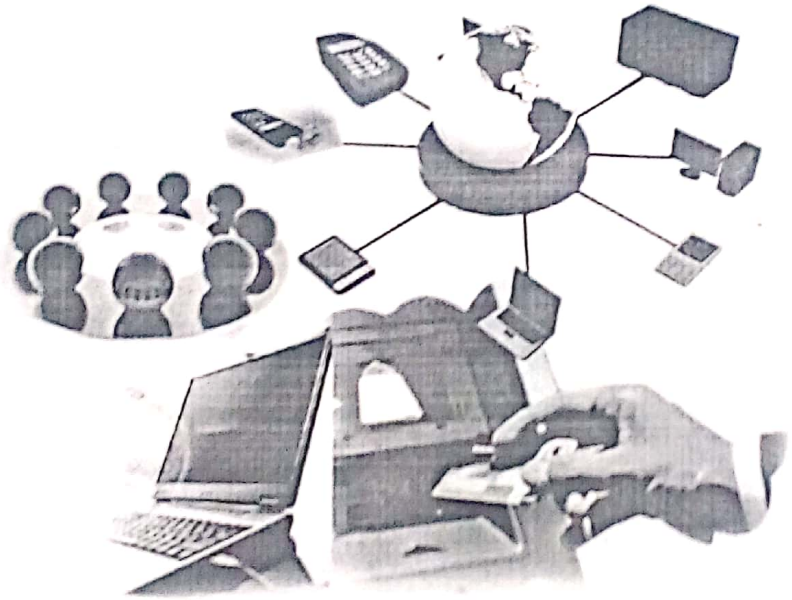
National Conference-2012

PROCEEDINGS

Perspectives of IT Development in Banking Industry



Dr. Makarand Wazal

Dr. Mrs. Vijaya S. Nawale

Prof. Pramod Bora

Sinhgad Technical Education Society's

SINHGAD COLLEGE OF COMMERCE

Kondhwa (Bk.), Pune (M. S.), India

(Accredited by NAAC)

14

Ways for Improving Information Security Using Easy Methods

Vrunda Deshmukh , Tushar Deshmukh

Abstract

Today's Digital Age is famous for the ability of individuals to transfer information freely, and to have instant access to information. Most of this information is collected, processed and stored on computers and transmitted across networks to other computers. Business firms, financial institutes, corporations, governments, military and many more build up with confidential information about their employees, customers, products, research, and financial status. If confidential information about a business fall into the hands of a competitor then such a break of security could lead to negative consequences. Protecting confidential information is an essential requirement of every business and in many cases it's a legal and ethical requirement.

***Information security** means protecting information and computers from unauthorized access or use or modification or destruction. Information security deals with the confidentiality, integrity and availability of data. It focuses on protection of information.*

Due to the rapid growth and widespread use of electronic data processing and electronic business conducted through the Internet, it is necessary to improve better methods of protecting the computers and the information they store, process and transmit. The paper focuses on some simple methods for improving information security. Three basic security concepts are important for information security is confidentiality, integrity, and availability. There are five simple measures to take the edge off information security risks. Two of these measures are non-technical and three are Technical. The non-technical measures to improve information security include the successful implementation of a sound information security policy and an effective employee education and training program. Technical measures to improve information security include an anomaly-based intrusion prevention system, the use of thin clients, and a properly configured application-layer firewall. This paper is based on those guidelines.

Key words: Security risks, confidentiality, integrity, availability, technical and non-technical measures of information security.

Introduction

1.1 Background:

In the early days of writing era, heads of state and military commanders understood that it is necessary to provide some mechanism to protect the confidentiality of written communication and to have some means of detecting unauthorized access. The end of the 20th century and early years of the 21st century saw rapid advancements in telecommunications, computing hardware and software, and data encryption. The availability of smaller, more powerful and less expensive computing equipment made electronic data processing within the reach of small business and the home user. These computers quickly became interconnected through the Internet. The rapid growth and use of electronic data processing and electronic business through the Internet, the need for better methods of protecting the

computers and the information they store, process and transmit become necessity. Now we are living in a society dominated by information technology and in an era of information where huge amount of Information can be speedily processed and saved on easily accessible media. For example, information that before was saved on a large amount of paper and physically difficult to steal can today be saved on a disk that can easily remove. Information security deals with several different trust aspects of information. It applies to all aspects of safeguarding or protecting information or data, in whatever form. Information security chain is needed when information is threatened, lost or misused.

The three basic security concepts are important for information on the internet are confidentiality, integrity, and availability. When any information is read or copied by someone not authorized to do so, it is known as loss of confidentiality. For some types of information, confidentiality is a very important. For example: research data, medical and insurance records, new product specifications, and corporate investment strategies. In some locations, there may be a legal obligation to protect the privacy of individuals. This is particularly true for banks and loan companies; businesses that extend credit to their customers or issue credit cards; hospitals, doctors' offices, and medical testing laboratories; individuals or agencies that offer services such as psychological counseling or drug treatment; and agencies that collect taxes.

When information is modified in unexpected ways, the result is known as loss of integrity. This means that unauthorized changes are made to information, whether by human error or intentional tampering. Integrity is particularly important for critical safety and financial data used for activities such as electronic funds transfers, air traffic control, and financial accounting.

Information can be erased or become inaccessible, is called loss of availability. This means that people who are authorized to get information cannot get what they need. Availability is the most important attribute in service-oriented businesses that depend on information for example, airline schedules and online inventory systems.

Concepts relating to the people who use that information are authentication, authorization, and nonrepudiation. To make information available to those who need it and who can be trusted with it, organizations use authentication and authorization. Authentication is proving that a user is the person he or she claims to be. That proof may involve something the user knows such as a password or something the user has such as a smartcard, or something about the user that proves the person's identity such as a fingerprint. Authorization is the act of determining whether a particular user has the right to carry out a certain activity, such as reading a file or running a program. Security is strong when the means of authentication cannot later be refuted means the user cannot later deny that he or she performed the activity. This is known as nonrepudiation.

1.2 Methods

There are five easy measures to help information security risks. Two of these measures are non-technical and three are Technical. If an attacker makes it through one layer of defense, another layer will stop the attack.

1.2.1 Technical Measures:

The technical measures include an anomaly-based intrusion prevention system, the use of thin clients, and a properly configured application-layer firewall.

Intrusion Prevention System (IPS):

An anomaly-based Intrusion Prevention System (IPS) is one of the most effective technologies for information security. An IPS that is anomaly-based is utilized to block network traffic based on its level of irregularity. These IPS devices are typically implemented at the organization's network boundary between the organization's network and the Internet provider service delivery point. Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to block intrusions that are detected. IPS can take actions as sending an alarm, dropping the malicious packets, resetting the connection or blocking the traffic from the offending IP address. An IPS can also correct Cyclic Redundancy Check (CRC) errors, unfragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options

Anomaly-based IPS devices are difficult to initially configure because they require lawful network traffic for an organization to be defined. Defining lawful network traffic is often a critical task because of poor network documentation. Once the lawful traffic for an organization is defined, the IPS can be configured to block traffic that does not fall within the lawfully defined traffic. For example, suppose an organization only has one email server that communicates with the internet on TCP Port 25 then the SMTP (Simple Mail Transfer Protocol) traffic only from the email server to the Internet is a lawful traffic. If an attacker compromises the company DNS server and attempts to use it as a SPAM relay, the IPS would block this traffic. A SPAM relay communicates with SMTP. The IPS blocks the traffic because the only authorized device can communicate this Port.

An anomaly-based IPS forces an organization to define legitimate traffic and develop a greater understanding of their network. This increased network traffic insight combined with the active blocking and alerting functions of the IPS, greatly increase information security.

Thin Clients

Thin client is a computer or a computer program which depends on some other computer (its server) to fulfill its traditional computational roles. Many information security machines are caused by infected client machines. Client computers are typically compromised when a user installs unauthorized software either from downloading it from the Internet or bringing it from home. A thin client does not contain a hard drive and has no storage capacity. It is a diskless computer with a network interface card, memory, a keyboard, mouse, and monitor. The thin client is used to run a session from a server. These sessions emulate a standard desktop computer environment for the user.

Thin clients can be configured without floppy drives or even USB drives. This removes the opportunity for a user to bring unauthorized software or data into an organization. Thin clients also provide more extensive logging capability since all the session data is stored on a central server. Another benefit of a thin client is portability. With thin clients a user can use any client available and have the same desktop and tools available from any client.

Thin clients provide the capability to easily standardize the user environment and centrally manage every user session, plus floppy drives and USB drives can be eliminated. These capabilities make thin clients a smart choice for improving information security.

Thin-client computing is also a way of easily maintaining computational services at a reduced total cost of ownership.

Application-layer Firewall

An application firewall controls input, output, and access from, to, or by an application or service. It operates by monitoring and blocking the input, output, or system service calls. The application firewall is typically built to control all network traffic on any OSI layer up to the application layer. It is able to control applications or services. Application-layer firewalls enhance information security by providing intelligent monitoring and filtering of traffic in and out of an organization. Application-layer firewalls are intelligent enough to understand applications, such as HTTP, SMTP, and DNS. This intelligence allows application-layer firewalls to inspect packets entering and leaving an organization for content as well as header information.

Many attackers today use tunnels to extract information or to communicate with remotely controlled bots. Application-layer firewalls stop attackers from using tunnels and can prevent users from accessing malicious websites. Application-layer firewalls are an effective component to a defense-in-depth strategy for obtaining a secure information environment.

1.2.2 Non - Technical Measures:

The non-technical measures to improve information security include the successful implementation of a sound information security policy and an effective employee education and training program.

Information Security Policy (ISP):

An information security policy (ISP) lays the foundation for an organization's stance on information security. The ISP is designed to formally document an organization's information processing roles, responsibilities, and procedures. The ISP must have top-level management support and must be articulated to all employees.

Some of the main items an ISP should include are procedures to add users to the network, procedures to handle compromised computers, procedures for backing up data, procedures for employee termination, and computer use and abuse policies. The procedures to add users to the network include items such as validation of user employment, determining which data the user needs access to and what type of access the user needs, initial user training, and user remote access requirements. Procedures to handle compromised computers include a delineation of who is responsible for various steps in the process, what steps to take with the compromised computer, and how forensics should be performed. Data backup procedures should be outlined in an ISP to include how often the data is backed up, where the backed up data is stored, how the data is stored and transported off-site, and how often recovery procedures should be practiced. The ISP must include procedures for employee termination, such as access removal, identification card turn-in, notification of termination, procedures for employee escort off corporate facilities, and employee record updates.

A properly written and implemented ISP greatly increases information security for an organization.

Employee Education and Training

Employee education and training are vital for information security. Many computer outages and compromises are caused unintentionally by employees. Educated employees on information

security issues are less likely to fall for social engineering ploys, phishing scams, or violate security policies. Social engineering is simply the user of non-technical means to gain authorized access for example, making phone calls or walking into a facility and pretending to be an employee.

Employee education helps mitigate information security threats such as social engineering and phishing scams by educating employees on these types of commonly used tactics. Social engineering scams can be as simple as an attacker posing as a helpdesk administrator and calling an employee asking for the employee's password. Employee awareness as a result of adequate training teaches the employee standard organizational procedures, such as there is no circumstance when the helpdesk would call and ask for a password. Phishing emails are commonly used by attackers to gain access to a system:

The tone and content of phishing emails are always the same. First, they warn that users must update their account by typing in some valuable information, often a credit card number. Finally, the email provides a convenient link that leads to a seemingly legitimate web page where the victim can type his credit card number. Victims enter their credit card numbers and unknowingly give that information to a con artist.

Employee education should teach employees not to open emails from persons they do not know and to ask the helpdesk about any emails that seem suspicious. Employee training not only educates employees on information security benefits, but the training also helps improve employee efficiency. Employee efficiency is improved due to the employee's better understanding of the computer network and processes. Educated and trained employees are one of the best lines of defense against information security threats.

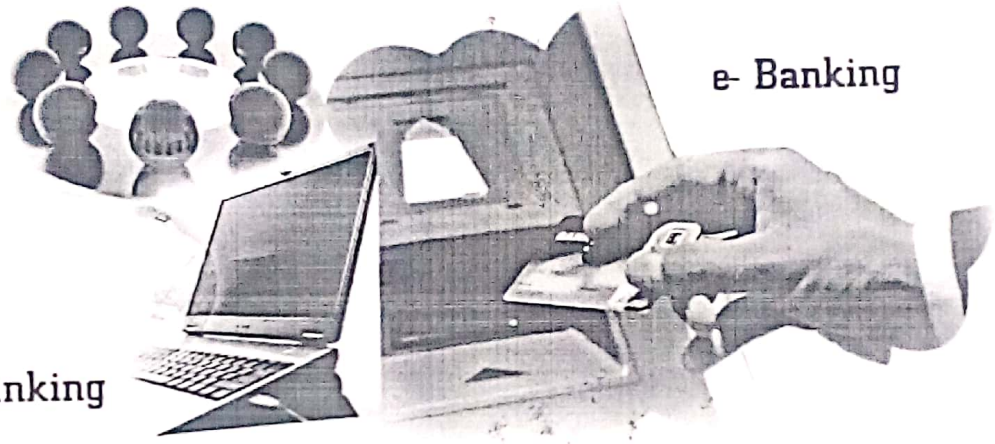
Conclusion

These methods definitely help for improving information security. A well-developed and implemented information security policy lays the foundation for a secure network. Employee education and training on the information security policy, computer and internet use, and information security procedures adds another line of defense in information security protection. An anomaly-based intrusion protection not only stops attacks but improves network documentation, knowledge, and understanding. Thin clients facilitate network administration, provide centralized management, and improve overall information security. Application-layer firewalls provide content level inspection and can prevent unauthorized traffic from entering or leaving an organization's security perimeter. Successful implementation of these five security measures will definitely search network intruders.

References

1. Computer Security Basics By Deborah Russell & G.T. Gangemi, Sr.
2. www.technoparkcorp.com
3. www.securityresponse.symantec.com
4. Information Security Management: NHS Code of Practice
5. Integrating IT Security and Control Process by Joan Hash.

IT & Core Banking



e- Banking

CRM in Banking

Financial Inclusion & Green Banking

ISBN: 978-81-923324-0-6

Sinhgad Technical Education Society's

SINHGAD COLLEGE OF COMMERCE

S. No. 40/4A+4B/1, Near PMC Octroi Post,
Kondhwa - Saswad Road, Kondhwa (Bk.), Pune - 411 048 (M.S.), India

http://www.sinhgad.edu