Network Security Essay, Research Paper

1.0 INTRODUCTION 2

FACTS AND FINDINGS 2

2.4.1 Passwords 6

2.4.2 Data Encryption and decryption 6

2.4.3 Historical and Statistical Logging 7

2.4.4 Closed User Groups 7

2.2.5 Secure Transmission Facilities 7

2.2.6 Firewalls 7

2.2.7 Physical security 8

APPENDIX B 9

APPENDIX C 9

Security: How do you secure business Information

1.0 Introduction

As we know the need of data communication becomes vital in the 20th century as we call it Information Age . Both business and government were concerned with security and the need for data security becomes evident. Therefore the computer processing, centralised database storage techniques and communication networks has increased the need for security. The concerns about security of an organisation is not directly depend on the data communication related areas but also the control mechanism which implements, restricts and protects the threats from in and out side the organisation. This report proposes the need of security and ways in which the organisations secure their business information will be discussed.

Facts and findings

2.1 What is Security?

Security is the state of mind [1]

An example is mission impossible one of the detective movies who show how easy it is to tap a telephone- Although it is illegal unauthorised access is gained, damage can be done to sensitive data if leaked from one company to another which can provide criminals with the electronic gold mine of fraud opportunities.[2]

so this justifies the need for security.

Many definitions say that security means ..unauthorised access, such as preventing a hacker from breaking into your computer (Fitzgerald and Dennis, 1996, pp426). This statement shows the importance of the computer security, because the computer data storage device such as hard drive and other computer storage devices, which contain the information to use efficiently within organisations, should be prevented. The means of security can also be the physical control of the information that should be prevented from loosing and to be prevented from natural disasters which is called traditional security according to Fitzgerald and Dennis (1996).

2.2 Why Organisations need security?

As discussed above, the organisations in this century more increasingly depend on data communication for the daily business communication, database information retrieval and the internetworking of LAN s. This led the management into more consideration on converting manual operations into computerised systems and relay on them. In fact, organisations then considered that .many potential hazards such as fraud, errors, lost data, breaches of privacy and the disastrous events that can occur in a data communication (Fitzgerald, 1984, pp620). The above consideration statement was considered about fifteen years ago but still holds valid reasons.

Computer and network address three requirements

[1] Securecy

Requires that the information in a computer system only be accessible for reading by authorised personnal or parties. This type of access includes printting, displaying , and other form of disclosure, including simply revealing the existence of an object.

[2] Integrity

Requires that the computer system access can vbe modified only by authorised personnals. Modification includes writting, chaning, changing status, deleting, and creating.

[3] Avalibility Requires that the computer system access are avalible to authorised personnel.

2.3 Do Organisations need a security policy?

The essence of security operations is managing and controlling access to equipment and facilities within an organisation. The crux of the security problem is providing simple and inexpensive access on a wide-reach basis even protect the physical securities from harm and sensitive information from unauthorised users. Therefore, the organisations can define their own security policies and responsibilities for various aspects of security within, which would lead to a great successful in reducing the threat of the organisation. (Keen, 1994). In an article called PC Magazine by Lindhe (1997) brings the same argument that the first step should be either to devise or to revise a comprehensive security policy for the organisations and that should be educated to the employees about their responsibilities for protecting the organisation s information. (Appendix A)

Types of Attacks

There are two types of attacks involved in release of message contents and traffic analysis.

A release of message contents is easily understood . A telephone conversation, an electronic mail message, a transferred file may contain sensitive or confidential information.We would like to prevent the opponent from learning the contents of these transmissions.

The second passive attack,traffic analysis is more sublte. Suppose that we had a way of masking the contents of messages or orther information traffic so that opponent, even if they captured the message, could not extract the informstion from the message. The common technique for masking contents is encryption. If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be use full in guessing the nature of the communication that was taking place.

Passive attacks are very difficult to detect because they do not involve any alteration of the data.

However, it is feasible to prevent the success of these attacks.

Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.

one is Passive attack and active attacks. Passive attacks means the evasdropping on, or monitoring of,transmission. The goal of the opponent is to obtain information that is being transmitted.

ACTIVE ATTACKS

The second major category of attack is active attack. These attacks invovles some modification of the data stream or the creation of a false stream and can be subdivded into four categories:

a) Masqurade

b) Replay

c) Modificattion- of messages

d) Denial- of services

a) A masqurade takes place when one entity pretends to be a different entity. A masqurade attack usually includes one of the other forms of active attack. Like the example given below authentication sequences can be captured and replayed after a valid athentication sequence has taken place, thus enabling an authorised entity with few privileges by impersonating an entity that those priviliges.

b) Replay involves the passive capture of data unit and it s subsequent retransmission to produce an authorised effect.

