SECURITY ENHANCEMENT FOR TYPICAL CORPORATE NETWORKS

Hans Christian Marwi
Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Atma Jaya Makassar
Alamat e-mail: hansmarwi@gmail.com

Abstract

In the midst of the growing use of the Internet and electronic commerce, security becomes more significant. This paper reported the results of a case study of security enhancement for a typical corporate network. This paper will discuss about the risks and priorities in security. Several methods that should be considered to be implemented in corporate networks will be given. In addition, suggestion to help the improvement will also be provided.

Keywords: *Security, Information, Internet*

1. Introduction

Information is very valuable for every organization that possesses it. In this internet era, information is put at a very high risk since it could be accessed on line from remote areas, whether inside or outside the organization that owns it. To consider about information security means to consider about information protection. Security is a continual process as long as the computer system exists. Stephenson stated that "… security is a means to protect information no matter where it resides or travels on the network"[1].

As a system administrator for a corporate computer system, one should consider many elements to secure the network. They must stay aware of new security issues and then apply new security measures constantly.

2. Literature

Even though security is crucial, a very high security level could not be applied without thinking of the performance of the computer systems. If the security level is too strict, the performance could become low, e.g. slow response of transaction processing system or slow respond of request from web browser. Therefore, performance is important to be measured as well.

Obviously, every element need to be protected, but the level of protection for each element could be varying. The elements are the hardware, applications, and operating systems in the servers and clients. The servers that need to be protected are the application, network, file, web, print, and communication servers.

A security service named CorpInfo Services, informed that [2]

> "the objectives in securing this area are to protect against denial of service, unauthorized disclosure, unauthorized modification of data, unauthorized use of a client, server or application, subversive acts of trusted people and systems, both internal and external, and to ensure that data confidentiality and integrity is preserved, clients and servers are securely configured, configuration management of all clients and servers are ongoing, applications are integrated with no reduction in security".

Typical corporate computer system running with a combination of several operating systems (Windows and UNIX in many variants) and has at least these components:

- Web servers
- Mail servers
- Modem Servers
- Production servers
- Wireless Local Area Network
- A WAN with several LAN based on Bus topology
- Sensitive and insensitive information
- Several more components to support the features of the network.

In this study, the servers would run under a Red Hat Linux operating system, and to integrate the hardware, Samba is used. As a server, Samba shares Linux files and printers with Windows systems. Samba gives Linux users the access to files on Windows System.

The picture of corporate network configuration that was designed can be seen at figure 1.

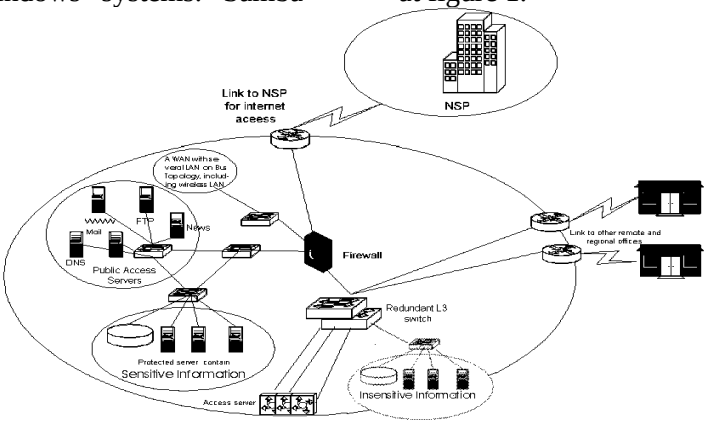

Figure 1 The Configuration of Typical Corporate Network

Strebe claimed that the security zones includes human user, system users, client computers, the network, network servers, data stored on servers, methods used to remotely access the network, the Internet and other public networks[3].

The definitions of each element are as follow.

1. Human Security: it means to legalize potential users before they are involved in the system.
2. User Policy: to regulate the normal use of networked systems by authorized users.
3. Client Security: the practices to make safe client computers from either authorized or unauthorized use.
4. Network Security: control the software, file systems, user accounts and logon methods used to connect to network servers.
5. Server Security: standardize the services and applications that run on servers.
6. Data Security: protects the data stored on servers.
7. Physical Security: defines the measures that secure the containers, spaces, facilities and campuses.
8. Remote Access Security: guards networked systems from unauthorized access via direct remote attachment.
9. Internet Policy: defends the networked systems from unauthorized interference from public networks (the Internet).

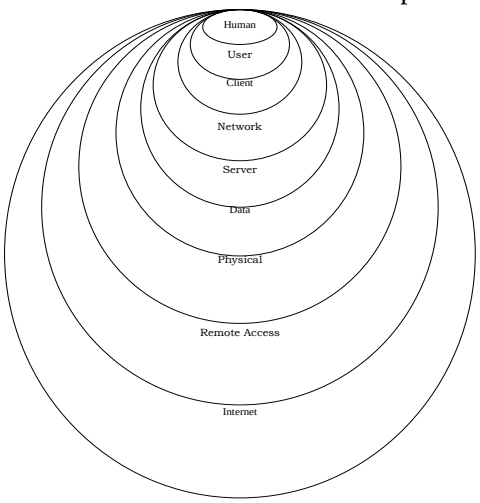

Figure 2 Security Zones
Source: Strebe ("NT 4 Network Security", pg. 741, 1999)

3. Methods to Identify the Risks and Priorities for Security

Risk analysis is to find out what elements that need to be protected, the sources that might attack them, and the ways to protect them. It is the procedure of evaluating all of the risks, and then places those risks into priorities by level of strictness. Garfinkel defined that there are "three key concepts in risk assessment, which are [4]:

- Identifying the assets
- Identifying the threats, and
- Calculating the risk"

3.1. Identifying the Assets

Fraser has adapted one list of categories to identify all the elements that need to be protected which is [5]:

- Hardware: CPUs, modem, boards, keyboards, terminals, workstations, personal computers, printers, disk drives, communication lines, terminal servers, routers, etc.
- Software: source programs, object programs, utilities, diagnostic programs, operating systems, communication programs.
- Data: during execution, stored on-line, archived off-line, backups, audit logs, databases, in transit over communication media.
- People: users, administrators, hardware maintainers. This includes the safety, health and privacy of personnel.
- Documentation on programs, hardware, systems, local administrative procedures, audit records, manual, etc.
- Supplies: paper, forms, ribbons, magnetic media.

3.2. Identifying the Threats

The next stage is to observe to find out what is the potential for data loss. This phase helps network administrators to consider what threats could occur in their computer systems. The following are some threats that they should consider.

- Illegal access to resources or information
- Loss of phone/network services (for a short of prolonged time)
- Accidental or unauthorized disclosure of information
- Denial of service
- Illness of key people (one or many, e.g. epidemic)
- Flood, lightning strike, fire, earthquake, explosion, etc
- Theft of disks/tapes, laptop, PC, etc
- Viruses attack
- Hackers or crackers
- Email spoofing: when one email message appear to have originated from one source when it fact it has been send by the other source.
- Packet sniffing: hackers could to sniff out username/password and confidential information from the network.
- Buffer Overflow: an attack that if succeeded could give the root access to a hacker. This problem is due to the memory management of the software.

3.3. Calculating the Risks

To put the threats in a scale of priority, they must include the cost-benefit analysis, because every action has its own price and advantage. There are numerous difficulties in trying to protect against every possible threat. Risk management is basically the process of identify the risks and decide what to do about them. They must identify the possible cause of the risk, evaluate the possibility of those risks to occur, prioritize the risks based on impact to their corporate priorities, and then plan to minimize that probability. All risks are not equally damaging. Assuming that in Makassar disasters frequency is fairly low, and the level of networked system usage is high, they should list the priority as follows:

- Protecting from inside attackers, e.g. unauthorized access, data manipulation, unintended disclosure of information, etc.
- Daily data backup and maintenance, and full backup each week.
- Protecting against hackers/crackers and viruses with a firewall, e.g. illegal access, denial of service, buffer overflow, worm, etc.
- Physical security, e.g. locks, secure building, guards.

- Insurance from disasters, e.g. an assurance communication link from a phone company in case the circuit being disabled, fire, etc.

3.4. Advance Plans in an Emergency

To handle an emergency situation, they should create an Incident Response Team to cope the incident. These team members would come from various positions and locations in the corporate, and the team leader would come from the Information Technology Department. Their task is to make sure the corporate system would run again as soon as possible after a disaster strikes. They should take turn to be ready 24-hours a day to manage in case a vital circumstance appears.

Smith listed the details to prioritize in an emergency as follow [6]:

- Human safety. In case a disaster occurs (e.g. earthquake, fire), human safety should always be given the highest priority.
- Destruction of data. If data loss occurs without having backup of it, it would be a catastrophe for the corporate. Therefore, they should make sure that the data is backed up properly to remote storages, and there is a quick way to access it when it is needed. The backup should be secure from any attacker as well.
- Disclosure of confidential information. Data such as employee or customer information is confidential. If an attacker can gain access to the information, my corporate would lose the customer confidence. Therefore, if an incident happens, they should make sure all sensitive information is secure at its places.
- Loss of Services. If the system is down during the emergency situation, the corporate would lose the use of Information Technology services. To avoid this, they should have a mirror server in a remote place as a backup; hence they could switch the services to that backup server.
- Annoyances. This is least critical, but quite important. They have to make sure that during the emergency (e.g. running a backup server), all users are not annoyed, for example, they still could use the system as usual without having to do additional efforts to utilize it (e.g. they have to create a new account).

3.5. Good Security Practices for Users

The first line of defenses against system abuse is a secure user accounts and passwords. People who want to gain unauthorized access to a system could try to guess the passwords of legal users. This could be done by trying possible passwords from a database (e.g. dictionary attack) or by stealing a copy of my corporate password file then trying to crack the encrypted passwords inside it.

The best way to keep a system secure is to make sure the unauthorized users cannot get into the system. This can be done by teaching legal users about good password security and making sure they stick to good security practices.

To create an extensive defense model, the corporate must educate their users about how to protect their accounts from unauthorized attacks. According to Microsoft this could be done by encourage the users to follow best practices for password protection, as follow [7]:

- Always use strong passwords. Strong password means a password that is not an ordinary word (e.g. combination of letters and numbers), that is difficult to guess, but still easy for the legal user to remember.
- It is better not to write down the passwords, but if passwords must be written down on a piece of paper, store the paper in a secure place and destroy it when it is no longer needed.
- Never share passwords with anyone, even to best friends. We could not predict what they could do with the passwords.
- Use different passwords for all user accounts.
- Be careful about where passwords are saved on computers. Some dialog boxes present an option to save or remember a password. Selecting this option poses a potential security threat, because the password has bigger chance to be stolen.

- There is a limit for failed logons allowed (e.g. wrong password is entered many times) before the system locked out

3.6. Enforce Security for User Accounts and Passwords

Good passwords commonly are hard to estimate, since they have the rules as follow:

- A combination of uppercase and lowercase letters
- Contain digits and/or punctuation in addition to letters
- Could include special control characters and/or space
- At least eight characters long
- Easy to remember by the users, so they do not need to write them down.
- Nevertheless, a good password that is being used for a long period could turn to be a bad password, because the passwords files could be stolen and cracked or somebody could see it when it is being typed by the legal users. To avoid this, several rules could be applied:
- One time password, "a password that is used only once". For example, the computer may prompt out a number that my user have to calculate (using a formula with a calculator) and the result would be the password [8].
- Bott suggests that "password should be changed at least every 90 days"[9]. An attacker could try a technique to guess every combination of letters, numbers and characters. This effort could take months to succeed, but if the password is never changed, then the attacker could gain the access. By changing the password, we have limited the possibility of the attacker to be succeeded with their mission. To complete this task, I should enforce password history rule setting so that several previous passwords are remembered. With this rule setting, my users cannot use the same password when their password expires.

