Example of report on fundamentals of network security

Law, Security

Abstract

The incidence of security threats across networks have been increasing at an exponential rate every year. This increase has also necessitated an increase in the level of security measures to be put in place by organizations in order to safeguard their business from these threats. It is imperative for all the members of staff of the business to familiarize themselves with basic issues and best practices in the implementation of network security. This will go a long way in protecting the organization from the nefarious acts of malicious individuals.

Introduction

In order to achieve a foolproof and security tight business network environment, it is important that all members of staff of the company acquire basic knowledge about how networks work and how to protect them from security breaches. However, it should be stated that such knowledge alone is not sufficient to eliminate all security breaches to the network. It can only take care of some certain problems and help to recognize if indeed there has been a breach. This paper will present some fundamentals of network security with a view to educating the CEO and other staff of the company and as such, prevent practices that can put the network in jeopardy.

It has been said that in the network security schema, people are the weakest link. This is not only because they are the ones that operate the hardware but also because they are the ones responsible for keeping secrets such as access codes and passwords that serve as the basis for implementing network security. All security systems depend on measures deployed to control or monitor access, protect the disclosure of sensitive information and verify the identity of any individual that wants to access the network. A breach in any of these protocols would therefore mean that the network is compromised. Moreover, security breaches can also arise as a result of human error, for instance, failure to change manufacturer provided default settings, including passwords and access codes. This is usually the first level breach that intruders exploit in order to gain unauthorized access to a system. Employees need to realize this and take appropriate precautionary measures.

One of the initial steps to take in securing a network is to have a full extent of the network. This involves having a documented inventory of resources, systems and assets that make up the network. things to be considered includes, but is not limited to servers, storage systems, routers, switches, computer systems, backup power modules, printers to mention just a few. It is important to document the location of all these equipment including dependencies.

Another step is to define the scope of the network with a view to identifying potential threats that can be encountered. Threat could either be internal or external. They may be automated or human based. Viruses can be e-mail viruses, network viruses, web based, server based attack, denial of service attack or even a network user attack.

Physical security of facilities and resources should also be carried out. It is important to control physical access t equipment and network resources as this is critical in ensuring security of the network. Any physical access to an internal site automatically places the site at risk of being compromised. Data, including passwords and secure files can be obtained this way. It is therefore important to keep these equipment in physically secure locations under lock and keys in rooms or secure filling cabinets.

It is also desirable to partition and protect network boundaries with fire walls. It is not only basic to control physical access to the network; digital restrictions should also be created. This helps to deter intruders. This means securing the points at which the network is connected to the outside world - the internet. This can be provided by a firewall.

On the part of the network host, a number of measures also need to be put in place in order to ensure total security of the network. It is important to turn off services that are not in use. This is because these unused services represent a potential opportunity for unauthorized intrusions, attacks by worms and Trojans. It would also not be too much to lock down communication ports that are not in use as they can also be used to initiate attacks on the network. This can easily be accomplished by some software programs. This practice is important for internal protection of the network, especially when other measures have been put in place to secure the network from the outside world.

It is also important to implement a strict username-password management regime. This is usually a bone of contention in most networks. This bottleneck can be circumvented by the use of sophisticated, centralized authentication systems. It is important not to use passwords that can be easily guessed. These include spouse's names, nicknames or even the name of one's favorite sports team. It is also better to use longer passwords and even combine with other characters that are not alphabets. As I mentioned earlier, all default passwords on systems and resources should always be changed. It is important to always give a lifespan to passwords so that they are changed periodically.

It may also be desirable to have an access control list which defines individuals that can access specific resources at each point in time. The list specifies hostnames that are authorized to access particular resources and denies whoever is not on the list this access.

In the case of this credit card company, it is also important to secure information being exchanged over the network so as not to compromise the credit card information of customers. This can be avoided by encrypting the information that is transmitted. this will ensure that even if the information is ever intercepted by a third party, such a person would not be able to make any meaning of the enc1rypted information, rendering it useless to them.

It is not just encryption of data that is needed in preventing data theft. It is also desirable to have s secure connection whenever sensitive data, like customer's credit card details is being transmitted. This will also ensure that no other person can " listen to" the data exchange because the communication line is secure.

Fundamentals of firewalls and VPNs

A firewall is a mechanism by which a barrier is introduced into a network for the purpose of controlling the flow of information into and out of an organizational intranet. Firewalls are application specific routers. A firewall can be software that runs on a general server platform. The firewall would have two interfaces, i. e. one for either side of the firewall- the intranet [which is the internal network] and the internet [which is the external network]. The firewall controls what data is allowed t pass through it to the external network and also determines what data passes from the internal network to the external network. This would depend on how it is configured. A firewall can be fairly simple of very complex. The complexity of a firewall would depend on such factors as the services that need to be protected, traffic level and the complexity of the rules required. The complexity increases concomitantly with a greater number of services that passes through the firewall.

A firewall is like a two-edged sword. If it is configured properly, it can offer protection against a wide range of malicious attacks, including denial of service attack. On the other hand, however, if it not configured properly, it can be the source of vulnerability through which malicious attacks are launched on the network. Also, it can be a huge headache because if not configured properly, it can also deny users legitimate services, thinking it is denying malicious access.

The basic function that the firewall performs is to block network traffic to certain areas on the network, including IP addresses and particular service ports.

Firewall arrangements may involve a firewall placed between the private network and the internet. This would ensure that port restrictions protect the whole of the network. However, this approach may end up preventing people from legitimately accessing the internet so another approach is to designate a virtual Demilitarized zone (DMZ) and deploy two different firewalls. The firewall would serve as the boundaries of the DMZ and the FTP server would be placed in the DMZ. This would ensure that all traffic from the internet terminates in the DMZ and all requests from the internal network pass through the DMZ. In this way, people can still do legitimate transactions and at the same time, protect the network from intrusion attacks. Moreover, the network can also be broken down into several parts and a firewall placed in each part. This would function to limit damage to the network if there were to be an attack on the network. Absence of this could have meant that the whole network would have been compromised.

A virtual private network provides connectivity over a physically long distance without sacrificing the security of the connection. The important feature of the VPN is its ability to make use of public networks, like the internet, to provide secure connections.

Virtual private networks allow data to be transmitted across the internet using the internet as the public infrastructure. VPNs allow an individual to access an intranet network from a remote location. It also allows multiple intranets to be interconnected within an organization. VPNs also allow several networks to be interconnected among several organizations, forming an extranet.

With these capabilities, a VPN can be used to interconnect devices within an organization in a particular location it also possesses the ability to interconnect computers in the same company but at different locations. Also, VPNs can also allow several organizations to interconnect their devices for the purpose of data exchange. In all, VPNs are ideal for global companies that have branches in different locations, even at different parts of the world.

Also, it allows a user to access their information from remote locations. VPNs work based on the client/server model. The VPN client is the end user and it allows remote connection by that device to be connected via a VPN server to another network.

Virtual private networks and Firewalls are separate security solutions that can be successfully integrated into one single security solution. This will eliminate the need to separately configure a firewall and also set up a virtual private network separately. An example of this is the bizGuardian, s software solution that integrates VPN protection with firewall protection. It has easy to set up wizards which would allow computer end users to easily set it up and install on their system. This is ideal for medium sized businesses. I would therefore recommend this kind of software solution to this company.

In ensuring security in this enterprise, there are a number of measures that I would put in place. In securing the network, I would make sure that there is perimeter security, meaning that the network applications are protected from attack from the external network with the provision of firewall protection. I would also make sure that there is data confidentiality and integrity through the provision of security solutions such as Virtual private networks and the use of Secure Sockets layer.

I would also make sure that the network infrastructure is protected from attack by ensuring that each device on the network is not a weak link for intrusion attacks by ensuring that antivirus programs are installed and up to date. I would also make sure that all security software and the operating system are updated regularly so as to keep them up to date. This would ensure that all security updates are installed and up to date. I would also make sure that each user on the network only has access to resources they do not require. It is also common knowledge that physical security of the network and its resources is an invaluable way of securing the network. I would ensure that all equipment that make up the network are all in secure locations under lock and key in order to prevent physical compromise of the network from tampering.

A regular review of the network security activity a period of time is done in order o evaluates the network and review risks and vulnerabilities with a view to increasing security features, if necessary. Also a prompt action would be taken if any system is suspected to be compromised. I would make sure that such a system is taken off the network pending disinfection in order not to serve as the source of infection for other computer systems on the network.

Conclusion

Maintaining a secure network is a collaborative effort that all users of the network must participate in. it requires putting in place a solid security framework that includes a firewall and a Virtual Private Network. It also requires that all the modalities that have been discussed in this paper be put in place in order to ensure a secure network.

Above all, the human effort is most important. Secure passwords and keycodes must be assured by periodic changing. If all these are put in place, I believe that this company will have little or no problem securing its network.

REFERENCES

P Warren (2005). Ten Steps to Secure Networking. Security: ComputerWorld.

B Waring (2007). How to Secure Your Wireless Network : Following A Few Easy Steps Can Ensure That No One Intercepts Your Wi-Fi Traffic. PCWorld; Networking and Wireless. Accessed 7th January 2011 from http://www. pcworld. com/article/130330/how_to_secure_your_wireless_network. html

BizGuard (2004). BizGuard Data Sheet V35. Integrated VPN/Firewall. Firewall Security Solutions Ltd. http://www. bizguard. com

Windows (2012). Why Should I Secure my wireless network?. WIndows. accessed 7th january 2012 from http://windows. microsoft. com/en-US/windows-vista/Why-should-I-secure-my-wireless-network

O Reginald (2009). How do I secure my home Wi-fi Network. CNNTech: Encryption. Accessed 7th January 2012 from http://articles. cnn. com/2009-03-17/tech/pirillo. wireless. security_1_wireless-access-point-wireless-directory-mac-address? _s= PM: TECH

G DeLaet, G Sahauwers (2004). Network Security Fundamentals. 1st Ed. Cisco Press.

C Leidigh (2005). Fundamental Principes of Network Security. white Paper #101. American Power Conversion [APC].