C) Modification of messages simply means that some porpotion of messages can be altered, delayed or recorded to produce an unauthorised effect.

D) The denial of the service prevents or inhibits the normal use or management of communication facilities. Another form of service denial is the disruption of an entire network or by disabling the network or by overloading it with messages so as to degrade performance.

Active attacks present the opposite charecteristics of passive attacks, passive attacks are difficult to detect, measures are avalible to prevent thier success. It is difficult to prevent active attacks absoultley, as to do so would require physical protection of all communication facilities and paths at all times. Instead, the goal is to detect them them and to recover from any distruption or delays caused by them

These attacks happen by:

Above is a diagram of normal flow of data

Interuption An asset of the system is destroyed or becomes unavalible or unusable. This is an attack on avalibility. An example of this is disabling, cutting communication link or the disabling of a file managment system.

Interception

Interception is when an unauthorised personnal gains access to an asset. This is when an attack is on confidentiality. E.g wiretapping or copying of files. Below

Modification

Modification is when when a personnal gains access to data this is an attack on the integrity . (eg altering the message being sent or program)see below:

Fabrication

Fabrication is when a person inserts counterfiet objects into the system. This is an attack on authentication . an example of this is when the insertion of spurious messages in a network or the addition of record file.

2.4 Methods of securing business information

Most of today’s network needs to meet all possible security measures in terms of securing the business information. The protection against the business information is depends on how much security issues concerned and these can be distributed through data communications and ” can be implemented through host computers, terminals, modems, special security devices, and even transmission facilities” (Beyda, 1996, pp118).

2.4.1 Passwords

Password is very important to each single user of a network and to the entire network, therefore an article in Windows NT Magazine by Smith (1998) it is suggested Passwords are the keys to your corporate network and they can fall into the wrong hands just as physical keys can (Smith, 1998, pp127). This statement gives a clear and make any network user or any person who reads this statement to think that how much is a password valuable to a network user. It is not a thing to be shared with other users. Each user is alone responsible for the security of their account by protecting the passwords. If unauthorised access is allowed into the network through an individual s account, the entire network is at risk. It is even possible for persons outside the environment to run programs designed to gain unauthorised access to the particular account. Therefore the users should make ’secure’ and ‘quality’ passwords (Appendix B).

2.4.2 Data Encryption and decryption

Why Should I encrypt my mail ?

You should encrypt your email for the same reason that you do not write all your correspondence on the back of a post card. Email is actually far less secure than the postal system. Take a look at the header of any email message that you receive and you will see that it has passed through a number of nodes on it s way to you. Every one of these nodes presents the opportunity for snooping.

Encryption is a process of distinguishes information whereas decryption is the process of restoring it to readable form. These two processes need perform the encryption task, otherwise it will not make sense. When a user sends a message usually a text message, which is known as a ‘clear text’ or ‘plain text’ to an encryption device. Once it encrypted it is called ‘cipher text’ ( Beyda, 1996). This is from the encryption device of the sender to the receiver’s. Once the ‘cipher text’ reaches the receiver’s encryption device the message again will be ‘decrypted’. Therefore it would not be possible to understand the data which passes through public data networks, satellite or microwave for those who eavesdrop. Even though hackers can break an encryption method, it will make difficult, take more time and powerful resources that are needed.

The encryption method can also use ’secret keys’, which are the keys for the algorithm and it should be kept secretly as oppose to ‘public’. Accepting a large amount of keys which can be reduced for a single ‘clear text’ then it would be a tedious job for a hacker to do an exhaustive computer search would take an inordinate amount of time or would cost more than the value of the encrypted information.

However, the strength of the security lies in maintaining the secrecy of the encryption and decryption function of the message of a sender and receiver. This function is called ’secret key’ encryption-the key needed to decrypt a message which is different from the one used to encrypt is a ‘public key’ (Appendix C). For each employee of an organisation, there is a unique identifier instead of name, address and phone number is called their ‘public key’ that another employee can send message to. However, the received message can only be read if the employees secret key is known. The valuable ‘business information’ and the ‘privacy’ can be maintained within organisations by using these ’security methods’.