3.7. The Protection against Physical Attacks

To protect a system against physical attacks, they should apply the following rules [09]:

- Any computer contains sensitive information should be put in a room with a locked door, and only legitimized users can enter that room. This way, an intruder could not gain unauthorized access to the computer.
- To prevent a computer being stolen, they should use external locks to physically bolt a computer to a desk.
- If a computer is not being used (e.g. the user is not in front of the computer) for a length of time (e.g. ten minutes), it should be locked or the user should logged out before leaving the computer.
- Restrict physical access to servers, allowing access only to those people who are supposed to use the servers. This includes the wiring closets and important network elements like file servers, modem and routers.
- There should be security officers to guard the servers 24-hours a day.
- Fire distinguishers and other emergency tools in every room in case the attackers are trying to sabotage my system by setting a fire or a bomb.
- For a LAN which is wireless, they have to obtain an extra effort to secure it. Anyone who has computer with a wireless adapter can attempt to connect to the network. Therefore, they should disable remote administration of the access point, change the network name (SSID – Service Set Identifier) of their access point so it would not match the hardware defaults, turn on Wired Equivalent Privacy (WEP encryption) and set strong keys, and using virtual private networks for wireless connection. By encrypting the wireless transmission, even though attackers could gain access to the system, it would be hard for them to get the plaintext.

3.8. The Protection against Denial of Service Attacks

Maiwald defined Denial of Services (DoS) attacks as "attacks that deny the use

of resources to legitimate users of the system, information, or capabilities". Actually, these attacks are simply hacker's vandalism that could be broken down as [10]:

- Denial of access to information. The attackers may have moved the location of some files, erase them or change their form from one into another (e.g. change a database file into a binary file), that result in unavailable access to the files.
- Denial of access to applications. The attackers could do the same things to the applications (e.g. EXE files), which would make my corporate cannot perform some tasks.
- Denial of access to systems. This type of attack, if succeeded, would make my corporate computer system totally down.
- Denial of access to communications. A sample of this attack is cutting my network cables/wires or sabotage my wireless broadcast. Even though the system is still running, some users could not gain access to the servers.

The wires and wireless systems could be protected physically, and the rest could be protected with a strong password, but it is quite hard to protect the system if the hackers were attacking the routers (including firewalls, proxy-servers, etc.) or flooding the network with extraneous traffic.

An attack on the router is intended to cause it to stop forwarding packets, or to forward them improperly. This could be done by modification of the configuration, the injection of a false routing update, or a "flood attack" (i.e., the router is bombarded with un-routable packets, causing its performance to degrade).

Fraser stated that "the solution to most of these problems is to protect the routing update packets sent by the routing protocols in use (e.g., RIP-2, OSPF)" [5].

To perform this protection, there are three steps:

- clear-text password,
- cryptographic checksum, and
- encryption.

The rule of protection with password is similar to section 3.4. The next one is cryptographic checksums, which protect against the insertion of fake packets, even if the attackers have direct access to the physical network. Combined with a series of number or other unique identifier, a checksum can also protect against "replay" attacks, in which an old (but valid) routing update is retransmitted by either attackers or a misbehaving router. The complete security is provided by fully encryption of sequenced routing updates. This prevents attackers from determining the topology of the network.

3.9. The Protection against Outside Attacks

Outside attacks could be an intruder (hacker/cracker), a worm, a Trojan horse, a virus or any other form that could bring my network system down. To secure their network from outside attackers (mainly over the internet), network administrators must protect the web server, mail server, production server and modem server.

Schweitzer, stated that the most often used methods to protect servers are [11]:

- Erasing unused or unrelated software
- Fixing software flaws and shortcomings
- Using internal or external firewalls
- Remote administration security
- Recognizing attacks to the web site (by applying network and host based intrusion detection).
- Restricting an intruder's access when he is caught
- Protecting the reminder of the network when an attack is detected

For the web server, they should protect the directories with access control (e.g. AuthGroupFile, AuthUserFile, AuthNane, etc.), allow only the control of *safe for initialization* in ActiveX, and use cookies to obtain information from my users.

For the mail server, they could use PGP encryption with digital signature as a default, apply packet filtering feature for their routers to prevent spoofing e-mail, and block some files when they came as attachments in e-mails (EXE, BAT, COM, etc.) to avoid possible danger (e.g. virus, Trojan horse, etc.). In addition, they should educate their users not to download any file that is coming from unknown/in trusted sender.

