

Management Information Systems (MMBA 6110-SP)

Research Paper: Internet Security

Michael S. Pallos

April 3, 2002

Walden University
Dr. Pamela Luckett-Wilson

TABLE OF CONTENTS

Internet Security	1
Executive Summary	1
Introduction.....	2
Overview.....	2
Emerging Threats.....	3
Computer Crime.....	3
Viruses	5
Effective Solutions.....	9
Policies and Procedures	9
Firewalls.....	9
Anti-Virus	10
Summary	11

INTERNET SECURITY

Executive Summary

The Internet provides users and corporations with a powerful communication tool supporting collaboration, research and accelerated business processes. As the benefits of the Internet expand, so do the exposures and threats one may experience. Internet security requires corporations to ensure their information technology infrastructure, including applications and data, is protected from malicious attacks from internal and external sources. Enterprise systems, as well as the personal home user, may become vulnerable to computer crime, hackers, viruses, Trojan Horses, and worms (Symantec 2002).

Internet users, including corporations, now need strong policies, software and hardware to reduce the exposure to malicious Internet emerging threats. While protection must be incorporated, one must not sacrifice the essential gains realized by the Internet. An evaluation of Internet requirements and desired level of security must be ascertained (Microsoft 2002).

The computer industry offers many effective solutions that are best implemented in a multiple layered approach. Using a layered approach, an Internet strategy ensures an

attacker who penetrates one layer of defense will be halted at a subsequent layer. The layers included in a traditional network-computing model are; 1) system level security, 2) network level security, 3) application level security, and 4) transmission level security (IBM 2002).

An effective Internet security strategy also contains an audit component allowing for risks to be uncovered and mitigation practices to be incorporated. Internet tools are also available to identify potential areas of penetration.

The Internet offers advantages to businesses, consumers, and home-users. Emerging threats exist that attempt to wreak havoc on existing systems of the home-user and corporations. However, the information technology industry has responded with many effective solutions providing multiple layers of security allowing all Internet users to achieve strong Internet security while maintaining high levels of flexibility and productivity gains.

Introduction

Overview

As the Internet becomes a vital part of everyday life for many American corporations and people, the need for

Internet security becomes increasingly vital to safe operation of this new frontier. The World-Wide-Web enables global access to information regardless of location and time zone. This flexibility and access also provides malicious Internet user a unique opportunity to wreak havoc. This paper addresses Internet security threats and effective Internet security solutions for the end-user and corporations.

Emerging Threats

Computer Crime

Computer crime ranges in degree from non-intrusive to deadly, as in the murder of Amy Boyer in 1999 by a computer stalker (Haag pg 328). The most non-threatening attacks are known as passive attacks. During a passive attack, the computer hacker simply monitors traffic (IBM 2002). One tool available for passive network monitoring is a sniffer. A sniffer allows the network administrator to debug, optimize and work constructively with a network. However, a hacker may attach a sniffer to a network and watch traffic flow by, usually looking for user names and passwords.

Another type of attack is an active attack. Active attacks penetrate the security defenses and enter the networked environment. There are currently four types of

active attacks system access attempts. There are spoofing, denial of service attacks, and cryptographic attacks (IBM 2002).

In system access attacks, the hacker attempts to penetrate the infrastructure by looking for holes in the security. Once in the system, the hacker attempts to gain control over the system.

Another type of active attack is spoofing. Spoofing is the process of masquerading as someone else. This allows the hacker to penetrate systems poses as another, and receive an others information. A common type of spoofing is called IP (Internet Protocol) spoofing. This type uses the TCP/IP (Transmission Control Protocol) protocol, which is the one used by the Internet. All IP messages have the IP address for their origination point contained in their header. This allows the receiving process to confirm whom the message is from. A hacker who is spoofing will update the IP header with someone else's IP address. Thus posing as this person. Hackers are able to intercept the return IP message. The target system believes it is communicating with the owner of the IP address. However, actual communication is occurring with a hacker who is updating the IP header section of an TCP/IP message.