An encryption device is normally used to encrypt text, which involves ‘hardware’ and ’software’ combination. The encryption algorithm can be “changed” on a device and it is difficult to determine by anyone by simply looking at an encryption device. However, the algorithm can be changed using the ’software’ that contains all the ‘cipher’ messages. Therefore, it is possible someone can copy the software unless the ‘rights restricted’ and it is dangerous when loosing the ‘key’ as well as the ‘algorithm’ (Beyda, 1996).

2.4.3 Historical and Statistical Logging

All data passing between a server (host computers) and the terminals can be recorded by using a device, and captured in a historical log – this is called ‘historical logging’. This method would help to identify the mystery by ‘replay’ the ‘historical log’ by which user altered the files and folders (For example an employee’s salary increased or decreased) of the server or personnel computer. The same method can be used to identify ’static logging’, which includes the details of users who logged on to which port, total time logged on, the files which are accessed. Identifying the user’s ‘method of access’ as well as ‘action’ can make “business information” more ’secure’ in the ‘future’.

2.4.4 Closed User Groups

2.2.5 Secure Transmission Facilities

2.2.6 Firewalls

I have nothing to hide. Why do I need security/privacy?

Show me a human being how has no secrets from their family ,her neighbors, or her colleagues, and I ll show you some one who is either an extraordinary exhibitionist or incredible dullard.

Show me a business that has no trade secrets or confidential records, and I ll show you a business that is not very successful.

As the Internet becomes a facility used by businesses in their day to day operations, security and integrity are becoming crucial. The need for reliable data communications, their exists an increasing need for security of both the transmitted data as well; as controlled access to the corporate network over which the data is transmitted. [ Internet]

A firewall is a system or a group of systems that enforces an access control policy between two networks. The firewall can be thought of as a pair of mechanisms: one which exists to block traffic, and the other which exists to permit traffic. The most important thing about a firewall is that it implements an access control policy.

Generally firewalls are configured to protect against un-authenticated interactive logins from the outside world. This helps prevent vandals from login into machines on your network.

More elaborate firewalls block traffic from the outside to the inside, but permit users on the inside to communicate freely with the outside. The firewall can protect you against ant type of network-borne attack if you unplug it .

Firewalls are also important since they can provide a single choke point where security and the audit can be imposed. Unlike in a situation where a computer system is being attacked, by someone dialing in with a modem, the firewall can act as effective phone tap and tracing tool.

Firewalls provide an important logging audit ing function ;often thay provide summaries to the administrator about what kinds and amounts of traffic passed through it,how many attempts there were to break into it.

2.2.7 Physical security

(placing the hardware and backup devices-due to theft and disaster)

Physical security files, folders,

People with right mind, attitude, and dishonesty.

Appendix A

For example, awareness training should let people know what to look for, and what to do when strange situations occur. Whatever you do, don t make it into an if you do this, you will be fired type of presentation. This scares people away from security, and encourages them to avoid you. If someone asks someone s password, shouldn t give it to him or her. And let security know about it. The goal is to have hole organisation looking for problems, as oppose to just the owner and the security staff. This way thousands of people helping to protect your information, not just a dozen.

(By Ziff-Davis TV Inc, http://www.zdnet.com/zdtv/cybercrime/spyfiles/jump/0,3698,2127639,00.html information collected on 22/02/99)

Appendix B

Good password means difficult to guess, have both UppEr case and loWeR case letters contain special characters and numbers such as #109$28%G8, it should be easy to remember so users do not need to write anywhere, more than six characters long, it should be typed quickly. So some body wouldn t notice what the user types by looking the keyboard.

Good passwords also include some techniques such as

1) If there are too short words can be combined with a special character or number such as eye-brow .

2) Substitution of numbers for letters such as g1n0la instead of ginola .

The characteristic of bad passwords

1) Persons name or spouse s, parents, pet s, child s, friends, boss s and any bodies name.

2) A word in the English dictionary or a place.

3) Passwords of all same letters and it should always differ from login name and old password.

4) Never change back to the initial password assigned by the computer services for example IT-Centre. (http://www.8j.net/local\_forms/passwd.html)

Appendix C

“Public keys are a common use of asymmetric keys. Though secret keys are easy enough to implement between two users, what if we need to contact many different users, and all of the messages need to be encrypted? It is inefficient to call each person, and make up a new secret key, for each transmission. These calls also jeopardise key security”. (Beyda, 1996)