For their production server, they could use XML signatures and XML encryption in order to make transactions safer in case a hacker breaks in to their system.

For their modem server, they should not allow users to install a modem line without proper authorization. This includes temporary installations (e.g., plugging a modem into telephone line for several hours). They should maintain a register of all their modem lines and keep their register up to date. They should perform regular (if possible automated) site checks for unauthorized modems.

3.10. Updating Systems and Coping the Security Risks

After they developed a complete security policy and have developed procedures to assist in the configuration and management of their corporate network in support of the policy, the next step is to review policies and procedures on a regular basis. This is due to the fact that the technology is always changing; therefore they have to update their system to cope with the new technology, which would lead to new security risk that need to be consider as well. Fraser suggests several steps that I could follow to obtain this [5]:

- Subscribe to advisories that are issued by security incident response teams (e.g. CERT Coordination Centre) and update their system against those threats that apply to their site's technology.
- Monitor security patches that are created by the vendors of their network equipment, then obtain and install all patches that apply.
- Actively watch the configurations of their system to identify any changes that may have occurred, and examine all anomalies.
- Review all security policies and procedures (minimum once a year).
- Read applicable mailing lists and USENET newsgroups to stay current with the most recent information being shared by associate administrators.
- Frequently verify for fulfillment of policies and procedures. This audit should be performed by someone other than network administrators.

4. Result of Securing Data and Information

Since the corporate network contains both sensitive and insensitive information, they should separate the storage in different servers. Insensitive information would only need low level of security, and should be able to be accessed quickly by the users (including people from outside my network). Therefore, the server does not need to be put behind a firewall. Performing authentication and authorization is adequate for users to access this information.

On the other hand, sensitive information server would need to be put behind the firewall (refer to figure 1). Cheswik defined that “a firewall is any device, software, or arrangement or equipment that limits network access” [12]. With the term “any device”, he means could be inside routers, modems, wireless base stations, IP switches, etc.

The levels of firewall filtering in a network protocol stack are:

- Packet filtering
- Circuit level gateways
- Application gateways

For a typical network, they should install a dynamic packet filter, which is a mix of a packet filter and a circuit level gateway, which would give stronger protection, including routing filters.

Nevertheless, firewall is useless from inside attackers. Therefore, physical protection to the sensitive information server should be higher than the others. The server should be put in a locked room where only legitimated staff can gain access to that room. In addition, only high level managements would be given authority to access the sensitive information server on line.

To protect the information from inside attackers, they should apply audit trails. Goggans (“Audit Trails”, pg. 129, 1995) stated that “audit trails are any files that record the time users log in, from where they log in, what they try to do, and any other action an administrator might want to save for later analysis”.

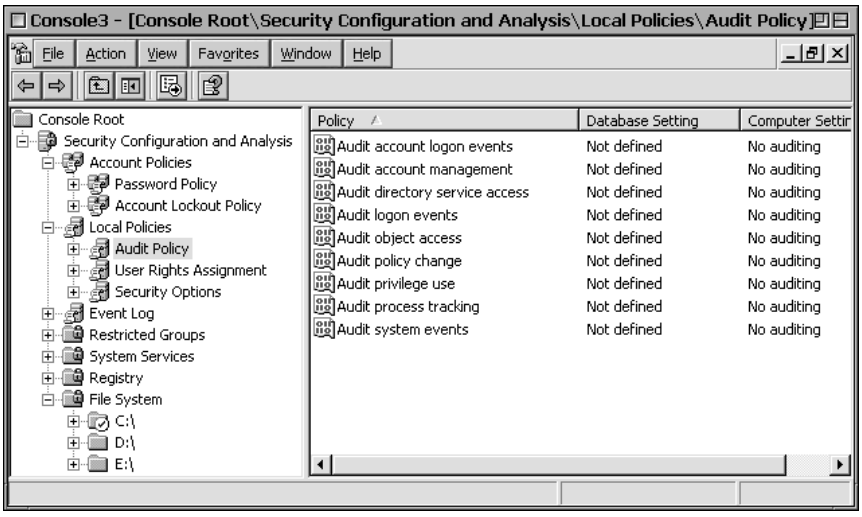

Figure 3 Sample Security Configuration and Analysis in Windows XP

Audit trails can be implemented at any operating system. Figure 3 illustrates an example of audit trails setting under MS-Windows XP Professional. The picture shows an earlier stage of the configuration with database setting "not defined" and computer setting "no auditing" since it was taken from a home PC, with only one user, which is the writer. Figure 4 shows the sample events that occur in the PC. For a corporate server, the setting would be more complicated since it would involve many users.

