Abstract

This paper focuses on computer security as a profound concern of an organization. Organizations normally find that putting together a security policy that restricts both users and attacks is time consuming and costly. Users also become disgruntled at the heavy security policies making their work difficult for no discernable reason, causing bad politics within the company. Planning an audit policy on huge networks takes up both server resources and time, and often organizations take no note of the audited events. A common attitude among users is that if no secret work is being performed, why bother implementing security.

There is a price to pay when a half-hearted security plan is put into action. It can result in unexpected disaster. A password policy that allows users to use blank or weak passwords is a hacker's paradise. No firewall or proxy protection between the organization's private local area network (LAN) and the public Internet makes the company a target for cyber crime.

Organizations will need to determine the price they are willing to pay in order to protect data and other assets. This cost must be weighed against the costs of losing information and hardware and disrupting services. The idea is to find the correct balance. If the data needs minimal protection and the loss of that data is not going to cost the company, then the cost of protecting that data will be less. If the data is sensitive and needs maximum protection, then the opposite is normally true.

Computer security is a huge topic and can’t be covered in just a few pages, so we hope to give a few worthwhile information on just a few quick points.

1. Introduction

Computer security involves safeguarding computing resources, ensuring data integrity, limiting access to authorized users, and maintaining data confidentiality. Effective computer security therefore involves taking physical security measures (to ensure hardware and media are not stolen or damaged), minimizing the risk and implications of error, failure or loss (for example by developing a resilient back-up strategy), appropriate user authentication (for example by employing strong passwording), and possibly the encryption of sensitive files. We live in a world where "information wants to be free" and in which people are getting used to having access to whatever information they want anytime, anywhere and from a wider and wider range of computing devices. Unfortunately, in terms of the security and control of the resources to which computers permit access, this can prove quite a problem. Indeed, many users unfortunately often view security and control measures as inhibitors to effective computer use. Computers and networks originally were built to ease the exchange of information. Early information technology (IT) infrastructures were built around central computers or mainframe solutions while others were developed around the personal computer. What some thought impossible became reality and today businesses are being driven by the power of the personal computer that users access with just a user name and password. But as the information revolution opened new avenues for IT, it also opened new possibilities for crime. Attackers used these opportunities to steal passwords and gain access to information or to create disastrous effects on networks and computers. For example: Activist group RTMark attempted to justify its attack on eToys' Web site by citing the eToys versus etoy case as the victory of corporate greed over art and freedom of expression. Declaring a war of revenge against eToys, RTMark sought to rally the public to use a denial-of-service tool called FloodNet to saturate the eToys.com site with network ping floods. RTMark also engaged the help of the Electronic Disturbance Theater; a hacker group claiming to attack sites only on behalf of social causes to help cripple eToys or deface its Web pages. "We're going to make an example of them," claimed Ray Thomas, a San Francisco-based accountant and RTMark's spokesman, describing how the group wants to "destroy" eToys.

2.1 Understanding attack types an organization can encounter

Due to the complexity of software and networks today, most organizations are susceptible to a number of different types of security attacks. Understanding the different types of attacks and methods that hackers are using to compromise systems is essential to understanding how organizations can secure their environment.

There are two major types of attacks:

- Social engineering attacks
- Network attacks

2.2 Social Engineering

With a social engineering attack, the attacker compromises the network or system through social interaction with an individual, through an e-mail message or phone call, and tricks the individual into divulging information that can be used to compromise security. The information that the victim divulges to the hacker would most likely be used in a subsequent attack to gain unauthorized access to a system or network. The key to protecting yourself and fellow employees from social engineering attacks is education! Keeping all personnel aware of the popularity of social engineering attacks and the different scenarios that could be examples of social engineering attacks will help raise the security level of the organization.

There are a number of different examples of social engineering attacks. The following are some of the most popular scenarios:

- Hacker impersonates administrator: In this example, the hacker may call the employee and impersonate the network administrator. The hacker will try to convince the employee to change their password or divulge password information.
- Hacker impersonates user: In this example, the hacker calls an unsuspecting network administrator and plays the role of a frustrated user who cannot log on to the network. The network administrator naturally helps the user by resetting the password and helping them log on; problem being it is actually the hacker!.
- Hacker impersonates vendor: In this example, the hacker may e-mail a customer pretending to be the vendor of a piece of software. In this example, the hacker tries to get the user to install an update, but the user doesn't realize the update is really a Trojan virus that gives the hacker access to the system.

2.3 Network-Based Attacks

Most types of attacks are considered network-based attacks where the hacker performs the attack from a remote system. There are a number of different types of network attacks:

- Eavesdropping attack: This widely used type of attack typically involves the use of network monitoring tools to analyze and read communications on the network.
- Spoof attack: In a spoof attack, the hacker modifies the source address of the packets he or she is sending so that they appear to be coming from someone else. This may be an attempt to bypass your firewall rules.
- Hijack attack: In a hijack attack, a hacker takes over a session between you and another individual and disconnects the other individual from the communication. You still believe that you are talking to the original party and may send private information to the hacker unintentionally.
- Denial of service: A denial of service (DOS) is a type of attack that causes the system or its services to crash. As a result, the system cannot perform its purpose and provide those services.

- Distributed denial of service (DDOS): The hacker uses multiple systems to attack a single target system. A good example is the SMURF attack, in which the hacker pings a number of computers but modifies the source address of those packets so that they appear to come from another system (the victim in this case). When all of these systems receive the ping request, all systems will reply to the same address, essentially overburdening that system with data.
- Buffer overflow: A buffer overflow attack is when the attacker sends more data to an application than is expected. A buffer overflow attack usually results in the attacker gaining administrative access to the system in a command prompt or shell.
- Exploit attack: In this type of attack, the attacker knows of a security problem within an operating system or a piece of software and leverages that knowledge by exploiting the vulnerability.
- Password attack: An attacker tries to crack the passwords stored in a network account database or a password-protected file. There are three major types of password attacks: a dictionary attack, a brute-force attack, and a hybrid attack. A dictionary attack uses a word list file, which is a list of potential passwords. A brute-force attack is when the attacker tries every possible combination of characters. With brute force a file is not read. A hybrid attack is similar to a dictionary attack in that it uses a word list file, but it also places numbers at the end of the word to catch passwords that are not dictionary words because the user placed a number at the end. For example, a dictionary attack would not find the password “pass1,” but a hybrid attack would.

3.1 Guidelines for protecting an organization’s network

There are number of concepts that can be applied to your network to help secure the company and its data. This section is intended to provide a best practice guide to guarding your corporate investments. Although it is not designed to be a complete list, this section outlines common practices that should be followed to help create a more secure infrastructure. One of the most important things to understand about network security is that you should take a layered approach to securing network data. In other words, don’t focus too much on just one area of protection but implement all layers of protection.

3.2 Physical security

Physical security plays an important role in any security plan. If someone can get physical access to a system, you can pretty much guarantee they will have access to the system. It is important that you take the necessary steps to ensure physical access to systems is controlled.

The following is a list of physical security measures that should be considered:

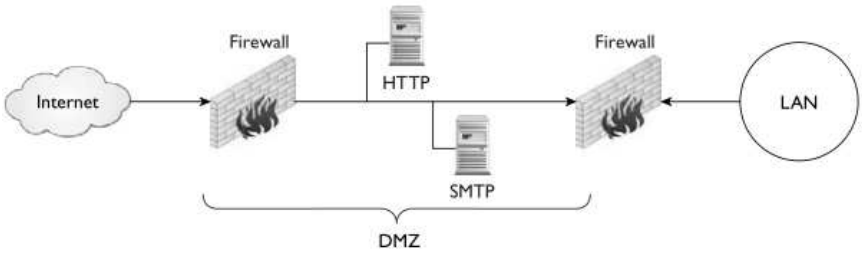
- Physical perimeter security: In high-secure environments a fence is placed around the perimeter of the location and a guard at a gate is used to control who gets access to the premises.

- Swipe cards: Within the facility you can control access to different areas with swipe cards or keypad locks.
- Locked doors: It is important that critical systems be locked in a room and access to that room be controlled. Servers should be placed in a locked server room so that physical access to the server can be controlled.
- CMOS settings: You can change a number of CMOS settings on the system that deals with physical security. For example, you can ensure that the system cannot boot from CD-ROM. If someone can boot from CD-ROM, that person can load his own operating system and potentially bypass security. You can also disable ports such as USB ports in CMOS, which will ensure someone is not using a thumb drive to take data away.

3.3 Firewalls

One of the first things an organization should do to protect their network from attacks from the Internet is to make sure that they have a firewall between their corporate systems and the Internet. In addition, they should create a demilitarized zone (DMZ), which is an area on the network where you have selected certain data from the Internet to pass through and reach selected services, such as a web server.

The figure below displays a DMZ created by configuring two firewalls; one firewall allows HTTP traffic destined for port 80 to pass through it, and the second firewall connects to the private LAN and allows no traffic to pass through it, essentially protecting internal resources.



A DMZ is used to publish servers while maintaining security through controlled access to those servers. The DMZ is also used to protect the private LAN. When designing your firewall strategy, do not be afraid to create multiple layers of firewalls by using multiple firewalls and allowing certain traffic to pass through different resources. Also, when using multiple firewalls, be sure to use different vendors for each firewall so that if there is vulnerability in a firewall and a hacker learns this and bypasses the security of the first firewall, the hacker cannot get past the second firewall using the same technique. For additional security, consider installing personal firewall software on every device on the LAN.

3.4 Product Updates and service Packs

A number of people believe that if they have a firewall they are safe from network attacks a belief that most hackers hope for. The firewall can help protect us against data or services that we have not requested, but what about services that we ask for, such as e-mail? Hackers can attack the system by sending an e-mail that includes an attachment, hoping you open the attachment, which will then attack your system. This is why it is so important that you not open or run any program from an e-mail whose source you are not familiar with.

3.5 Intrusion Detection Systems

As part of your security best practices you may look to install an intrusion detection system, an intrusion detection system (IDS) is a security device that monitors system or network activity and then notifies the administrator of any suspicious activity. The IDS is an important device to complement the firewall because it will notify you not only of suspicious activity against the firewall, but also of suspicious activity inside the network.

There are two types of intrusion detection systems:

- Host based: Host-based intrusion detection systems monitor the local system for suspicious activity. A host-based IDS is typically a piece of software installed on the system and can only monitor activity on the system the IDS was installed on.
- Network based: A network-based IDS monitors network traffic for suspicious behavior. A network-based IDS has the capability of monitoring the entire network and comparing that traffic to known malicious traffic patterns. When a match is found, an alert can be triggered. A network-based IDS can be software loaded on a system that monitors network traffic, or it can be a hardware device. Intrusion detection systems can be either active or passive. An active IDS will monitor activity, log any suspicious activity, and then take some form of corrective action. For example, if a system is doing a port scan on the network, the IDS may log the activity but also disconnect the system creating the suspicious action from the network. A passive intrusion detection system does not take any corrective action when suspicious activity has been identified. The passive IDS will simply identify the activity and then log to file any information needed during an investigation. The passive IDS does not take any corrective action.

5.1 Disaster recovery and fault tolerance

Nobody can stop nature from taking its course. Earthquakes, hurricanes, floods, lightning, and fire can cause severe damage to computer systems. Information can be lost, downtime or loss of productivity can occur, and damage to hardware can disrupt other essential services. Few safeguards can be implemented against natural disasters. The best approach is to have disaster recovery plans and contingency plans in place. Other threats such as riots, wars, and terrorist attacks could be included here. Although they are human-caused threats, they are classified as

disastrous. Fault tolerance is the concept of duplicating devices such as drives, power supplies, and network links so that if those components fail, another one becomes operative right away. If for some reason the fault tolerance plan is not effective, a disaster recovery procedure would be in place to help recover from such failures.

5.2 Fault Tolerance

Fault tolerance is the concept of ensuring that systems will continue to function because a solution has been created that involves having backup copies of power supplies, hard drives, and network links. If one of the links goes down, there would be another link ready to kick in at any time, reducing downtime and ensuring an available solution to clients on the network. The following is a list of widely used fault-tolerant components found on the network.

- RAID solutions: Redundant Array of Independent Disks (RAID) is the concept of storing redundant data on additional drives in case one drive in the RAID solution should fail. RAID solutions can apply to hardware or software. The hardware solution involves having a RAID controller that controls the RAID array, whereas in a software solution the RAID solution is managed by software such as the network operating system. The software solutions are cheaper, but the hardware solutions offer better performance and are more flexible.
- Power: A number of network devices such as servers support a fault-tolerant power source such as a power supply in case the original power supply fails.
- Network link: In a number of networking environments a fault-tolerant network link is created to ensure that one network location can communicate with another location at all times or that there is a constant connection to the WAN environment or Internet. A number of business applications require a network link at all times; therefore, when you design the network infrastructure, you should decide whether the organization requires a fault- tolerant network link.

5.3 Disaster Recovery

Disaster recovery is a matter of ensuring that you can help the company recover from any kind of disaster. When preparing for disaster, you need to make sure that your disaster recovery plan includes backup and restore plans, contact information for product vendors, and step-by-step instructions on how to recover each part of your information systems. The disaster recovery plan should contain detailed steps for recovering from any kind of data loss or physical disaster. The step-by-step plan should contain the location of backup tapes, specify which tapes to restore in different scenarios, and list the steps for rebuilding servers, including detailed information on what to do when a disk fails and how to replace and rebuild the data. A number of disaster recovery documents overlook key elements such as location of software and CD keys needed to rebuild the system. Be sure that contact information for hardware and software vendors is included in the plan so that if you need to replace an item such as a disk

you can contact the vendor. Along with detailed recovery steps, a disaster recovery plan should contain detailed information on backup and restore strategies, offsite storage, hot and cold spares, and hot and cold sites.

6.1 Backup and Restore Strategies

If you have not created a strong backup plan that specifies what to back up and how frequently, you may not be able to recover from disaster. Be sure to review your backup strategy and make certain that you have all the necessary data stored on backup media. You should periodically verify that you can actually restore data using a test environment. Further, make sure that you know and have documented the restore strategy to implement when disaster strikes.

6.2 Offsite Storage

It is absolutely critical that you store a copy of the backups offsite in a secure location. You cannot totally rely on the backups stored on your own site, because they will be of no value if the building burns down, destroying all your servers along with the tape backups stored at the location. You must make certain a copy of the backups is stored offsite.

6.3 Hot and Cold spares

When preparing for recovery, organizations typically maintain spares of equipment ready to be used in case of device failures. For example, they may have a spare power supply, hard drive, or network card available in case the original one fails. By having the spare available, you don't need to wait for a part to be delivered to your facility after a device has failed, creating excessive downtime. With a spare available, downtime is minimized. There are two types of directions that you can take with spares, listed as follows:

- Hot spares: A hot spare is a spare component that is typically connected and powered on in case the primary device should fail. When the primary device fails, failover kicks in, allowing the spare device to take over the workload immediately. No time is needed to connect the device or power on the device; hot spares are ready to work.
- Cold spares: A cold spare is a device that is not powered and is usually sitting on a shelf in a server room. A cold spare involves an increase in downtime, because the device must be connected and powered up before it can take over the function of the original device.

7.1 Hot, Warm, and Cold sites

Disaster involves more than your servers and the data on them; you need to ask yourself, "How can I continue business in the event of a disaster? What if my building burns down? Where can my employees perform their work and continue business operations?" You need to investigate whether your organization will invest in an additional work location, known as a site, in case the original office building becomes unavailable because of fire, flood, or an

extended power outage. When deciding on an alternative location, or site, to continue business operations in the event of a failure, you must choose among a hot site, a warm site, and a cold site. Each site type is explained as follows:

- Hot site: A hot site is an alternative location that provides adequate space, networking hardware, and networking software for you to maintain business operations if disaster strikes. This hardware and software should include any data that would be needed by your staff in the event of a disaster, so the provider of the hot site should ensure that the data is up-to-date and the hot site is ready 24/7 if your organization needs it.
- Cold site: A cold site is an alternative location where you typically have arranged to have the space available but not the networking hardware or networking software. Providing the hardware and software would be your responsibility in the event of a disaster. A cold site takes time to prepare following a disaster because only the space is made available.
- Warm site: A warm site occupies the middle ground between a hot site and a cold site. It is an alternative location with office space and spare networking equipment, such as a server and backup devices, so that you can quickly restore your organization's network in an emergency.

8.1 Training and Awareness

One of the most overlooked security measures that can be taken within any organization is training and awareness. It is vital to the success of any security protection program that all employees within the organization are given seminars that make employees aware that their actions could cause security incidents. One of the best examples is an employee password. Passwords should be changed frequently, and when they are changed, they should be strong passwords (mix of letters, number, symbols, and case). A security manager for a company would ensure that all employees saw a demonstration on how easy a program such as LC4 can crack simple passwords, but at the same time have difficulty cracking strong passwords. This style of training and awareness will show the value of policies such as frequent password changes and the need for strong passwords. If we don't make the employees aware, they won't really care. There are a number of methods that you can use to train employees.

The following are a few popular delivery methods:

- Lunch and learn: A popular method of raising awareness is to have small one-hour sessions during lunch hour. These sessions, termed lunch and learn, are typical short sessions focused on one topic. For example, today there may be a session on protecting passwords, while tomorrow the topic may be physical security.
- Intranet site: You could create training videos and post them on an intranet site for employees to watch. These are typically not as effective because you need to ensure you have control measures in place that ensure employees are watching the videos. You could also post documents on the intranet that explain security best practices.

- Awareness seminars: Instead of relying on lunch time, you could allocate time in the day for short awareness seminars. This is the same idea as the lunch and learn, but you are not using up the employees' lunch time.
- Training courses: A training course is a longer version of awareness seminars and normally goes into a lot more detail. Typically the network administrators will need to be educated on how security compromises are happening and how to protect against them. These courses could range from three to five days in length.

8.2 Vulnerability Testing

The last point about network security is that there are a number of vulnerability scanners available that can scan your network, making you aware of common security mistakes and unpatched systems. These vulnerability scanners can inform you of such things as:

- The number of network administrator accounts
- Group memberships
- Updates that have not been applied
- Weak passwords used by user accounts
- Common security practices not followed

  The foregoing list is a small example of the features available from vulnerability scanners, such as the Microsoft Baseline Security Analyzer (MBSA) or GFI's Languard.

  You can download both of these tools from the following URLs:

- MBSA: www.microsoft.com/downloads
- Languard: www.gfi.com/pages/files.htm

Languard does a better security assessment of your network infrastructure. Languard reports a long list of items to you such as a list of user accounts, groups, permissions, open ports, services that are running, and missing patches. The benefit of a security scanner is that it can scan the entire network and report all of these issues to you in one screen for all the systems on the network.

9.1 Conclusion

This paper presents computer security as a profound concern of an organization, it is worthy to know that you can never have a 100 percent secured system, in one way or the other there are still hidden loop holes for attacks to occur, it just takes time for them to be discovered. This paper also introduced a few best practices relating to securing an organization's resources.

References

Glen, E.C., (2009).CompTIA N+: Certificate Study Guide, New York: McGraw-Hill Publishers

Microsoft (2012) Security threats, https://msdn.microsoft.com/en-us/library/cc723507.aspx

Christopher, B. (2013) Security, http://explainingcomputers.com/security.html