User authentication

Introduction

I was appointed as the new Network Manager for Philadelphia Inc. It is a large multinational organisation which has an extensive network of PCs comprising more than 1000 systems. This organisation relies heavily on its vast network for its day to day operation. Any potential risks need to be identified and minimised as far as possible. Recently a large number of PCs were affected by a virus, causing a work stoppage among the administration and accounting department. Following this incident of large scale virus infection, the company management has decided to completely review all the computer security precautions and procedures in use within the organisation. So, I have been designed to ensure that I can identify potential threats to the security of the organisation's network and formulate appropriate action plans and security policies to minimise the risks.

Research and document the various aspects of network security that need to be addressed including each of the following topics:

Access control

User authentication

Firewalls

Virus protection

Accessing the Internet (15 Marks)

I'm research and document the various aspects of network security that need to be addressed.

Access control

Access control is the methods for imposing controls that allow or deny user access to network resources, usually based on a user's account or a group to which the user belongs. Access control is security features that determine which resources users are permitted to access, what type of access they are allowed, and how many simultaneous users can access a resource at the same time. They ensure data privacy and protection and help maintain a productive computing environment.

User authentication

User authentication is a security feature that allows an administrator to control who has access to the network and what users can do after they are logged on to the network. This might involve confirming the identity of a person, the origins of an object, or assuring that a computer program is a trusted one. Authentication is the process of determining the identity of a network user by verifying a set of user credentials, typically a user ID and password.

Firewalls

A firewall is a combination of hardware and software components that provide a protective barrier between networks with different security levels. Rules for transmitting and receiving information to and from the other network can be established for the firewall so that specific types of items or addresses are not allowed to pass between the networks. It sits between the computer and the rest of the network, and according to some criteria, it decides which communication to allow, and which communication to block. Firewalls protect a computer or network from unauthorised access and attacks designed to cripple network or computer performance. Moreover, it is also a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all computer traffic between different security domains based upon a set of rules and other criteria.

Virus protection

Virus protection means securing data from viruses that is designed to destroy data or make the computer or network operate inefficiently. Computer viruses are the programs that must be triggered or executed before they can infect the computer system and spread to others. Viruses can then be spread by sharing infected files on a network drive, portable drive, or other media, by exchanging infected files over the internet via e-mail attachments, or by downloading debatable files from the internet.

Accessing the internet

Accessing the internet is the telephone communication system that also covers the world linking telephones together. As with the telephone system, each device attached to the network can be reached through a unique code that represents that device's location. The telephone system access and services are supplied to phone users by an array of competing local, long-distance, and wireless telephone companies, access to the internet is also supplied through a number of access and hosting companies using an array of different connectivity methods.

A user in your company calls to report that she's unable to log on to email. You respond with a couple of quick questions. Because you know that no one else is using the network right now, you cannot determine if the problem is unique to her machine or if the problem affects the entire network. Probing further, you also learn that she’s unable to print. You decide this problem is probably easier to troubleshoot from the user’s computer.

Using the structured troubleshooting method, outline the things you must check and the questions you must ask when you arrive at the user’s office. Based on the possible responses to your questions, describe the actions you will take to correct the potential causes. (10 Marks)

One of the users in our company reports me that she’s unable to log on to her email account. So, I asked her some questions-

How long the duration of your user account?

Do you sure the log on user name and password is correct.

When it starts to unable to log on to your email?

After I arrive at the user department, I check her computer and network. I also learn that she’s unable to print to a network printer. Probing some of the check, other users of this department can able to log on to their email account and can able to print. Therefore, I ask her a couple of quick questions again-

What has changed since the last time you worked?

Have you installed anything on your own?

Are there applications on your computer that aren’t on other computers?

Firstly, I check the power is plugged in, the Caps lock is on, all the cables are attached and network permissions for her computer. Then I check that she can get a connection online or not by browsing Google website and I see there is no connection online. So, I check the Ethernet cable and connection setting. In checking her problem, I document that what I do, so I can undo it if I need to. I use Ping to check the computer can contact an IP address of another PC or not. (Ping is the simplest and most useful diagnostic tool to become familiar with and well worth a few minutes experimentation.) The reply message is “ Request timed out”. It is because of the connection or routing error. Then I restart the computer because 90% of all problems disappear when the computer is restart. To check the router, I Ping the local router, and it fails. So, the problem of the local LAN or the router is sure. Then, I find the router and switch to check the LED display. And I think they are not normal, so I switch the unit OFF, remove and immediately replace the power connection, then switch the unit ON. After it has done, I go back to the computer and retry to Ping the local router. I have successfully sent a message to the local router and receive a response. Then, I check the computer can get a connection online or not, and can able to browse the website or not. Then I see the computer successfully get a connection online. So, I check the email account can be able to log on or not and the printer can be able to print or not. Then I see the problems of the user are successfully solved.

Task 3

Produce a Security Review report, which details the specific threats to network security for ALL of the topics identified in Task 1, namely Access Control, User Authentication, Firewalls, Virus Protection, and Accessing the

Internet, along with your proposed solutions aimed at reducing the risks associated with each threat. (35 Marks)

Access Control

Access control can identify the users, and verify their identity through an authentication process so they can be held responsible for their actions. Good access control systems record and timestamp all communications and transactions so that access to systems and information can be audited later. The primary objective of access control is to preserve and protect the confidentiality, integrity, and availability of information, systems, and resources.

I use role-based access control and rule-based access control to identify the user. Role-based access control systems allow users to access systems and information based on their role within the organisation. It allows end-users access to information and resources based on their role within the organisation. Roles based access can be applied to groups of people or individuals.

Rule-based access control systems allow users to access systems and information based on pre-determined and configured rules. Rules can be established that allow access to all end-users coming from a particular domain, host, network, or IP addresses.

User Authentication

User authentication is an important aspect of network computer security. For network computer, harm can be caused by hacking, malicious messages, viruses, malwares, adwares, email attachments, downloading illegal materials and many other types of activity. Moreover, the secret information of the company can be stolen by the attacker using spywares and Trojan horses.

User authentication will reduce this harm by limiting individual's access to a few systems, rather than the whole Internet. Network operating systems include tools that enable administrators to specify a number of options and restrictions on how and when users can log on to the network. There are options for password complexity requirements, logon hours, logon locations, and remote logons, among others. After a user is logged on, file system access controls and user permission settings determine what a user can access on a network and what actions a user can perform on the network.

So I specify the numbers of options and policies for user authentication. I specify that the password is required for all users of the company, to use the company's computer. The user password length must be typically a minimum of five to eight characters and user passwords must have three of these four characteristics: lowercase letters (such as abc), uppercase letters (such as ABC), numbers (such as 123), and special characters (such as !@#). And I specify the policy that can lock the user account to prevent from logging on, when a user enters an incorrect password five times. According to the user account and password, I control which user can access to the network and what he/she can do on the network.

Firewalls

Firewalls protect against outside attempts to access unauthorized resources, and they protect against malicious network packets intended to disable or cripple a corporate network and its resources. Second use of firewalls placed between the internet and the corporate network is to restrict corporate user access to internet resources.

Firewalls can identify and block remote access Trojans (Trojan horse). Trojan horse is a program that purports to be a useful software tool, but it actually performs unintended (and often unauthorized) actions or installs malicious or damaging software behind the scenes when launched. Sometimes get some program via ICQ or via IRC and believe this program to be something good, while in fact running it will do something less nice to the computer. Such program is called Trojan horses. The difference of a Trojan and a virus is that a virus has the ability to self-replicate and to distribute itself, while a Trojan lacks this ability. A special type of Trojan is Remote Access Trojans (RAT). These Trojans once executed in the victim’s computer, start to listen to incoming communication from a remote matching program that the attacker uses. When they get instructions from the remote program, they act accordingly, and thus let the user of the remote program to execute commands on the victim’s computer.