5. Conclusion

Several methods to enhance security for typical corporate networks system have been introduced and implemented. Those methods should be used together as they are complemented to each other. If one or more components were not implemented then the risks would become higher significantly.

One of the main barriers of the security concerns is to train the users to aware of the risks. Security is tough to achieve if the users were not supporting the rules. Therefore, besides regular maintenance and update to the networks, frequent education for the users is required.

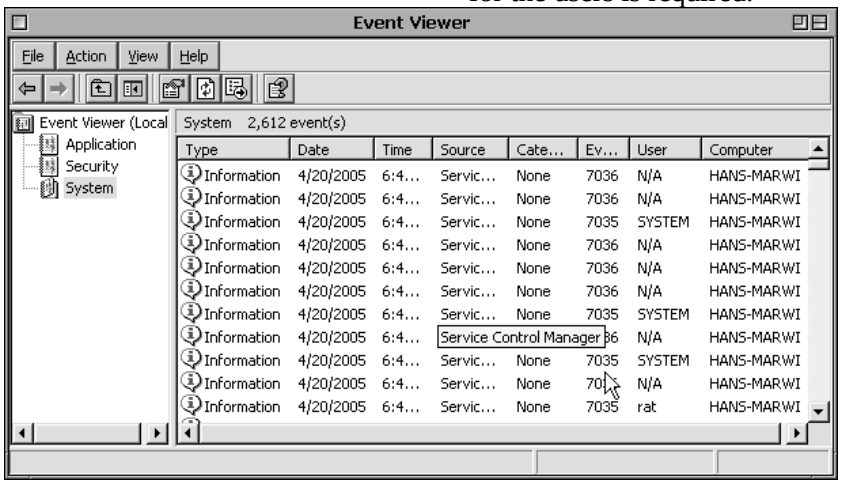

Figure 4 Sample Event Viewer in Windows XP

6. Bibliography

[1] Stephenson, P. (1995a), Definition of Security, in: Implementing Internet Security, New Riders Publishing, Indianapolis

[2] CorpInfo Services (2002), Defense in Depth, A Strategy for Securing Information in Today's Networked Envi-ronment, Available: http://www.corpinfo.com/files/

Defense_in_Depth.doc, (Accessed: 2005, April 17, 15:35)

[3] Strebe, M. (1999), NT 4 Network Security, SYBEX Inc, Alameda

[4] Garfinkel, S. (1995), PGP: Pretty Good Privacy, O'Reilly & Associates, Inc., Sebastopol

[5] Fraser B. (1997), Site Security Handbook, Available: ftp://ftp.isi.edu/in-notes/rfc2196.txt, (Accessed: 2005, April 15, 13:35)

[6] Smith, B. & Komar, B. (2003), Microsoft Windows Security Resource Kit, Microsoft Press, Redmond

[7] Microsoft Corporation (2005), Password Best Practices, Available: http://www.microsoft.com/technet/, (Accessed: 2005, April 16, 10:00)

[8] Garfinkel, S. & Spafford, G. (1996), Practical UNIX and Internet Security, O'Reilly & Associates, Inc., Sebastopol

[9] Bott, E. & Siechert C. (2003), Microsoft Windows Security Inside Out for Windows XP and Windows 2000, Microsoft Press, Redmond

[10] Maiwald E. (2003), Network Security: A Beginner's Guide, McGraw-Hill/Osborne, Emeryville

[11] Schweitzer, D. (2002), Internet Security Made Easy, Amacom, New York

[12] Cheswick, W. R. (2003), Firewalls and Internet Security, 2nd Edition, Addison-Wesley, Boston