, and sure you are backing up everything you cannot afford to lose.

On a Windows NT system, along with a backup of the computer system, a current backup of the registry is a must. The registry is where the configuration information is stored and maintained and is not automatically backup by the Windows NT backup software. Therefore you must put forth the effort to make sure the registry is getting backed up. The Windows NT Resource Kit supplies to utilities to help you with this operation, they are called Regback and Regrest. Just as the names apply, Regback is used to backup the registry, and Regrest is used to restore the registry keys if necessary. This is just an example to point out that you must be attentive with your backup procedures, make sure they are being followed, and keep those backup procedures updated. So whether it is from firsthand experience or just because someone keeps telling you, we are all aware of how important it is to do those backups, just in case.

POINT OF ATTACK

Now that you have started your journey down the Information Security highway by gaining knowledge of what is taking place in the computing world, keeping an ever watchful eye on what transpires on the computer system, and making sure you have a little insurance with backups. I would like to offer you one more idea to think about. What would happen if you flip over to the other side of the coin? As an alternative of trying to provide security for your computer system, why not try and attack it. That's' right, take a break from those sleepless nights wondering if you have plugged the latest hole discovered in the operating system. Put that imagination of yours to work and start thinking like the bad guys. What better way is there to learn how vulnerable a computer system is then by attempting to exploit it yourself. There is also a great side effect to discovering the doors through which an attacker may enter, and that is all of the knowledge you will gain about how your own computer system operates.

If you are successful in making an entry into the computer system you have the opportunity to go on a fact-finding mission, see exactly how much information you can collect about the system, because this is what an intruder would do. Along with this, you will learn just how unprotected the system is by noticing all of the damage that could be inflicted. Uncovering all of the weaknesses in your computer system can be a bit scary, but you need to look that this as an asset. Now that you have seen what is vulnerable you can start to take the appropriate steps to help secure the company's resources. Your first step is to assemble a tool kit to aid you in your quest.

A good place to look for utilities is in the resource kit if your operating system has one. Software companies supply these utilities to help make administrating the computer system easier, and because they allow more control over the system, they are usually the tools of choice for intrusion into the computer system. Another good resource for tools of course is the Internet, there are a lot different utilities available, like password crackers, and TCP/IP port scanners. "A port scanner is a nifty little software tool that lets you probe a machine for all listening TCP/IP ports. You can easily find unwanted services, secret Web sites running on your employees' workstations (there's nothing like a little free bandwidth!), unwanted FTP sites, and many other oddities you don't want. On the other hand, port scanners are a vital part of the hacker's toolkit — yet another reason why they must be a vital part of your toolkit as well". Some of the utilities you find are free, and others you will have to pay for. The idea here is to know what types of tools are available, learn about their potential, determine their danger, and minimize the risk if used against your computer system.

SUMMARY

The four suggestions here are nothing but the tip of the iceberg in Information Security. As mentioned before the hope is to offer a stepping off point. The biggest problem is the starting, once you get going you will begin to discover all the aspects of securing a computer system. It can be quite a

challenging job, but so can scaling a ten-foot wall. Pick up the ladder and start your climb.

References.

Verton, Dan. "FBI investigating widespread Web site break-ins by crime groups".
URL: http://www.computerworld.com/cwi/story/0,1199,STO58395_nav47_sto58414,00.html

CSI/FBI Computer Crime and Security Survey 2001.
URL: http://www.gocsi.com/

Monitoring and Auditing for End Systems.
URL: http://www.microsoft.com/technet/security/monito.asp

Concepts and planning Manual, Chapter 9 monitoring Events.
URL: http://www.microsoft.com/TechNet/winnt/Winntas/manuals/concept/xcp09.asp

Edwards, Mark Joseph. "Attacking Your Own NT Networks." December 1997.
URL: http://www.windowsitlibrary.com/Content/121/09/toc.html

Last Updated: July 24th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	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 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
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 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 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 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
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
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor