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

Ralf Duken
Employees are either a company's lifeline or noose
GSEC Practical assignment, Version 1.4b, option 1
28 August 2003

Abstract

Network operators and managers today realize that hackers do not represent the only source of security threats to an organization. Organisations rely on firewalls to ensure their systems from external attacks and malicious code, whereas an internal user can compromise the integrity and security of information systems in numerous ways. Attackers who have physical access to company facilities, workplaces, computer systems, and networking components have a much higher success ratio of performing a successful break-in**.** " The FBI is also seeing rampant insider hacking, which accounts for 60% to 80% of corporate computer crimes, according to consultants such as Gartner Group." [1]

An external attacker is not motivated to do much damage, does not know much of the internal network and is more than likely to stumble into an Intrusion Detection System (IDS). The attacks that cause the most damage are those from a disgruntled employee who is personally motivated to come after you. This paper describes how internal threats manifest themselves and tries to provide the reader with an outline on what needs to be done to control internal access to restricted data and protecting company assets from damage. By no means is this paper detailed enough to provide all the answers but instead hopes to create awareness of the seriousness of internal threats and how to protect against them. All-too-often companies believe that implementing a firewall and an IDS is sufficient to protect its data but that leaves little defence against insider attacks. The structure of this paper begins with a discussion on how employees pose a risk, followed by how both physical and technical controls need to be put in place and how they help a business if they are implemented properly. We discuss how to limit internal threats from successfully attacking local resources, and also how to protect the network from being the source of an attack. The paper closes with points to remember when creating a policy concerning internal security.

Networks are increasingly becoming not only a target of attacks but also a source. Management must establish a corporate culture that values security. This helps in keeping the honest people honest and makes it easier to deal with those who choose to cross the line. Fostering that corporate culture requires a security program that uses a top-down approach from management, meaning that the initiation, support, and direction come from top level management and work their way through middle management and then on to their staff members. A top-down approach ensures that the key people (managers) actually responsible for protecting the company's assets are also in charge of handling the security program. The more the business and security objectives are in alignment, the more successful the two will inter-operate with one another. While this document tries to highlight the danger employee's pose, by heightening their understanding of security risks they can also become a company's best defence if they understand and follow the security policy.

A security policy is a blueprint for a company's security program and serves as the key cornerstone on which to develop further. This policy will be continually referenced to ensure that all security procedures and components stay in step and follow the security objectives.
Policies can fall into one of the following categories:

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

- **Regulatory**: This policy is written to ensure that the organization is following standards set by a specific industry and is regulated by law.
- **Advisory**: This policy is written to strongly suggest certain types of behaviours and, activities that should take place within the organization.
- **Informative**: This policy is written to inform employees of certain topics. [2]

How employees pose a risk and how to woo them over

The typical disgruntled employee is what usually comes to mind first as the dangerous person within a corporation. Such a person might have been passed over for a promotion or a bonus or might have been laid off. He then uses his knowledge of the company and his remaining access to the corporate network to satisfy his vengeful hunger. There is also always the favourite, corporate espionage. When an employee earns a yearly salary of $40000 and a man approaches them with a $10000 offer for a piece of information, it just might be too tempting for them to resist. Another scenario could be an employee is leaving the company and decides that data from a project he was working on might come in handy at his new position. Big company layoffs can be a nightmare of security risks as the IT department spends weeks closing down network connections, cleaning up network configurations and plugging the holes. During layoffs, companies must follow certain guidelines to reduce threats from resentful employees,

- Be honest with employees about the stability of the company and the potential for layoffs;

- Clearly and completely document each worker's access to the network, applications, servers and the physical building;

- Shut down remote connections, including PCAnywhere and VPNs; Close down user names and passwords; If the person worked in IT, change route access and network access;

- Shut down telephone access from the outside; Make sure handheld devices, smart phones and cell phones are turned in along with PCs and laptops; Collect security ID cards;

- Have monitoring software in place to keep an eye on network traffic;

- Make sure the worker's own manager is able to tell the employee that he is being laid off -- not someone unfamiliar from HR;

- Offer a financial cushion or severance package; Offer outplacement services; Offer counselling services." [3]

Of course if you are working for a technological or manufacturing company, layoffs are an even larger threat as now you are dealing with people who have the know how and potential skill to cause serious damage. Companies in these fields should take extra precautions such as backing up all company data before they commence with the planned layoff. These backups serve a dual purpose of allowing recovery of data should a system be compromised and can also be used as forensic evidence should the culprit ever be brought to trial.

