Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Possible Points of Failure in the Information Security Environment

Working as a defense contractor, one knows the importance of security regulations and directives. However, do these regulations really protect our mission critical data?

Copyright SANS Institute

Author Retains Full Rights

AD

Possible Points of Failure in the Information Security Environment

GSEC Practical Assignment
Version (1.4b) Option 1

Marion Qualls
April 19, 2004

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Table of Contents

1.0 Abstract **3**
2.0 Introduction **3**
3.0 A false sense of security: Firewalls **4**
4.0 Lack of knowledge, experience and education: The Coffee Shop Graduates **8**
5.0 Patch Management **10**
6.0 Virus Protection **13**
7.0 The User Community **15**
8.0 Summary **16**
References **17**

© SANS Institute 2004, Author retains full rights

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

1.0 Abstract

Internet connectivity has become a common household service over the last ten years, from dial-up to broadband. This connectivity has come at a cost to the business world. It has exposed many vulnerabilities in various systems, so that a person with the intent to cause information disruption and damage now has the tools at their disposal. Precautions have been taken by most, but oversights and misconceptions are still prevalent throughout the information industry. I touch upon several of these points, illustrating areas where failure might occur but can be minimized with the application of a Defense In-Depth approach to security.

2.0 Introduction

In the early 1970's through the mid-1980's, the Information Technologies (IT) industry was comprised mainly of stand-alone systems with a specific function. As components were reduced in size and systems increased in computing power, people realized that a system could be utilized for multiple purposes simultaneously. The next logical step was to connect all of these various systems together to exchange information, increasing job efficiency. At this point the information world should have been a utopia; as with all things, there is bad that comes with the good. Some individuals were not content to have an infrastructure in place that would benefit humanity. Emerge the Hackers. The hackers take great joy and pride in trying to bring IT infrastructures to their knees. They have no concern about hacking's impact, only that they achieve their goals, which could be retaliation for offenses, monetary gain, or espionage.

The Information Technologies industry was forced to address this seriously growing problem and come up with a defense mechanism and defense strategy. The most reliable and potent defense mechanism (besides improvement in hardware technology) is the development of an Information Assurance (IA) professional.

The optimum strategy at this time is using a layered security (called Defense In-Depth) to thwart the ever-growing and highly motivated hackers of the world. An IA professional has to be an expert in many areas to prevent from developing security breeches within an IT infrastructure.

In the following paragraphs we will begin to explore areas that have either experienced successful attacks or have known shortfalls that I have observed that could lead to a security opening and could have led to possible exploitation.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

3.0 A false sense of security: Firewalls

We within the security industry should be aware that firewalls are not total protection mechanisms for IT infrastructures; a misconception held among both senior and junior IT professionals is, “The system is protected by a firewall and nothing can gain access that we have not allowed’’.

This misconception has caused other vulnerabilities to be overlooked because the thought process is, “There’s no need to worry because we have a firewall in place to protect the network”. However, firewalls only block what we administrators program them to do, and contrary to popular belief firewalls, do not block viruses or worms.

Even the most unsuspecting user can circumvent firewalls. This occurred, for example, when users installed file-sharing software (Morpheus, KaZaa, and Gnutella) on their systems to download music. The software acts as a file-sharing server while simultaneously acting as a client, searching for and downloading files from other users. Not only is a peer-to-peer network established, but also inherent vulnerabilities weaken firewalls and reveal internal network information that could be used to launch a distributed denial of service attacks. This is possible because the software counts on the firewall policy, which trusts any connection behind it. Why? Because we told it to.

Figure 1[1] graphically illustrates how the Gnutella software accomplishes this:

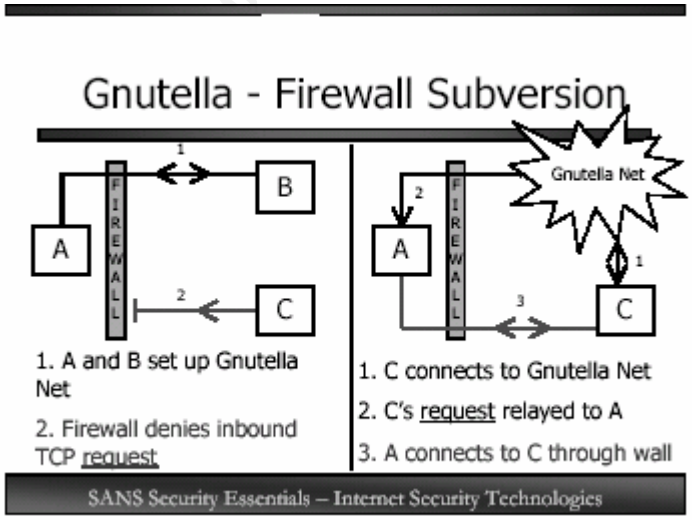

Figure 1. Gnutella – Firewall Subversion

With the capability of a user to create the vulnerability it is important to always take the Defense In-Depth approach. Regrettably most organizations fail to do

[1] Cole, Fossen, Northcutt, Pomeranz., p. 694

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

this, relying predominantly on the firewall and then the virus scanner. According to Surf Control, INC, "Unfortunately, many companies have stopped short of implementing a more secure 'layered' approach to network security and have chosen to rely solely on the firewall/virus scanner approach. While firewalls and virus protection are necessary, by themselves they address only one factor of a potential security risks and may contribute to a false sense of security."[2]

Vulnerabilities to networks and intellectual properties do not magically disappear with the installation of a firewall. A large number of companies spend incredible amounts of money on firewalls and then proceed no further in implementing a layered security solution or enforcing good security practices after the firewall has been installed.

One very good example of a poor security practice concerning firewalls can be seen at the site where I am currently employed. Due to recent budgetary shortfalls the company decided not to renew one of the firewall administrator's positions. The company, not wanting this person to think they had been cut due to poor performance, did not remove any of his privileges when the news was given to him that his position would be deleted in two weeks.

For those two weeks the network was at danger and at a high state of risk, because this individual still had full access to the firewalls that protect both of our domains from any malicious activity via the Internet.

Fortunately for the company, this individual was highly trustworthy, which is not always the case, "Every study that looks at the perpetrators of effective (if that is a reasonable word to use) network-based intrusion shows the majority are insiders, or outsiders working with inside help. Because firewalls do not keep out people who are already inside, they are of limited assistance in these cases."[3]

As the above excerpt states, firewalls are usually very limited in this type of situation since they are designed to protect from external threats and not internal ones.

The optimum solution to the previous example would have been to move that person to a position which did not require him to have access to the firewalls, thereby reducing the risk of a malicious attack from the inside by the employee.

Another limitation that most companies unknowingly impose on themselves is the lack of backup equipment or personnel. Again I will use my last three job sites as examples in the recent past.

---

[2] McCullough, Surf control.
[3] Bradner, NetworkWorldFusion.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

All three sites had networks, and all three of these networks had firewalls, not multiple firewalls for each network but a single firewall per site for protecting multiple networks from the outside world.

A misconception throughout the information systems world is that firewalls do not break, and many tend to ignore the need for redundancy. After being in the information industry for many years, I know from experience that this is a fallacious thought process.

All equipment is prone to failure regardless of the warranties. Hardware and software are man-made; i.e., equipment is built in factories, and programs are written and designed by individuals.

Malfunctions occur, so to reduce the chances of catastrophic failure, for this you need to either have a hot spare or a backup to bring your system back to an online state as quickly as possible. The misconception that firewalls are infallible is prevalent in the Department of the Navy. One site I worked with practiced this misconception on a daily basis.

This event was never published and was briefed as just a minor glitch to senior management. The site is considered a major hub for the United States Navy's protect of its important resources for the "war fighter". Every ship that is located pier side receives a T-1 connection, which allows them Internet connectivity, email, and other data through this single focal point. Even the hub's information infrastructure was routed to the Internet from this one single firewall.

It had been proposed during several budget discussions that a second firewall be purchased and integrated into the network. Several times this was denied due to cost. Slowly the degradation started. First it was an occasional blip on the scope that forced the firewall to be rebooted. Only a momentary loss of connectivity and protection was experienced.

Eventually the firewall started taking longer and longer to reboot. Then it began to impact the ships that were conducting readiness exercises, causing delays and events to be rescheduled. Shore activity message traffic being routed across the Internet, was also severely affected.

Finally critical mass was reached, and the firewall would not boot at all. After several hours of trying to revive the machine, it was determined to remove the firewall from the network while an emergency acquisition of a new firewall was being made. It was decided to route traffic and data in the clear to keep from impacting readiness of the ships.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

For a period of fourteen hours the fleet was vulnerable to outside attacks. Fortunately there was enough situational awareness by the network and security teams to set up watches while the network was in this weak state that kept this from happening.

The failure in the security posture could have been avoided with the purchase of the additional equipment and software when it was initially proposed. This is the classic example of a single point of failure and the complacent attitude people have toward firewalls. The next paragraph defines this attitude with crystal clarity.

While sitting at my desk at my current job, a friend of mine frantically called me, asking if our Solaris administrator was there. We both work for the same company and the sites had on occasion provided personnel to each other to accomplish some tight deadlines. I assumed he was having a Solaris issue. Noting the urgency in his voice, I inquired why he was frantic so when I found the administrator I could bring him up to speed quickly. He half-heartedly mumbled something over the phone, which I could not quite hear. I asked him to repeat what he said and he blurted out, “I think we have been spoofed.”

At that point I saw the administrator he was looking for, quickly brought him up to speed and handed him the phone. I then went to our manager and informed him what was happening since we were connected to this site through a VPN. When the administrator finished the phone conversation, he apprised the manager of the situation and was promptly dispatched to the other site.

We then began severing all connectivity between our site and theirs. After several hours I called back, as Paul Harvey (a famous radio personality) says, “To get the rest of the story”. What occurred is detailed as follows.

My friend had been working as usual when he received a call from a major command they provided service to. The person from the command was calling to let him know that the Naval Criminal Investigative Service was currently standing at his desk wanting to know who owned a particular IP address. They wanted to know because several other commands had been compromised, and the firewall my friend was running was the culprit. He and one of his administrators went through the logs but could not find anything out of the ordinary. He then contacted us to see if he could utilize our Solaris administrator, since his firewall was being run on a Solaris box, to help find out what was happening.

Our Solaris administrator examined the system, noting its operating system was not the correct version level and many of the patches had not been installed. He also noted that a “Torn root” kit had been placed on the system. At this point I asked my friend where the firewall came from and who was responsible for

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

maintaining it. The firewall had been obtained from a remote site in New Jersey. The administrators at his site had installed it after receiving it from the remote site. When they installed it, they did not check to see if the OS or the patches were up-to-date. The response he received from them was that it had been running fine at the remote site so they assumed it had been maintained and they had not received any error indications or trouble when installing it at his site. While discussing with them the proper steps for implementing new equipment, he realized that neither had very much experience in Solaris or firewalls. He has since rectified this situation.

The whole situation resolved down to one major and two minor issues. The major issue was the dependency on firewalls to keep the network safe from all outside threats, which is usually the case (with the exception of worms and viruses which I cover later). The two minor issues are: (a) the experience of the personnel responsible for the firewall, and (b) the improper maintenance of the system. Proper coordination with IA professionals at my site could possibly have prevented this from happening, since the first step we go through is a scan of any system before integration into the network.

In the next section I highlight how the inexperience of personnel played into this scenario, and in the section following I discuss how patch management plays a major role. All three of these sections define how the interplay of one with the other two, if not properly maintained, can lead to single points of failure within the Information Assurance environment.

4.0 Lack of knowledge, experience and education: The Coffee Shop Graduates

In today's IT environment you can find almost anything you want to know at your local Barnes and Noble (www.barnesnoble.com), especially a series of books with the words "for Dummies" in the title, which cover everything from how to take a course to managing personal investments (in this instance CISSP for Dummies). Order a cappuccino, grab a book off the shelf, get comfortable, and start reading. For the total cost of 74 dollars (4 dollars for a cappuccino and 70 dollars for CISSP for Dummies), you can begin a new career. Study for a couple of weeks, and then go online and register for certification exam preps, go to a local certification authority to take a 3-7 hour test, and wham! there you go, you are now a certified CISSP. For basically less than 500 dollars, you could one day be in charge of the security for a major company or, even better yet, a DOD system. Boy, isn't this a scary thought?

Information Assurance is the hottest and latest crave in the IT industry. A lot of current employees within the Information Assurance arena have no real basic functional experience. These same individuals are now applying for positions in the IT security industry as certified IT security professionals.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

In recent times the Security Professionals were home grown from System Administrators because of their extensive background in the service side of the industry. They were placed into the security field and these chosen few focused on acquiring the knowledge and education to identify themselves as Information Assurance professionals. These same individuals decided they were no longer going to be victims to the ever-growing world of hackers. So today's line-up is IA professional versus hackers.

From these same professionals came the awareness that most companies suffered from the same problem when it came to Information Assurance. There were no standards for the minimum knowledge required for a person to get started, and there were not enough people coming online to fill the chasm in the industry. Hence, organizations like International Information Systems Security Certifications Consortium, Inc (ISC)2 (www.isc2.org) and System Administration Network and Security Institute (SANS) (www.sans.org) were born.

Both institutions took steps to help the IT community start a foundation for helping the IT professional become conversant in Information Assurance techniques, laws, and governing policies. (ISC)2 has established the Certified Information Systems Security Professional (CISSP) certification and SANS founded the Global Information Assurance Certification (GIAC), which has allowed thousands of security professionals to prove their skills and knowledge required to meet the challenges in the information systems world today. Both organizations have taken great steps to ensure these certifications do not turn into the Microsoft MSCE paper administrators of the nineties. The major differences between the Information Assurance professional and the systems administrator is as a system administrator you can make a mistake that may not cost you your environment, but within the Information Assurance world one bad decision could lead to major disaster.

Even with these steps there are still personnel just entering the industry claiming the credentials of the CISSP. Human Resources personnel interviewing these people do not have the knowledge or background in information security to conduct thorough interviews. They become excited and are easily impressed when individuals start using buzz words like CISSP, Firewalls, Intrusion Detection Systems and Network Scanner, just to mention a few.

In the Department of Defense world it is critical that an IT professional becomes familiar with the various manuals and publications governing IT security since they are the foundation for building an accredited network. In the civilian sector of the information assurance industry, these various documents and publications can also apply.

September 11th, 2001 spawned a new era with companies doing business for the federal government. They were given a mandate to provide knowledgeable

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

employees, especially in the AIS security realm. One major problem is that knowledgeable and seasoned Information Assurance professionals are in short supply. Companies are forced to hire less than perfect candidates that only have a basic (if any) knowledge base to meet contract requirements. Having someone in the position that is not truly trained or knowledgeable entails a great risk, as mentioned in the following excerpt from in the Red Hat Linux 9: Red Hat Linux Security Guide: “Inattentive Administrators”:

> Administrators who fail to patch their systems are one of the greatest threats to server security. According to the System Administration Network and Security Institute (SANS), the primary cause of computer security vulnerability is to "assign untrained people to maintain security and provide neither the training nor the time to make it possible to do the job. This applies as much to inexperienced administrators as it does to overconfident or unmotivated administrators.
>
> Some administrators fail to patch their servers and workstations, while others fail to watch log messages from the system kernel or network traffic. Another common error is to leave unchanged default passwords or keys to services. For example, some databases have default administration passwords because the database developers assume that the system administrator will change these passwords immediately after installation. If a database administrator fails to change this password, even an inexperienced cracker can use a widely known default password to gain administrative privileges to the database. These are only a few examples of how inattentive administration can lead to compromised servers.[4]

The second paragraph of this excerpt reinforces what I mentioned in Section 2 about experience and patch management. If the personnel had been properly trained and had checked the operating system version they would have realized that the patch levels were also behind. Section four covers patch management.

5.0 Patch Management

All information systems are only as good as the patches that have been applied. Keeping up with all the relative patches for each operating system can be a full time job in itself. One of the Top Ten Security Exposures listed by the University of California, Davis is an operating system patch, particularly a security fix, which has not been installed on a system.[5]

---

[4] Red Hat Linux 9: Red Hat Linux Security Guide, Chapter 2.
[5] University of California, Davis.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Many system administrators barely have the time to do the normal day-to-day operations along with the required maintenance functions to keep the systems operational with relative efficiency. Needless to say, applying new patches could result in overburdening the already overworked administrators, and this is what hackers are praying for. Frequently the patches don't get applied, and this is a grave mistake indeed.

Hackers are always prowling the network. Most hackers are knowledgeable of the system administrator's time-consuming task of checking and installing new patches against his operating environment. One of the first things the system administrator has to ensure is that no damage is incurred with installation of new patches. The biggest hurdle is getting approval from management, who want to know how, why, is it really necessary, how much time will it take, what is the cost, but most of all, how does this affect our clients. At my current job site, the administrator is informed the patch must wait for the next available maintenance window, which might be up to a week away. This is one of the things hackers count on to help them wreak havoc or intrude into various systems to see what can be found.

This is highlighted by the following excerpt taken from the "Red Hat Linux 9: Red Hat Linux Security Guide" under the "Threats to Server Security":

> Developers and system administrators often find exploitable bugs in server applications and publish the information on bug tracking and security-related websites such as the Bugtraq mailing list (http://www.securityfocus.com) or the Computer Emergency Response Team (CERT) website (http://www.cert.org). Although these mechanisms are an effective way of alerting the community to security vulnerabilities, it is up to system administrators to patch their systems promptly. This is particularly true because crackers have access to these same vulnerability-tracking services and will use the information to crack unpatched systems whenever they can. Good system administration requires vigilance, constant bug tracking, and proper system maintenance to ensure a more secure computing environment.[6]

It is not only important to keep the patches up to date but also to keep the procedures for patch implementation flexible as illustrated by the following question and answer from the Windows Server System Magazine:

> *Q:* The recent flurry of security threats against various Microsoft products has us scrambling to try to keep our servers and workstations up-to-date. Do you have any recommendations on how we can facilitate this process? It seems a bit overwhelming.

[6] Red Hat Linux 9: Red Hat Linux Security Guide, Chapter 2.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

—Nancy, Tampa Bay, Fla.

A: Danielle: You're right Nancy; patch management is a lot of work. In fact, it forces us to rethink our deployment strategies because when we receive a critical warning of a security flaw and an accompanying patch, we pretty well have to deploy it right away. Just look at the MSBlaster worm. That worm came out a little more than a month after the Microsoft warning and security patch release. It is easy to understand why this worm caught people. Before the storm of security patches and associated threats we've seen recently, Nelson and I advocated a four-month schedule for service pack and hot-fix update deployment within most networks. This gave you a lot of time to collect, test, and aggregate the patches you needed to deploy. Of course, we also provided our customers with an emergency deployment process that could be used when the circumstances were dire enough. But what we're seeing now is that the emergency mode is becoming the norm, whereas the standard schedule is sometimes being dropped altogether. [7]

This also reveals how the recent flood of security threats has highlighted the need for updated patches as well. Patch management is useless unless the source companies issue reliable patches on a timely basis.

As noted above, the need for patch management has become paramount for helping to ensure a secure system. The reality of the situation is that both the civilian and military sectors of the United States are slow to react, causing disruption of services or theft of intellectual property. The number one factor is not the proactive System Administrator, but the reaction of Senior Management to the need to take down the network to implement security protocols. Potentially, millions of dollars could be lost in a short period of down time. This will induce hesitation in the onsite supervisor/manager to make the decision, since monetary considerations frequently take precedence over security issues until it is too late. Then you have a situation where loss of jobs, confidence, and most of all loss of more revenue is incurred.

In November of 2002 it was reported by “Computer Weekly” that Gary McKinnon[8], an unemployed system administrator in the UK exploited well-known security vulnerabilities in the Windows operating systems. He identified systems without crucial security patches installed that were connected to the Internet. He then exploited these vulnerabilities to download files of user-names and then utilized brute-force techniques to crack the passwords to gain access to sensitive computer systems at NASA, the Pentagon, and the Department of Defense.

[7] Ruest, Windows Server Systems Magazine.
[8] ComputerWeekly.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

He then is alleged to have installed a Commercial-Off-the-Shelf (COTS) network administration tool allowing him the ability to remotely control machines from a PC in his home.

This all occurred while the whole world and especially the United States was pre-occupied with the upcoming war in Iraq. Media attention was focused on the war preparations. Not only was data lost but also systems impacting US battle readiness were affected. It is estimated that McKinnon's intrusion cost over a million dollars in damage to these unsecured systems. Additionally, his hacking could have cost enormous loss of life in our fighting young men and women. Ask yourself, were you more interested in watching the television or protecting your network during those weeks and months? Do you remember seeing or hearing about this in the mainstream media during this timeframe? I don't.

The interesting irony in this story is that security officials rated Mr. McKinnon to be only average in computer hacking and not a true black hatter. A group of true hackers or a terrorist group sponsoring professionals could have done the same thing, and the repercussions could have been crippling. Thank God for small favors.

This case demonstrates the difficulty that organizations with tens of thousands of systems face each and every day, keeping a system up-to-date with security patches and security fixes. With the myriad of tools on the open market for purchase and the massive amount of freeware that is available, ensuring our system security patches are up-to-date is still a monumental task and a responsibility our system administrators must endure.

Now that we have covered firewalls, lack of experience, and proper patch management, let's step into the next area that can be a single point of failure but most times can be easily handled: Virus Protection.

6.0 Virus Protection

Computer viruses are mysterious at best and could be one of information assurance professional's defining moments. Do not be mistaken; viruses will get our immediate attention when launched. A properly engineered virus can have an amazing effect on the worldwide Internet. Some in the past have shown us how interconnected we truly have become in this digital age, not just within our borders but globally. They show us how vulnerable we are, and how some intentional and non-intentional scripts can cause more devastation than a natural disaster. Let's explore a supposedly "good" worm that defined a critical single point of failure in the Department of the Navy networks.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The following article highlights two very important issues, the first that code even deemed as “good” can be dangerous, and the second that having a contingency plan or alternate hot site is mandatory in case of an emergency.

> For the first time in its short history, the Navy Marine Corps Intranet fell victim to an outside attack.
>
> A virus, albeit a supposedly "good" one, wormed its way into the enterprise-wide network last week, causing many users to lose e-mail and Internet connectivity.
>
> NMCI users experienced "intermittent problems" connecting to outside networks, said Kevin Clarke, a spokesman for EDS, the lead vendor for the Navy's initiative to create a single network for its shore-based operations.
>
> The network did not fully crash, and users still had access to their desktop applications, officials noted. NMCI personnel distributed a patch from security firm Symantec Corp.
>
> “We are currently experiencing connectivity issues enterprise-wide to include e-mail, Web and shared-drive access due to a virus," said a hot line recording of the NMCI Strike Force, which is made up of Navy and contractor personnel who handle network problems.
>
> The so-called Welchia worm roots through networks looking for the Blaster worm that debilitated so many networks last week and automatically downloads and applies the Microsoft patch. But it does so at the expense of processing speed and bandwidth.
>
> It remains a mystery how the new worm got inside the NMCI network, according to Capt. Chris Christopher, NMCI's staff director. "We could bring the whole network down [to fix it], but we do not want to do that.[9]

With this “good” (Welchia) worm seeking out the “bad” (MSBlaster) worm, the US Navy was brought to its knees while in a time of war. The Navy has not experienced an attack of this magnitude since Pearl Harbor on December 7, 1941. Many top-level echelon commands were unable to communicate, including the command that was designated to be the information assurance principal for the US Navy.

I mentioned in Section 4 that monetary issues take precedence over security issues; this incident is another example. Instead of taking the network down and cleaning the worm out, it was decided to leave it up. The reason is the company

[9] French, FCW.com.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

that administers the NMCI project gets paid on a per seat basis. If the system is not at least minimally available, they do not get paid.

There are numerous ways a system can become infected. One of the most popular ways is through the e-mail system. We all have it, we all need it, and we are all susceptible.

Virus protection needs to occur on several levels:

First level: Anti-virus software should be installed on every client workstation. If it is not, virus protection for the whole system has been blown clear out of the water from the start.

Note: System Administrators should be the only ones to have the ability to disable this feature, but they should do so only after disconnecting the workstation from the network and ascertaining that the virus software was indeed causing the problem.

Second level: Anti-virus software installed on servers. The server provides protection for both inbound and outbound email.

Third level: Educated users and managers. Keeping the user community and management informed of the new viruses helps them understand the impact if the network or workstation gets infected.

Fourth Level: Virus Signature Updates. Systems can be protected from being infected or affected by viruses by keeping signatures on the virus software up-to-date. You don't want to put yourself or the network in jeopardy when you realize your signatures expire tomorrow and that night at midnight a virus is launched that you can't protect for. At this point you are the weakest link. Good-bye.

On the other hand, even if the signatures are up-to-date, by means of a live update from http://www.symantec.com or other means, it is still highly possible for a virus to sneak into the network. This is where the user community comes into play.

7.0 The User Community

The information assurance industry has made great strides within the last ten years in the areas previously mentioned. Unfortunately, as in most cases, education of the user community has fallen behind. Most users unknowingly set the enterprise up for an attack due to the failure to understand the impact of their actions. They do not properly protect their passwords after they have received them, creating and using easily cracked passwords, and walking away from

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

machines without signing out or locking them. The following excerpt is from "Software Wire" website, December 11, 2001.

> Many computer users do not understand how important it is to assure that their entire Internet related software is patched. Although the Internet software is designed to create a wall of security, that wall sometimes has small holes the can be used by viruses or hackers. The software manufacturers create patches for these security holes as soon as they become aware of a problem, but it is up to the user to know to install the patches.[10]

Some users disregard policies, providing the hacker with success as reported in the "Government Computer News" article: "Bryan said that out of 25,000 categorized attempts last year to hack into Defense systems, 245 were successful—and officials found that 96 percent of successful attacks could have been prevented if users had followed protocols."[11]

Education is only half of the battle in this situation. The other half is enforcement of information assurance policies that are currently in place. Only when these two equally important areas are joined will the user layer of security be a reliable tool of the IA professional.

8.0 Summary

In the compilation of this paper I have touched upon several points in the Information Assurance field:

- Dependency on equipment without a clear understanding of its function.
- Lack of knowledge and experience of some IA professionals.
- Failing to keep patches for systems current.
- The impact viruses can have if we are not diligent.
- Assets being placed under one umbrella without a clear plan if something happens.
- The education or failure to follow IA security protocols in the user community.

All of these points must constantly be kept in mind when embarking upon a career in information assurance. One oversight in any of these areas can cause major damage not only to the equipment in the local system but also to other systems on the Internet. With diligence and perseverance comes the reward of a secure operating environment and a good night's sleep for the Information Assurance professional.

---

[10] Softwarewire.
[11] Onley,Government Computer News.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

References

1. Cole, Eric; Fossen, Jason; Northcutt, Stephen; Pomeranz, Hal. "SANS Security Essentials with CISSP CBK", Version 2.1. Feb 2003. SANS Institute. Chapter 15, "Vulnerability Scanning", page 694. (April 2003)

2. McCullough, Jack. "Beyond the Firewall: Using a Layered Security Strategy to Address Internal Security Threats." Surf control, Inc. URL: http://www.bitpipe.com/data/detail?id=1028048649_631&type=res (01 May 2003)

3. Bradner, Scott. "Portable firewall circumvention." NetworkWorldFusion. URL:http://www.nwfusion.com/archive/1999b/0726bradner.html (26 Jul 1999)

4. "Red Hat Linux 9: Red Hat Linux Security Guide." Chapter 2 "Threats to Server Security". Section 2.3.3 "Inattentive Administrators." URL: http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/security-guide/s1-risk-serv.html#FTN.AEN588 (2002)

5. University of California, Davis. "Top Ten Security Exposures." Information & Education Technology. URL: http://security.ucdavis.edu/securityexposures.cfm (02 Sep 2003)

6. "Red Hat Linux 9: Red Hat Linux Security Guide." Chapter 2, "Threats to Server Security." Section 2.3.2 "Unpatched Services." URL: http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/security-guide/s1-risk-serv.html#FTN.AEN588 (2002)

7. Ruest, Danielle and Nelson. "Manage Security Patches." Windows Server System Magazine. URL: http://www.ftponline.com/wss/2003_12/magazine/columns/windowstips/Default.aspx (20 Nov 2003)

8. "'Average hacker' skills shut down US defense systems." ComputerWeekly.com. URL: http://www.computerweekly.com/Article117677.htm (21 Nov 2002)

9. French, Matthew. "Virus worms into NMCI." FCW.com. URL:http://www.fcw.com/fcw/articles/2003/0825/news-worms2-08-25-03.asp (25 Aug 2003)

10. "Computer Virus Spread Due to Lack of Education." Softwarewire.com. URL:http://www.softwarewire.com/news/scs_121001.htm (11 Dec 2001)

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

11. Onley, Dawn S. “DISA official: Users should be accountable for security.” Government Computer News. URL:http://www.gcn.com/vol1_no1/daily-updates/4028-1.html (25 Apr 2001)

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**