Denial of service attacks are when a hacker attempts to bring down a system by creating an overload of incoming requests. The most effective denial-of-service attacks include using many other computers in the attack. This is done by developing a virus that targets one system, such as Yahoo, then spreads the virus to many other computers used to implement the denial of service attack. The virus is then triggered. All involved computers will send as many requests to the targeted site at one time. Yahoo becomes overloaded and their system comes to a halt. February 9 2000 Yahoo's site was virtually inoperative for two hours from a denial-of-service attack (CNN.com 2002).

The last type of active attack is cryptographic where a hacker will attempt to guess the users password (IBM 2002). When organizations do not enforce password guidelines, users will use a simple word for their password. Some of the most common passwords are names, dates, and the user's name itself. Hacker programs are available that will continue trying to login a user using different common names including pet names.

Viruses

A computer virus is a small program developed to infect, spread and often cause damage to a person's

computer without their knowledge. The damage caused by viruses has been categorized into two groups; benign and malignant (Haag pg 328). A benign virus may display a message, but will not damage the computer. For example, the cookie virus in Unix would periodically display a message on the screen, "I want a cookie." To remove the virus, one simply had to type "cookie" at the virus' request. If one failed to, the virus would, at some random time in the future, ask for another cookie.

A malignant virus damages the software and/or data on one's computer. Currently no viruses exist that can damage a computer's hardware. The damage a virus inflicts in on software and data. For example, the "I LOVE YOU" virus would delete files on the hard drive when executed.

There are currently two primary vectors for virus infection the Internet and email (Symantec 2002). According to the Computer Security Institute, 59 percent of all attacks on corporations came from the Internet (CSI 2000). While just one email virus, the "I LOVE YOU" virus and its copycat strains infected an estimated 300,000 computers (Meserve 2000).

Computer viruses have evolved over the past twenty years from the early viruses to the hybrid viruses of today, including worms and Trojan Horses.

The early computer viruses were a small independent program written with a uniquely identifiable strand of code. These strands of code were known as virus signatures. Antivirus software would simply search the hard drive and the boot sector of a system, looking for virus signatures. This allowed for easy virus detection and removal.

Virus developers then began encrypting viruses. Encryption is the process of mangling the program into indecipherable code, hiding the virus signature. Therefore, the virus would have to first de-encrypt itself prior to execution or replication. In response, antivirus software incorporated de-encryption routines into their logic allowing them to identify virus signatures.

The next evolution of virus software was the polymorphic virus. Polymorphic means the ability to change or alter one's state. The virus includes a random number generator that is used as the encryption seed. This number is used as the key allowing for decryption. The process of guessing the seed variable used for encryption is complex. Therefore antivirus software users created a scheme that signaled polymorphic viruses to decrypt themselves (Symantec 2002). Once decrypted, antivirus software eliminates the virus prior to the virus spreading.

A Trojan Horse virus typically masquerades itself as a legitimate program. Trojan Horses do not usually replicate, but instead wait for a signal or trigger to execute. An example of a Trojan Horse trigger is the computer date, such as Valentines Day. The Trojan Horse sits dormant until the computer date reads February 14. At that time the Trojan Horse virus logic is executed.

Another virus categorization is known as a *worm*. A *computer worm* is a program designed to replicate itself to other computers without requiring human intervention. "Worms are insidious because they rely less (or not at all) upon human behavior in order to spread themselves from one computer to another" (SARC 2000). There are worm viruses, which enter a computer and systematically start sending itself to everyone in the Outlook address book.

The final type of viruses is known as *hybrids*. Hybrids combine technologies from the different existing types of viruses, creating malicious code that is exponentially more lethal (Symantec 2002). One of the greatest concerns of hybrid viruses is the speed at which they can spread through an organization. According to Symantec, an infected networked computer can spread a virus to another computer in about 15 minutes.

Effective Solutions

Policies and Procedures

A security policy identifies what is to be protected, and what is expected from the system users. There is always a trade off with security implementation. The more security implemented, the slower the system processes. Therefore, organizations must decide on the level of security required. Microsoft recommends that organizations identify a Corporate Security Office (CSO) responsible for ownership of the security policies and procedures (Microsoft 2002). An example of security policies is password structure. Many organizations require a users password to be a mixture of alphanumeric characters, such as "Mike123".

Firewalls

One of the most common Internet security polices is a known as a demilitarized zone or DMZ. A DMZ is a computer network that is not attached to the Internet. Organizations are ensured of Internet security since they are not connected.

A looser definition of a DMZ allows the internal network to be connected to the Internet only through a firewall. A firewall is a device that inspects the content of each message attempting to enter the organization.

Firewalls only allow known addresses to pass through. Most organizations incorporate a hardware firewall. Firewalls are also available in a pure software form. This is useful for mobile end-users or smaller organizations. For example, Black Ice is a software firewall that identifies unauthorized intrusion (Network Ice 2002).

Anti-Virus

Antivirus software offers exceptional defense against Internet and email viruses. Antivirus software is a computer program that is always running on a system evaluating each message entering and leaving the system including network traffic, CDs, and floppy disks. The two market leaders are Symantec's Norton AntiVirus and McAfee. Antivirus software is only as good as it's virus definition files. Virus definitions are the antiviruses' local library of all virus strands. They provide the software with the ability to detect viruses. Since new viruses are created daily, the antivirus software must be updated often, weekly at a minimum. Antivirus software firms, such as Norton, include one-year virus definition subscription updates free. Subsequent years may be purchased at a fee of 9.95 dollars per single user (Norton 2002).

Since antivirus software inspects each Internet message, floppy disk, CD, and email, one's processing speed is reduced. This is one of the trade-off that a user and organization must decide when implementing a security procedure.

Summary

The Internet brings many advantages to corporations and users. As reliance on the Internet increases, so does one's vulnerability. Computer crimes and viruses are a real threat to the Internet community. Fortunately technology continues to advance offering effective solutions countering computer crimes and viruses. Some of the most effective solutions are the use of firewalls and antivirus software. Organizations and users should implement an Internet security policy while incorporating emerging technologies to reduce threats and vulnerabilities.

References:

CERT Coordination Center, *CERT/CC Statistics 1988-2000*, Retrieved March 12, 2002 from <http://www.cert.org/stats/>

CNN.com, *Cyber-attacks batter Web heavyweights*, Retrieved March 27, 2002 from <http://www.cnn.com/2000/TECH/computing/02/09/cyber.attacks.01/index.html>

Computer Security Institute, Federal Bureau of Investigation, *CSI/FBI 2000 Computer Crime and Security Survey*, Retrieved March 27, 2002 from <http://www.pbs.org/wgbh/pages/frontline/shows/hackers/risks/csi-fbi2000.pdf>

Dekker, M., CERT Coordination Center, *Security of the Internet*, Retrieved March 12, 2002 from http://www.cert.org/encyc_article/tocencyc.html

IBM, *The Layered Defense Approach to Security*, Retrieved March 12, 2002 from <http://as400bks.rochester.ibm.com/pubs/html/as400/v5r1/ic2924/index.htm?info/rzaj4/rzaj4rzaj45zssecurityplanning.htm>

Meserve, J., *People Around the World Bitten by Love Bug*, Retrieved March 27, 2002 from http://www.nwfusion.com/archive/2000/95707_05-08-2000.html

Microsoft, *Security Considerations for the End User*, Retrieved March 12, 2002 from <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/sconsid.asp>

Network Ice, *Black Ice 2002*, Retrieved March 27, 2002 from <http://www.networkice.com/>

Symantec, *Internet Security for the Web*, Retrieved March 12, 2002 from <http://securityresponse.symantec.com/avcenter/reference/security.for.web.pdf>

Symantec, *Norton Anti-Virus*, Retrieved March 12, 2002 from <http://www.symantec.com>