Job rotation is often an overlooked part of keeping operations healthy and productive. No one person should be allowed stay in one position for an extended period of time. Keeping an employees interest in their work high increases their productivity level. From the beginning

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

administrators should tightly restrict the access to company resources by employees. Giving rights to a user later is much, much easier than tacking those rights away from the user without causing some resentment. Employees should only have access to the data and systems they need access to from day one. This might sound rather simplistic but it is not unusual for employees to have 10 to 20 times mores access to resources than they need to accomplish their job roles.

Social Engineering threats

Any hacker worth their salt will be good at social engineering, using the information they coaxed out of people to their advantage. The notorious hacker, Kevin Mitnick spooked the judge assigned to his case in 1995 so much, that the judge placed him in solitary confinement, away from people that he could "influence." This should speak volumes about the danger social engineering poses.

Social engineering is not a technical problem but one where you have to make changes in peoples behaviour and their interactions with others. Most people are instinctively trusting. Teaching employee's to cultivate a healthy level of paranoia will make hackers think twice before making attempts at people who are likely to see through them. The security policy will include an outline of the companies user education program. Employees must be taught to question everything, and to always verify the source. Hackers always do their homework and will research as much as they can about the person they are going to interact with and their colleagues.

Popular information gathering tools include these:

- Employee directory: A great source of employee names, email addresses/ phone numbers, and department names can usually be found with just a few clicks on the company's home page.
- Company phone systems: Some phone systems include dial-by-name and employee name lists from which a hacker can get real employee names to use for impersonation or to determine targets.
- Lobby directories: Office numbers, names, titles, and other useful information 3 presented for anyone to read.
- Usenet posts and email list archives: Hackers can search archives for emails and posts that originated from the target company's domain. Not only can they gather employee names, but they can determine what people are interested in and learn their writing style. Often the signatures on the posts contain position and contact information.
- Online databases: Searches for phone numbers and postal and email addresses are quick, easy, and free at numerous locations on the Internet.
- Home pages: Today everyone seems to have a home page, where they happily tell you all about where they work, where they went to school, who heir friends are/ and what foods they like. Hackers can get all the information they need simply by reading it straight from the source.
- Public DNS information: Searching the Internic databases can yield administrative and technical contact information and email addresses. [4]

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

As the only real defence against social engineering is by heightening the users understanding of security risks, user training must be an ongoing process, not just a once off session. When developing an awareness-training program, one must keep in mind the three different audiences that it must cater to, namely management, technical employees and staff. Management benefits from short and focused lessons that deal with assets, financial gains and losses, and how security policies need to be integrated into the company. Technical users need in-depth technical training on their daily tasks and on incident-handling procedures when a security breach occurs. Regular employees are the most important group and they need to understand the importance of security and why it is in place. They need to understand that security begins with them personally and why they must follow the security guidelines.

The company's security policy must address these types of issues and must be put into operational configurations that are enforced across the board in the company. It is no good training employees and then not keeping them on their toes by not doing routine security checks.

Physical Security.

Recently physical security and IT security are becoming ever closer interlinked. Just as there is ever-increasing communication between Human Resources and the IT department, so is there between the onsite security personnel and the IT staff.

> "People should move away from the mindset of separating IT security and physical security", argues information security consultant Daniel Lewkovitz.
>
> "Someone who knows how to install a firewall may not know how to assess camera technology," he said. But Lewkovitz said that over-riding concepts such as risk assessment, risk treatment and overall approaches were similar for physical and IT security. "The risk of anonymous hackers may be as great as someone coming and setting fire to your building," he said. "So the concepts are very similar—if you're protecting a computer, a person, or a building." [5]

Physical security is a very important consideration when it comes to guarding against internal threats and is also an all-too-often overlooked one. Having your firewall in a broom closet doesn't add to the company's security. All the money and hours you've spent securing your networks from electronic intrusion will all have been for nought if someone can simply walk into the wiring closet and access your network from the inside.

Don't just let anyone wander around your building. Lighting should be used to discourage any intruders and provide safety for the employees. Any thief, be they an employee or an outsider, does not want to be seen and with adequate lighting in place you can deny them this comfort. Keep all the important networking nodes and servers under lock and key and install cameras in those rooms. The cameras wont stop anyone from tampering with the equipment but they provide evidence that the systems had been compromised. Control the climate and environment in these rooms carefully at 10-26 degrees Celsius (50-75 degrees Fahrenheit). Install heating and cooling systems with air filters to protect against dust and other impurities in the air. A hygrometer can be installed to monitor the humidity level.

Critical business information must be restricted to confined areas, separate from any information that requires a lower level of security. Every company should have system in place for categorizing the access level for all its data. The company's internal structure must reflect

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

this by providing different access levels for its employees and the compartmentalized data they have access to. All employees must have a badge, preferably divided into different colours, one colour group for each sensitive area. All guests, consultants, and service personnel such as phone, computer and wiring technicians must be provided with a guest badge and must be escorted at all times within the sensitive areas. Badges should expire and employees must be "reauthenticated" before they are issued with a new badge.

Users behaviour has to be sculpted to the objectives outlined in the security policy. Teach employees to keep their workplaces clean and locked and not to write down sensitive information that somebody walking by can quickly read. All users must use good screen saver passwords and must log off their systems when leaving for home. Users must be aware of the existence of keystroke loggers, both physical and software such as eBlaster, and how to check for them. Staff must be taught not to smoke near computers as smoke causes damage, nor should staff be allowed to eat at their desks. Adequate fire extinguishers and smoke detectors should exist near all equipment. Make certain staff are trained in the use of all fire suppression systems. Fire prevention comes from training employees how to react quickly when faced with a fire and supplying them the right equipment to suppress a fire. For important machines and networking nodes you may want to install an automated fire suppression system.

All confidential material such as manuals should be shredded, preferably with a cross-cut shredder that shreds documents both horizontally and vertically to prevent dumpster diving. All dumpsters should be located in well-lit, secure areas. To prevent sensitive information on storage devices from being retrieved when thrown away, use a strong magnet to permanently erase all content.

Securing valuable company information through regular backups is the best defence against a natural disaster, a hack job or a virus. Backing up data might seem like a hassle except for the day when you wish you had one to fall back on. One cannot predict when something will go wrong. A disaster recovery plan requires a great deal of thought, planning, time and effort to properly identify threats and to counter them with a detailed plan that can be implemented immediately should the need arise. A disaster recovery plan is needed should a disaster happen, and we have all heard "It was an act of God." Don't get caught with your pants down. Natural disasters, fire, floods, sabotage and environmental issues all need to be planned for. At the very least a company must store backups in a secure location on encrypted media. A second set of backups must be periodically archived and stored at a secure remote location. If using tapes as the backup media, store them away from any large metal objects to avoid them being damaged from magnetic fields that can be caused during lightning strikes.

An intruder with access to company computer equipment could just reboot a logged off workstation, insert bootable media and take control of that machine, including reading all the data on the hard disk if encryption is not employed. Countermeasures include using a BIOS password with the correct BIOS boot-up order settings in place or removing the actual CD-ROM drive and floppy drive. Tools such as Trinux allow an intruder to boot up a running version of Linux, albeit a small one, that is packed with enough tools to enable him to further compromise nearby networked machines. Such an approach is not very stealthy and should be noticed by users if they are trained to report such oddities. This explanation is taken from the Trinux website.