Firewalls can identify and block remote communication efforts to the more common RAT and by thus blocking the attacker, and identifying the RAT. There are many other types of Trojan horses which may try to communicate with the outside from the computer. Whether they are e-mail worms trying to distribute themselves using their own SMTP engine, or they might be password stealers, or anything else. Many of them can be identified and blocked by a firewall.

So, I run the firewall on the server and all the desktop computers to protect Trojans, malware, and to prevent users from accessing offensive Websites or bandwidth-intensive content that might not be the best use of an employee’s time or the network’s bandwidth.

Firewall devices from different vendors vary quite a bit in configuration details, but they are all based on one premise: Rules are created to determine what type of traffic is allowed to enter and exit the network. To configure a firewall, I build rules that allow only certain packets to enter or exit the network. The firewall can examine all incoming packets and discard packets with a destination address of the network’s restricted segment.

Virus Protection

In internet-connected networks, virus attacks are a regular threat. Users download programs, bring disks from home, memory sticks, and open e-mail attachments are normal computing activities, but they can also bring viruses into the network.

A virus is a program that spreads by copying itself into other programs or documents. Computer virus can attack computer systems and perform a variety of functions ranging from annoying to dangerous. Its individual purpose is to disrupt computer or network operation by deleting or corrupting files, formatting disks, or using large amounts of computer resources. If a server file accessed by other users on the network is infected, the virus can spread through the network in a matter of seconds.

To protect the spread of viruses, one of the most effective ways is to buy virus-protection software from a reputable source. Antivirus software is program that can scan and remove known viruses which have contracted. Most antivirus software is also designed to detect and prevent worms and viruses. The software can also be set to automatically scan disks when inserted into the disk drive, scan files when downloaded from the Internet, or scan e-mail when received. However antivirus software is available in many commercial and open source versions, the license-version of the antivirus software from reputable source is more secure and reliable than others.

So, I run the standard antivirus software from reputable source in server and every desktop computer, and turn-on the scanning features. But by running antivirus software can only protect against viruses that it knows about. Therefore, virus definition files (update files) for antivirus software are needed to download from the internet daily or weekly. To get the maximum protection against viruses on the computer, make sure to keep antivirus definition files current.

Another way to protect the data from virus infection is “ backup the files” which helps to recover the data if the original files infected by the virus.

Accessing the Internet

The internet access is the essential thing to communicate between internal or external organisation for many purposes. Thousands of companies have discovered the pervasive power of the Web in distributing information, selling products, supporting customer service, and staying in touch with clients and customers. By using the internet, we can get important business information which is necessary for competition and improvement of the company.

However the internet is useful for us, but also the internet attack can harm the business. The internet attacks are organised and designed to steal information and resources from the customers and the organisation. Input validation attacks using the Common Gateway Interface (CGI), Active Server Pages (ASP), and Cold Fusion Markup Language (CFML) programs stem from either a web developer or vendor failure. The basic problem happens from the lack of sanitizing the input to a particular script. Without input validation and sanitizing, it is possible for attackers to submit a particular character, along with a local command, as a parameter and have the web server execute it locally. Sometimes, the virtual website of the attackers steals user information and user's credit card details.

If all kinds user can get permission to access the network, the private information of the organisation can be stolen by the attacker using the internet. So that I control the user access to the network resources by using access control and identifying the user account to verify the network permission for the user.

Task 4

Create a set of Acceptable Use Policies for each of the following:

Accessing the WWW

Email Usage

Instant Messengers and chat rooms

Each of these documents should provide a set of guidelines for users which will minimise any associated security threats. (30 Marks)

To minimise any potential risks and associated security threats of the organisation’s network, all the staff of the company should agree the following policies for accessing the World Wide Web, email usage, instant messengers, and chat rooms. All the staff has responsibility to use the resources in an efficient, effective, ethical and lawful manner.

In our organisation, access to the internet is available for the staffs to support informational, educational and communicable. So, staffs should agree the following internet access policies.

Policies for accessing the WWW

The use of Internet is strongly restricted to “ official company business”. Personal use or time spent for personal gain is strictly prohibited.

Authorisation for Internet access must be obtained through your supervisor. Once authorisation is approved you are responsible for the security of your account password and you will be held responsible for all use or misuse of your account. You must maintain secure passwords and never use an account assigned to another user.

Staffs are strongly prohibited to accessing internet websites that contain obscene, hateful, pornographic, politics or otherwise illegal material.

Never copy or transfer electronic files without permission.

Prohibit copying and sending any confidential or proprietary information, or software that is protected by copyright and other laws protecting intellectual property.

Downloading a file or application from the Internet can bring viruses with it. Should be scan all downloaded files with standard virus prevention software before being saved on the company's network.

All downloaded applications must be accepted by the company's IT administrator or company owner before being installed on the company's network.

Hacking into unauthorised areas and other employee's computers are strictly prohibited.

Confidential information is not to be transmitted over the internet without proper encryption.

Introducing any form of computer virus or malicious software into the corporate network is strictly prohibited.

Email usage policy

Email is to be used for company business only. Company confidential information must not be shared outside of the Company without authorisation, at any time.

When conducting company's business, only use the company's official email account for staff such as name@philadelphia. inc.

Staffs are not to conduct personal business using the Company computer or email.

All messages must show the genuine sender information (from where and from whom the message originated).

The representation of yourself as someone else, real or fictional, or a message sent anonymously is prohibited.

Emails for the purposes that violate company status or regulations, or for an illegal or criminal purpose may not be sent or forwarded through a company's network.

Management has the right to access all e-mail files created, received, or stored on company systems and such files can be accessed without prior notification.

Email attachments can bring viruses, you should scan for virus after and before downloading the attachments with standard virus prevention software.

Do not open any e-mail attachments if you do not recognize the sender.

Forwarding of company confidential messages to external locations is strongly prohibited.

Introducing any form of computer virus or malicious software into the corporate network is strictly prohibited.

Policies for instant messengers and chat rooms

Chats, also known as Internet Relay Chat (IRC), as well as Instant Messaging (IM), are very popular modes of quickly communicating with others. In using these IRC and IM, staffs should agree the following policies. These policies provide staffs with effective and consistent instant messaging (IM) use and content standards.

Staffs are prohibited from downloading and using personal instant messenger software such as MSN or Yahoo to transmit messages via the public internet.

All IM communications and information transmitted, received, or archived in the company’s IM system belong to the company.

The instant messaging and chatting system is intended for business use only. Staffs are prohibited from wasting computer resources, colleague’s time, or their own time by sending personal instant messages or engaging in unnecessary chat related to business.

Treat messages as business records that may be retained and used as evidence in litigation, audits, and investigations.

Always use professional and appropriate language in all instant messages. Staffs are prohibited from sending abusive, harassing, threatening, menacing, discriminatory, disrespectful, or otherwise offensive instant messages.

Staffs may not use instant messengers and chat rooms to transmit confidential, proprietary, personal, or potentially embarrassing information about the company, employees, clients, business associates, or other third parties.

Introducing any form of computer virus or malicious software into the corporate network is strictly prohibited.

Task 5

Prepare and deliver a short presentation to your tutor using a presentation package like Power Point which summarises the major points in your Security Report and your proposed Acceptable Usage policies. (10 Marks)

I prepare and deliver a short presentation to the tutor using a Power Point presentation which summarises the major points in my Security Report and my proposed Acceptable Usage policies.

Network computerised system can contain various potential threats. To minise that risks, network security is required.

In this presentation, I want to talk about five topics to configure network security

Access Control

User Authentication

Firewalls

Virus Protection

Accessing the Internet

Access control can control the user account and identify the user. It can verify user identity through an authentication process so users can be held responsible for their actions. Primary objective of access control is to preserve and protect the confidentiality, integrity, and availability of information, systems, and resources.

I use role-based access control and rule-based access control to identify the user. Role-based access control systems allow users to access systems and information based on their role within the organisation. Roles based access can be applied to groups of people or individuals. Rule-based access control systems allow users to access systems and information based on pre-determined and configured rules. Rules can be established that allow access to all end-users coming from a particular domain, host, network, or IP addresses.

User authentication can determine the identity of a network user. For network computer, harm can be caused by hacking, malicious messages, viruses, malwares, adwares, email attachments, downloading illegal materials and many other types of activity. User authentication can reduce this harm by limiting individual’s access to a few systems, rather than the whole internet. Network administrator can control user log on and specify user permission on the network.

So, I configure some options and policies for user authentication. I specify that the password is required for all users of the company, to use the company’s computer. The user password length must be typically a minimum of five to eight characters and user passwords must have three of these four characteristics: lowercase letters (such as abc), uppercase letters (such as ABC), numbers (such as 123), and special characters (such as !@#). And I specify the policy that can lock the user account to prevent from logging on, when a user enters an incorrect password five times. According to the user account and password, I control which user can access to the network and what he/she can do on the network.

Firewalls protect against outside attempts to access unauthorised resources, and they protect against malicious network packets intended to disable or cripple a corporate network and its resources. And also use to restrict corporate user access to inter resources. Firewalls can identify and block remote access Trojans (Trojan horse). Network administrator can configure the rules for what type of traffic is allowed to enter and exit the network. The firewall can examine all incoming packets and discard packets.

In internet-connected networks, virus attacks are a regular threat. Users download programs, bring disks from home, memory sticks, and open e-mail attachments are normal computing activities, but they can also bring viruses into the network. To protect the spread of viruses, one of the most effective ways is to buy virus-protection software from a reputable source. Antivirus software is program that can scan and remove known viruses which have contracted. Most antivirus software is also designed to detect and prevent worms and viruses. The software can also be set to automatically scan disks when inserted into the disk drive, scan files when downloaded from the Internet, or scan e-mail when received. But by running antivirus software can only protect against viruses that it knows about. Therefore, virus definition files (update files) for antivirus software are needed to download from the internet daily or weekly. To get the maximum protection against viruses on the computer, make sure to keep antivirus definition files current. Another way to protect the data from virus infection is “ backup the files” which helps to recover the data if the original files infected by the virus.

Accessing the internet is the essential thing to communicate between internal or external organisation. However the internet is useful for us, the internet attack can harm the business. The internet attacks are organised and designed to steal information and resources from the customers and the organisation. If all kinds user can get permission to access the network, the private information of the organisation can be stolen by the attacker using the internet. So that I control the user access to the network resources by using access control and identifying the user account to verify the network permission for the user.

To minimise any potential risks and associated security threats of the organisation's network, all the staff of the company should agree the policies for accessing the World Wide Web, email usage, instant messengers, and chat rooms. All the staff has responsibility to use the resources in an efficient, effective, ethical and lawful manner.

Reference

Web Reference

www. en. wikepedia. org

www. businesslink. gov. uk

www. 3w. net

www. answer. com

www. procompgroup. com

http://humanresources. about. com

http://netsecurity. about. com

http://answers. yahoo. com

www. zytrax. com

www. windowsnetworking. com

www. cryer. co. uk

Book Reference

Title: Guide to Networking Essentials (Fifth Edition)

Author Name: Greg Tomsho, Ed Tittel, David Johnson

Access date & time: 13 July 2009, 6: 30 pm

Title: Fundamentals of Hardware and Operating Systems (Operating System Technologies) A+ Fifth Edition

Author Name: Charles J. Brooks

Access date & time: 15 July 2009, 5: 00 pm

Title: Fundamentals of Hardware and Operating Systems (Software Service Technicians) A+ Fifth Edition

Author Name: Charles J. Brooks

Access date & time: 16 July 2009, 7: 00 pm