"SECURITY" @ Information Technology

Garima Ojha (Assistant Professor JECRC UDML, Jaipur)

Punit Arora

Abstract

My aim of this research is to present a better security system in information technology. This seemingly simple task has become a very complex process with systems that need to be continually updated and processes that need to constantly be reviewed. There are three main objectives for information technology securities according to research are:

Confidentiality,

Integrity,

Availability of data.

Within large organization information technology generally refers to computers, servers, routers, and switches that form a computer network, although information technology also includes fax machines and voice mail systems, cellular phones, and other electronic systems. Unauthorized access to paper documents or phone conversations is still an information security concern, but the real challenge has become protecting the security of computer networks, especially when they are connected to the Internet. Most large organizations have their own local computer network, or intranet, that links their computers together to share resources and support the communications of employees.

1. Introduction

Security Resources:

- **Security Overview**
- **Firewalls**
- **Intrusion Detection**
- **Security Policies**
- **Vulnerability Assessments**
- **Cryptography**
- **Portal Review**
- **About Security**

Security Overview:

Security is a basic human concept that has become more difficult to define and enforce in the Information Age. In primitive societies, security was limited to ensuring the safety of the group's members and protecting physical resources, like food and water. As society has grown more complex, the significance of sharing and securing the important resource of information has increased. Before the proliferation of modern communications, information security was limited to controlling physical access to oral or written communications. The importance of information security led societies to develop innovative ways of protecting their information. For example, the Roman Empire's military wrote sensitive messages on parchments that could be dissolved in water after they had been read. Military history provides another more recent example of the importance of information security. Recent innovations in information technology, like the Internet, have made it possible to send vast quantities of data across the globe with ease. However, the challenge of controlling and protecting that information has grown exponentially now that data can be easily transmitted, stored, copied, manipulated, and destroyed.

Within large organization information technology generally refers to laptop and desktop computers, servers, routers, and switches that form a computer network, although information technology also includes fax machines, phone and voice mail systems, cellular phones, and other electronic systems. A growing reliance on computers to work and communicate has made the control of computer networks an important part of information security. Unauthorized access to paper documents or phone conversations is still an information security concern, but the real challenge has become protecting the security of computer networks, especially when they are connected to the Internet. Most large organizations have their own local computer network, or intranet, that links their computers together to share resources and support the communications of employees and others with a legitimate need for access. Almost all of these networks are connected to the Internet and allow employees to go "online."

Information technology security is controlling access to sensitive electronic information so only those with a legitimate need to access it are allowed to do so. This seemingly simple task has become a very complex process with systems that need to be continually updated and processes that need to constantly be reviewed. There are three main objectives for information technology security: confidentiality, integrity, and availability of data. Confidentiality is protecting access to sensitive data from those who don't have a legitimate need to use it. Integrity is ensuring that information is accurate and reliable and cannot be modified in unexpected ways. The availability of data ensures that is readily available to those who need to use it.

Information technology security is often the challenge of balancing the demands of users versus the need for data confidentiality and integrity. For example, allowing employees to access a network from a remote location, like their home or a project site, can increase the value of the network and efficiency of the employee. Unfortunately, remote access to a network also opens a number of vulnerabilities and creates difficult security challenges for a network administrator.

Firewalls:

- **Organizational Guidelines**
- **Functionality Guideline**
- **Other Sources**

Introduction

Institutions and businesses need to protect themselves from threats created by the use of new technologies. Firewall technology is useful in offering this protection. Firewalls control all inbound and outbound traffic. The most common types of technology used in firewalls are packet filtering, application level firewalls, and stateful inspection firewalls. Packet filtering software works at the network layer where all packets are inspected as they pass through a router. Packets that match access control rules are allowed through, while those that do not match are dropped. Application-level firewalls work at the application layer. Most use proxy servers that act as an interface between internal users and the Internet. The proxy checks for permissions and enforces access control rules. Services that do not comply with these rules are blocked. Stateful inspection works at the network layer. IP header information is reviewed to determine which services to allow through and which to block. Adaptive proxy, a new firewall technology, combines packet filtering with secure proxy technology. Firewall appliances, as opposed to software applications, are becoming more popular. These devices stand-alone and typically combine hardware and software set into an operating system.

Organizational

- Establish application/business needs: Internet, intranet, extranet.
- Assess security risks: high, medium, or low**.**
- Establish security requirements.
- Establish operational capabilities.
- Check security budget allocation

  Establishing business requirements includes asking questions about:

  - What type of access to the Internet is required and by whom (internal employees, remote access, access from outside to company Web
  - Does the company intranet need a firewall to protect from internal attacks?
  - Does the enterprise want to conduct business with other business partners and suppliers via an extranet?

  Assessing the type of firewall to install requires an organization to review its network design and business objectives. By conducting a risk analysis, exposures and levels of risk may be determined. Then, based on the results of the risk analysis, an organization has the starting blocks from which its requirements will arise

  - A sampling of what may be uncovered during the risk analysis includes these:
- The threats, impact, and vulnerabilities of connecting to the Internet.
- Consider what Internet or external services are required, what features are required, and what level of assurance is required.

- This will help towards specifying a firewall according to the user's needs as opposed to selecting a firewall based on the number of features it comes with.
- The firewall must reflect the company’s existing security policy, not impose a new one. In the absence of a security policy, or where a security policy exists but does not

cover the Internet, an acceptable use agreement should be implemented.

- Operational capabilities should be established, i.e., what processes are involved in the day-to-day running of the system, check logistics, IT responsibilities, etc. Another important factor to bear in mind is to check where the security spending will come from: Does the enterprise have a dedicated security department with a dedicated security budget, or will budget have to be requested from the corporate IT director.

Functionality

Questions to ask include these:

- What authentication techniques does the firewall support?
- Can it filter java/ActiveX applets?
- Are there logging facilities for inbound/outbound traffic?
- Are there auditing and reporting tools?
- Does it carry out intrusion detection?
- Does it have alerting facilities?
- Is there a standby device in case of failure?
- Does the firewall support VPN?
- What types of encryption settings does it have?
- Can it centrally manage multiple firewalls?
- Does it offer secure remote management?
- Does it have ITSEC or ICSA certification?
- Does it have load balancing/traffic prioritization/bandwidth management?
- Does it support LDAP?
- Performance?
- Does it offer PKI support?

Intrusion Detection

Introduction to Network-Based Intrusion Detection Systems (NIDS)

"An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system."

Platform

Some IDSs function from a dedicated (black box) appliance, meaning that there is no need for the customer to load the operating system, install the application software, and harden the operating system separately. Others are software based and have to be installed on top of a supported platform and operating system.

Components

IDSs generally can be broken into two components: the sensor and the console. The sensor sits upon the network and acts as a sniffer, listening to network traffic in promiscuous mode. The console is the point of central management for an IDS system. By using the console, an administrator may take notice of any current attack alerts. In many cases, the console may be used to customize certain preferences for the IDS.

Security Policies:

- Introduction
- Overview
- Physical and Security Access
- Network Security and Configuration
- Authentication and Encryption Infrastructure
- Incident response & disaster contingency
- Acceptable Use of the Network
- Acceptable use of Software/Hardware
- Compliance
- Security Awareness
- Evaluation and Revision

Introduction

Need of the organization, especially as security and vulnerability assessments reveal weaknesses that need to be corrected. To be effective, a policy must be communicated an effective network security policy is the foundation of an adequate information security environment. A network security policy is the basic document that defines the expectations for network security and guides administrators and network users. A good network security policy should support the organization's overall goals and mission, set standards for acceptable behaviour on the network, identify assets that need to be protected, and hopefully reduce the number of security incidents. Security Polices can be written a high-level to allow for broad interpretation or at a low-level to provide specific guidance. A good security policy has a mixture of both, allowing for innovation in appropriate areas and providing numerous details in critical areas. A network security policy should be easy for all users to understand and adaptable to the to all network users, consistently enforced, and strongly supported by the organization's leadership. Although every organization's security needs are unique, these 10 elements should be evaluated when creating or revising a network security policy.

Physical Security and Access:

Unauthorized physical access to hardware and facilities can easily undermine more advanced technical defences. The policy should be clear on who has physical access to sensitive areas that contains servers and other network equipment. There must also be clear procedures in place to ensure network users only have access to systems the need to use to complete their work. Internal attacks and human errors often present a serious risk to many organizations and controlling user access helps maintain the reliability and confidentiality of information. The Physical security of organizational assets, like laptop computer, should also be covered in this section.

Network Security and Configuration:

This section should give system administrators and the leaders of the organization a clear picture of how different security tools (like Virus Detection Programs, Firewalls, Network Scanners, Intrusion Detection Devices) and strategies (like data sandboxing, demilitarized zones, and pluralism) will be used to protect the network. This section should define the individual responsibility of users to protect the network and prohibit unauthorized tampering with the network. It should spell out user responsibilities for remote access and other network features.

Authentication and Encryption Infrastructure:

Authentication is how users identify themselves to the network. This section will detail the authentication and verification tools the organization uses and the user's responsibilities for them. It should provide guidance on the need to change passwords, protect encryption keys, when to use digital signatures and certificates, or biometric devices. This section of the policy is critical to ensuring the confidentiality of data.

Incident Response & Disaster Contingency Plan:

An organization's ability to recover from a disaster or respond to a security incident is extremely important. The section requires should provide clear roles and responsibilities that include the reporting of security incidents and recovery procedures. Responsibilities for updates to anti-virus software and code patches should also be covered in this section. How well an organization functions when faced with a security incident or a disaster can have a significant effect on the confidence of network users. This section should include security measures for backing up servers and data and contain contact information for members of an emergency or incident response team.

Acceptable Use of the Network:

This section should cover the rights and wrongs of using the network. It should provide detailed guidance on how to use e-mail, the Internet, and the organizational intranet. This section might also address the use of computer games and whether or not an individual can use e-mail and Internet access for personal use and what type of material is allowed. This is often a sensitive area for employees and the rules in this area will be more accepted if the organization provides justification for it decisions. This is a good place to cover what expectation of privacy network users can expect.

Acceptable use of Software/Hardware:

This section will detail what changes to software and hardware are allowed and who can add or delete software. It should set acceptable behaviour for the personal use of company software and hardware.

Compliance

This section should also explain the penalties or actions that could be taken in the event of noncompliance. It might also state the methods that will be used to investigate breaches of the policy. Mandatory penalties, either minimums or maximum for violations policies are not recommended because they may tie the hands of the organization's leadership.

Security Awareness

Employees must manage passwords properly and be aware of "social engineering" attacks. To be effective, a network security policy needs to be communicated to everyone who uses the systems, whether they are internal or external users, administrators, and contractors. Users should receive awareness training and should acknowledge the security policy before given access to the network.

The security policy should also be clearly posted, preferably on the organization's home page for both the Internet and the Intranet

Evaluation and Revision The policy should provide for periodic reviews of the network's security and for revisions of the policy itself. Internal security assessments should be done frequently, but outside assessments by a trusted third party are also recommended. The policy should be revised frequently because new threats and vulnerabilities constantly emerge in this dynamic field, especially as the functionality of the network evolves and new service.

Vulnerability Assessment:

Introduction to Vulnerability Assessment

A vulnerability assessment on an enterprise network can be a major undertaking, but it's an important part of securing a network. Vulnerability assessment can be done by inside professionals (i.e. network administrators), but is usually outsourced to Managed Security Service Providers (MSSP). Each MSSP provides different solutions, has a different background, and different areas of expertise. It's crucial to select an MSSP that offers exactly what is needed. A couple of factors that determine what may be needed. First, how much of the network to assess and which parts? Second, what constitutes vulnerability? Determining what needs to be left vulnerable is as important as what needs to be locked-down.

Cryptography:

"Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world."

Private Key Cryptography

Before the concept of public key cryptography took root, private key cryptography was the main conduit through which encrypted conversations could take place. Both sender and receiver share the same key which must be kept private. The difficulty lies in the fact that if communication is to occur.

Public Key Cryptography

The premise of their collaborative effort, "Multi-User Cryptographic Techniques" was that it should be possible to create a multi-user cryptography system in which a message could be encrypted with one key and decrypted with another.

Portal:

ESecurityOnline.com also offers online courses in Web Development, Business, Certification, Desktop (design, graphics, Internet/Intranet) and Database development, Network Administration and Programming

About Security:

The term 'network security' is likely to call to mind the image of an innocent network needing protection from malicious attack. The term 'information security' suggests that there are people from whom information must be protected -- in other words, that some have a right or a privilege to certain information, while others don't.

- Introduction
- Ethical Hackers and Networks
- Ethical Hackers and Information
- Ethical Hackers and Politics
- Conclusion
- Sources
- Further Reading

References:

[1] http://world.std.com/~cme/html/timeline.htm

[2] www.wikipedia.com

[3] The Fundamentals of John E. Canavan.