> Trinux is a ramdisk-based Linux distribution that boots from a single floppy or CD-ROM, loads it packages from an HTTP/FTP server, a FAT/NTFS/ISO filesystem, or additional floppies. Trinux contains the latest versions of popular Open Source network security tools for port scanning, packet sniffing, vulnerability scanning,

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

sniffer detection, packet construction, active/passive OS fingerprinting, network monitoring, session-hijacking, backup/recovery, computer forensics, intrusion detection, and more. [6]

As previously mentioned, to provide protection against someone rebooting the machine and changing the BIOS settings, restrict access to the BIOS with a password. These BIOS passwords are weak as they can be flushed from memory by removing the C-MOS battery located on the motherboard or by setting the jumpers. Another weakness in BIOS passwords is that many motherboard manufactures make use of a system password, which when entered overrides the users set password. These system passwords are all too often publicly known on the Internet. By replacing all chassis screws with non-standard screws such as Torq screws, it makes it harder for an intruder to open the chassis and just walk away with a hard disk or to remove the C-MOS battery.

Many CD-ROMs come with an auto run function. This can allow a malicious user to execute or copy a virus to the hard drive without any visible trails being left behind, without even having to log into the system. In Linux this is not a problem as usually only an authorised user with sufficient privileges can mount the CD-ROM file-system. To turn this feature off on Microsoft machines, edit the system registry, move to this location, edit the key and set it to 0 (off).

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControllerSet\Services|CDROM

Keep all entrances that are not used by the public locked and monitor those that are with cameras and security checkpoints. The security personnel at these checkpoints should check all bags and briefcases if the security concerns of management are very high. Mantraps are another option whereby all personnel must pass a security guard and enter a double door area where they are subjected to additional authentication and identification checks. These security checks have a negative effect on company moral and are not recommended unless no other alternative exists to sufficiently secure the equipment and data of the company.

As most of the physical security solutions one can buy are unsightly to the eye, another option that exists is to fix a device to the inside of the computer case which lets out a loud alarm when the case is disturbed. The downside to these devices is they tend to go off when not wanted but they always attract attention when they do.

Laptops are always a prickly problem due to their value and size. One should never save any passwords or vital databases on laptops – it is far too easy for them to disappear unexpectedly. All laptops should be marked with a tag that contains the model, serial number and the name of the person who is allowed to remove it. A good tag for laptops is the STOP Tag security plate. Laptops are a prefect scenario for the use of encrypted file systems. Encrypting every file on a hard drive and encrypting a hard drive are two separate ideas. If you encrypt the hard disk itself, you can't even see the file structure, all you will be able to see is an encrypted partition. Use a good encryption algorithm like blowfish to encrypt all areas of the hard disk except for the files needed to boot the operating system.

Technical Controls

Technical controls are what many people assume should be the sole responsibility of the IT department. Security is the sum of all its parts combined, not just the technical area. Companies need to be concentrating on a holistic security architecture, which means making security a part of everything and not making it into its own category. With the increasing number of hacking scripts and tools that are being made available to the general public and the

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

simplicity of using them has made hacking rise in popularity. Thanks to the number of these easy-to-use hacking tools available today, intrusion incidents occur on virtually every computer network.

Security response teams are an essential part of every company's security policy. Organizations must prepare for the inevitable incident that will come one day by identifying who is in charge and what changes they will be permitted to do, who does what specific roles, and who responds to an intrusion by performing forensic analysis and eventually system recovery. Policies and the supporting documented procedures that are taught and enforced in the organization allow one to prepare teams that can respond in a quick and controlled manner. This allows one to exercise those procedures and work out any problems that might occur before an intrusion takes place. One could think of it as the response personnel being divided into an offensive, a defensive and into several special teams to quickly limit any intrusion and the damage that might be caused. These teams must hone their skills and streamline their responses to be as efficient as possible when an intrusion is taking place.

A firewall is a hardware device used to restrict access to one network from another one and are powerful tools when it comes to enforcing the security policy. All companies use a firewall to provide a logical barrier between a company's internal network and the machines lurking out on the public Internet. Once inside the network, there are few restrictions in place. Firewalls are necessary tools and the more the merrier. Firewalls need to be used not only on links to the Internet but also to secure certain sensitive network segments. A company must divide the network structure into different areas of importance and protect these sensitive networks with firewalls and IDS's. Important hosts and switches must be protected by stateful firewalls. The reason for using stateful firewalls is that these firewalls analyse each and every frame on all communication levels thereby providing a high level of security. Stateful firewalls also have much better performance when compared to a proxy firewall. Employees usually have free reign inside the corporate network and pose a real threat, but by using firewalls to your advantage, their actions can be controlled, stopped and logged. This provides a company with additional security against unhappy employees and in case an employee's account is compromised.

Valuable data must be confined to an area, away from normal data usage. Using Firewalls allows us to either permit or deny a users connection. What can be done when we need to allow a user into a sensitive area but only allow that user to access certain information? Every company faces the problem of maximising their network returns and at the same time balancing the benefits of user access with the risk of a compromise and the financial implications caused thereby. One cannot erase every in-house security threat but there is software designed to help you manage those risks and to reduce them to a pre-defined and acceptable level. These software categories that are to be mentioned provide valuable checks in controlling access to resources and overcoming weaknesses in computer systems.

Authentication software answers the question of, "Who are you" and asks you to prove it. If resources are valuable, it makes sense to restrict access to them on a need-to-know basis. Strong authentication software works on combining two out of the following three methods. To authenticate a user requires asking something that the person must know like a pass phrase, asking for a physical object such as a smart card or SecureID or requiring a biometric such as a palm or iris scan. Vendors such as Netegrity supply such solutions.

Authorization software determines which users have access to what files. Once a system has confirmed who you are, authorization software determines the access that the user will have. Unix and Windows operating systems provide these services as a core component but

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

applications and add-on packages can also provide this functionality. These applications are often quite difficult to implement and easy for a knowledgeable employee to bypass. IBM and Computer Associates, amongst other, make authorization software.

Administration software allows a company to automate and simplify security management. There are so many different products sold under the umbrella administration software that it is beyond the scope of this paper to discuss them. A possible implementation of such software would be to ease the workload on an IT helpdesk by allowing users to change their passwords themselves by logging into automated software. This in turn allows for strong password policies to be enforced as the software judges the quality of each password as it is changed. This allows a company to keep track of all users and what access they have to company resources. BMC and IBM's Tivoli system are popular vendors when considering this from of automation.

Audit software reports on security events, vulnerabilities network usage and any abnormalities it finds. It is vital for an organization to know when, how, and what to audit. Audit software pro-actively audits and assesses vulnerabilities. This software should deliver forensic evidence, data analysis, reporting and simplified management. Manufacturers include Counterpane and Bindview to name but a few. This software is essential for security as it provides a picture of the security and therefore the health of the company network.

By making use of applications in the software categories listed above and combining them with firewalls, VPN technology, encryption, and network Intrusion Detection Systems, a company can reduce their in-house risk dramatically.

We all know the importance of monitoring the corporate network for any unusual traffic and activity. The security budget usually has room for the purchase of an IDS system for the network, but there is other valuable security monitoring software such as SilentRunner [7]. SilentRunner is a protocol analyser on steroids that is combined with analysis and visualization tools. This software monitors network activity in real time, providing a virtual picture of network usage and traffic patterns. It does this by recording all electronic transmissions including all company e-mails and browser activity and analyses this data to allow the monitoring of intruders and their activities in real time. It is also able to combine logs from firewalls, routers, switches and Intrusion Detection Devices for an in-depth analysis of network activity.

From a technical point of view, keeping systems secures involves mainly patching all vulnerabilities as soon as they are posted on news lists such as bugtraq.

> Interestingly, 99% of all attacks come from known vulnerabilities. Though readily preventable, IT personnel are typically too overloaded to keep pace with the traffic. The sheer volume of OS updates, application upgrades and security patches means that IT rarely makes timely server updates, never mind plugging up gaping security holes at every desktop throughout the enterprise. Despite knowing about the threat, the time involved in manual updates makes it impossible for IT to keep up. [8]

This sounds easy enough but it takes huge effort to remain informed on the latest vulnerabilities and even more effort to keep machines patched. If a person responsible for keeping your network secure comes back from a weeklong holiday, their security information will not be up to date. They need to spend time researching all the security issues that were discovered while he was away before he can consider himself ready to do work again. Management must give their security professionals enough time to research new vulnerabilities and other security issues. Research is work and needs to be taken seriously by management.

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

Virtual LAN's enable you to logically group users based on resource, traffic patterns and security requirements, not just on physical location. VLANs allow us to apply different security policies to different groups of users. Administrators must liberally apply those different security policies to each VLAN depending on what access those users require. VLANs should be at the forefront of any security policy to restrict the virtual movements of its employees. There used to be a time not so long ago when no tools existed that could sniff their way past a switch and onto other local broadcast domains or VLANs. Today powerful tools such as Dsniff exist that are just too powerful to ignore. With Dsniff a user could listen on the wire and learn any sensitive information that has been handled by a switch. Dsniff is a collection of tools that allow the user to sniff switched networks and even to hijack connections that are going through the switched matrix. Even when running encryption software such as OpenSSH to encrypt the data on the wire, the risk of session hijacking is still great. For this reason Dsniff can only be countered by user training. Employees must be taught about session hijacking and be aware of the danger of not reading what onscreen messages say and accidentally agreeing to a potentially insecure connection.

Wireless technology poses a great security threat, for obvious reasons as doors; walls and locks are meaningless when the data just goes through the air. Any user with a laptop and a wireless access card can access any company network unless some logical barrier is in place. Most wireless devices are shipped from the manufacturers with security disabled. Be very cautious when planning to implement wireless technologies and know the boundaries of the wireless signal. An intruder could use the wireless access points to infiltrate the network and does not even need to be on company property. For example, there is a user with a laptop with a built-in wireless card. An intruder could tap into the network connection while the computer is booting up or after the user has connected to the wireless network. In effect the intruder is piggybacking on top of the connection and acquiring access to the corporate network undetected.

The key to securing the wireless infrastructure is that all information needs to be encrypted when transmitted. Users of the wireless network must be well trained in company security procedures and guidelines. Currently there are two options available to securing wireless LAN (WLAN). The first one is IEEE 802.1X for authentication and key management, plus Wired Equivalent Privacy (WEP), which provides strong authentication between a server and a client. The second method is to use IPSec VPN, which uses the encapsulating security protocol (ESP) to provide data confidentiality and integrity by encapsulating the data. Additional security measures include:

- Change the default SSID name
- Disable SSID broadcasting
- Change all access points administrator password
- If an access point uses SNMP, disable it

What would we do today without e-mail? Today E-mail and the Internet have become valuable tools for employees who use them for work and for recreational activities. "Upwards of eight million working hours are lost each year in the UK by employees surfing the Web (cyberslacking). Even legitimate surfing poses a threat to IT security." [9]

The sending and receiving of junk e-mail, the creation of spoof e-mails, and just surfing the web can make an organization's security weaker. Employees surfing the web for their own

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

amusement take up valuable bandwidth of those employees that are busy working. E-mail has brought fast global communication to the workplace and is also often the means by which employees send out sensitive information, whether intentionally or not doesn't matter. Even if a company uses some from of e-mail security, this does not check Web mail services such as Hotmail. E-mail is the means by which offensive materials circulate around a company, often causing insult to some people. What one person might find amusing, the next might find deeply insulting. Companies can be taken to court as a result of sexually or harassing internal e-mails. Ever thought about the bad advertising a company gets when an employee sends out a dirty e-mail to his friends, which then send it on to their friends and so on ad infinitum. The message header shows from where the message originated and even which company mail server was used to send it. This might not be the advertising a company wants.

The top level of management is held responsible for anything sent over their network, including all the racially and sexist messages employees send.

> Under the Data Protection Act, companies across Europe are responsible for the personal data they hold on individuals. Even if employees send information out of the company illegally or accidentally, companies are held responsible. The RIP (I think we should define this) Act decrees that companies are also legally responsible for any misuse of their IT networks and can monitor employees' e-mails to prevent or detect crime. However, businesses doing this could be infringing the new Human Rights Act (HRA), which states that employees have a right to privacy and companies must be careful as to the extent of any monitoring they undertake. By communicating a tailored security policy openly, companies can protect themselves and also avoid potentially damaging breaches of Human Rights laws. [9]

Companies need to protect their reputation by controlling all electronic communication. Firewalls and virus checkers are not designed to deal with insulting messages. Companies need to take this threat seriously and begin implementing content checking software that fits the company's security policy. Software such as CS MAILsweeper and CFI MailSecurity for MS Exchange provides policy based email protection. [10]

IT departments always remember to monitor the network because it's fun and technical, but what about the threat from employees installing pirated software onto company machines. This is not so glamorous for IT staff and often the reluctance to audit workstations is all too evident. Piracy is alive and thriving with reports stating countries such as Vietnam and China producing more than 80 percent of all pirated goods, which is a fair market share. Should a watchdog group walk onto company premises and do an audit, it could prove to be very expensive. Microsoft and Adobe formed the BSA to try and tackle piracy in corporate America.

> Vonage is not the first East Coast technology firm that has found itself under the BSA gun. Last week, the BSA announced that four New York area companies agreed to pay a combined total of $222,000 to settle claims relating to unlicensed copies of software programs installed on office computers. As part of the settlement, the four firms agreed to delete any unlicensed copies, purchase replacement software and strengthen their software management practices. [11]

Not only do users on the Internet want to break through your firewall and into the corporate network, they want to use your network to stage attacks on other business entities. Or there might be a few employees who enjoy hacking and have too much spare time on their hands. They then decide to use the company bandwidth to initiate an attack on company X by

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

breaking into the their web server located on the company's DMZ. Company X notices the attack and holds your company responsible.

Any system that directly connects with the Internet is a possible point of compromise. If a DMZ system, which does exchange information with the Internet directly, were to be compromised, it would become a platform for staging attacks against other Internet sites or against the internal network. An organisation should always protect their internal machines by implementing proxies that will communicate with Internet hosts on the workstations behalf. So should there be access lists on routers incoming network interface to prevent spoofing attacks from employees? Yes. Disgruntled employees could potentially spoof packets with addresses of the machines from the DMZ, in order to get them out onto the Internet. Access Control Lists (ACL) are used in many applications, routers and operating systems and provide a means of permitting or denying certain types of packets. ACL's must be applied to incoming interfaces to prevent spoofing, in other words, an ACL must filter packets before they reach the networking device or the spoofed packets will be routed to the intended destination. Always use incoming access lists on routers that stand guard over Internet links and the internal network to prevent the routing of spoofed packets. The last thing a company needs is to be held responsible for any attacks on another organization.

Courts in many countries are finding themselves in unknown territory when it comes to issues on cyber crime and are facing a steep learning curve in creating accurate precedents that will provide the foundation of future international cyber courts. Those court cases that have had to deal with cyber crime have shown that all services running on a machine must contain a banner that does not welcome any potential intruder but must provide a warning message that they shall be prosecuted if they should use this system illegally. Always connect to your open ports to see what banners are displayed and with what information. Banners should exist but they should not give out any useful information to any user about the local system. Tool such as Strobe can check banner messages for you.

Some company's employ large IT teams whose task it is to check every network configuration, and all their employee's workplaces and systems to check if they are in alignment to the security objectives outlined in the security policy. This can quickly become an expensive and monumental task in a large corporation. Another alternative is to use security policy automation software, such as that from Polivec, that checks network configurations against defined policies. Policy automation software monitors the entire network and once it has identified any misconfigurations or errors at the device level, it automatically in real-time corrects those problems found and for some companies might just be the missing link in their security solution.

Closing thoughts

The motivations for the new wave of security policy creation are numerous. Within the company security policy there must be a clear definition of the roles and the associated responsibilities that each member of the security team is assigned.

> Create a cross-functional security team led by a Security Manager with participants from each of your company's operational areas. The representatives on the team should be aware of the security policy and the technical aspects of security design and implementation. Often, this requires additional training for the team members. The security team has three areas of responsibilities: policy development, practice, and response." [12]

No matter what the motivation, security policies are the foundations when it comes to creating and maintaining a secure enterprise.

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

An important idea is that a company must emphasize its security policy from day one. Build security from the inside out so good security starts with whom you hire. Reference checks must be performed and all employees must sign a non-disclosure agreement. Teach users that security starts with them and that they need to take personal responsibility for the information they produce and work with. They need to be taught how to choose good passwords and that they may never tell anyone what their password is, even if the police are asking them for it. Set up access controls that allow a user just enough access to company resources to allow him to do his job. If you do this from day one it will avoid employees getting the impression that access levels have to do with them personally, but are simply a part of a particular job function.

Another key element is making security part of the culture. This can be a tricky process. Those companies that do decide to enforce stricter policies for their employees must be doubly sensitive to informing and educating their employees about the reasons for the change. If this is not done, employees will fill the information gaps with a negative perception that can only harm the company and its moral. Nothing spreads quicker than gossip not even the SoBigF virus. Also to enforce these policies one must punish those that do not adhere to the guidelines and the big question that arises is how to adequately but also not excessively punish them.

Companies need to know how to let go of their staff. Surveys state that being made redundant is one of the top five stresses that a human being can face. A little sensitivity from managers can go a long way in helping to avoid any sabotage or retaliatory attacks. The IT department must communicate closely with the Human Resources department to close down any accounts that are inactive or are about to become. During layoffs, you might want to consider giving those employees that are to be let go all new accounts with limited privileges to take away any temptation for them to cause large-scale damage.

In the end, time spent to limit in-house threats should amount to 80 percent of the time getting people to do the right thing and the other 20 percent should be spent making sure no one is tempted to cross the line. Security is an ongoing process and implementing measures that sound extreme are often the only viable solution. Managers need to allow their security professionals time to research new vulnerabilities. Security professionals are paid for their knowledge and in such a dynamic and volatile field such as security they need time to constantly acquire it. Network security is an immense umbrella of inter-related topics that must all be addressed to provide maximum security.

Always implement a holistic approach when it comes to securing the perimeter. As there are always ever changing conditions, no network will ever be or stay 100 percent secure. The key to avoiding nasty security problems is to understand how technology changes your business and what vulnerabilities are introduced with each new technology. Every company's evolution will be unique depending on the technology it has implemented, its security budget, its business needs and its strategic goals. One thing common to all companies is that they all have employees. Security planning and investments must be ultimately applied to internal practices. Whatever the reasons might be for implementing security, employees can and should become your best defence if they follow and understand the security policy of the company.

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

Bibliography

1. Alex, Salkever. "Revenge of the Laid-Off Techie."
   URL: http://www.businessweek.com/bwdaily/dnflash/jun2001/nf20010626_024.htm
   (26June, 2001)

2. Shon Harris. CISSP All-in-one Certification Exam Guide. California: Mcgraw-Hill/Osborne, 2002. 93-94

3. Sharon, Gaudin. "Corporate Layoffs Create Security Havoc For IT Pros."
   URL: http://itmanagement.earthweb.com/secu/article.php/1380141
   (July 2, 2002)

4. Brian Hatch. Hacking Linux Exposed. California: Mcgraw-Hill/Osborne, 2001. 137

5. Vivienne, Fisher. "Planning Physical Security Strategies."
   URL:http://www.zdnet.com.au/newstech/enterprise/story/0,2000048640,20273606,00.htm
   (10 April 2003)

6. http://trinux.sourceforge.net

7. www.silentrunner.com

8. Drew, Robb. "Breaches More Damaging"
   URL: http://itmanagement.earthweb.com/secu/article.php/1405031
   (15 July, 2002)

9. Raz, Panesar. "Internal Security Threats"
   URL: http://www.itsecurity.com/papers/mime5.htm
   (12 February 2002)

10. http://www.msexchange.org/software/Content_Checking

11. Ryan Naraine. "Pirated Software still an Issue in Hi-Tech"
    URL: http://www.cioupdate.com/news/article.php/2168501
    (21 march 2003)

12. Cisco Systems. "Network Security Policy: Best Practices White Paper."
    URL: http://www.cisco.com/warp/public/126/secpol.html,
    (16 July, 2003)

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

Last Updated: May 1st, 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 London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 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
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
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 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
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 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 Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 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
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
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS