Basics of Internet Security

Premraj Jeyaprakash

About Technowave, Inc.

Technowave is a strategic and technical consulting group focused on bringing processes and technology into line with organizational goals. Technowave provides best of breed solutions to real world problems for the Small to Medium Business (SMB) market. In addition to strategic consulting, Technowave provides system architecture, project management, development and implementation services. Technowave also provides technical and knowledgeable professional with Innovative Technologies to organizations on a flexible, contract and permanent basis focusing according to the client's dynamic needs.

For additional copies of this whitepaper, or to explore partnership opportunities with Technowave, please contact us as follows.

Technowave Inc.
900 Pump Road, Suite 69
Richmond , VA 23238
Tel: (804) 740-0957
Fax: (804) 740-0958

Businesses rely heavily on the integrity of an ever-increasing supply of data and information, as well as the associated processing and storage systems used to manage It. The complexity of access administration and security has increased significantly as we move from centralized to distributed computing environments. Especially increased Internet use in businesses has particularly high impact on security measures deployed at a company. This section of the paper discusses some of the major threats to Internet security, and explains how these threats must be addressed in enterprise-wide networking.

In every business, e-commerce and e-business initiatives are intended to bring together employees, customers, partners, suppliers, and distributors to exchange and access information through the Internet. However, these business environments create vulnerabilities that allow both internal and external users to damage the information systems through malicious acts of fraud and vandalism. Therefore, businesses should examine their vulnerabilities before developing any security solutions. The major network infrastructure elements that can be accessed and vandalized through the Internet will now be discussed.

Firewalls

A firewall is a device that is placed at the point where the Internet enters your facility, controlling network traffic for security purposes. Firewalls are specialized systems that are placed between external networks and companies internal networks to control access to systems connected to those internal networks. Firewalls work in conjunction with the routers to process all packets from or to remote network entities, and to allow only pre-approved traffic to or from pre-approved hosts. The following security measures should be employed to protect the firewalls:

- The firewalls should hide the identity of internal hosts by connecting remote entities to the firewall instead of to the actual server by establishing a separate connection to the real service provider.
- Configure to accept root login only from the connected console device.
- Configure to discard source-routed IP packets.
- Configure to detect and discard IP packets carrying tunneled network packets.
- Configure with appropriate proxy agents for applications such as ftp, telnet and smtp.
- Configure to reject telnet or ftp sessions originating from external hosts or received upon the external network interface connection.
- Capture and log the access violations.
- Check and apply security patches frequently.

Routers

A router is a device that determines the next network point to which a packet of information should be forwarded. Using the routing protocols and network layer of the OSI model, a router connects two or more networks. Based on the Vertical Market Security Report 2003, the financial sector is having the worst record for router security compared to other sectors, with 94 % of financial organizations tested showing basic flaws that could cause major disruption to online banking services. Therefore, routers are highly vulnerable to attacks, including gaining routing information, spoofing, and denial of service attacks. Routers can be protected from attacks by employing the following security measures:

- Use strong encryption algorithm for routers' password.
- Restrict any telnet access to a router.
- Display details of civil and/or criminal penalties during unauthorized access of the system.

- Use Simple Network Management Protocol (SNMP) Version 3 instead of Version 1 to access a router.
- Control access to a router through the use of the Terminal Access Controller Access Control System Plus (TACACS+).
- Capture and log the access violations.
- Authenticate and secure IP routing.
- Check and apply security patches frequently.

Hosts

A host is a server that provides the application services to other hosts that request them. These hosts can be utilized as web servers, operating systems, application servers, or data base servers. In addition, a host can use different hardware and software components from different vendors. Since the host is the point of communication for both internal and external users, it is extremely visible within the network. Therefore, hosts are highly vulnerable to virus attacks and unauthorized access to protected data. Hosts can be protected from attacks by employing the following security measures:

- Create user accounts only for those whose jobs require access to the system, and the accounts shall be configured securely.
- Disable unnecessary services.
- Provide essential services using the most current and well-tested versions of the software configured as securely as possible.
- Monitor the system configuration to detect intrusion attempts or other unauthorized system modifications.
- Capture and log the access violations.
- Check and apply security patches frequently.

It is also important to isolate the servers that are accessible to external hosts and applications. These "exposed" systems are connected to each other on a series of

isolation networks. The isolation of these exposed hosts from direct external connections reduces the likelihood that they may be compromised. Also, they should be isolated from internal systems to reduce the chance of an attack on internal resources.

Applications

Applications provide business functionality that is intended to bring together employees, customers, partners, suppliers, and distributors to exchange and access information through the Internet. Since the applications are easily accessible through the Internet, they are highly vulnerable to, for example virus attacks and unauthorized access to protected data.

Applications can be protected from attacks by employing the following security measures:

- Provide application access controls that will ensure the integrity, confidentiality, and availability of data and business processes which use the data.
- Control the least possible number of access privileges and is based on a demonstrated need to view, add, change, or delete data.
- Capture operating system's audit trails to ensure that authorized and unauthorized users are accountable for all access to online functions and data access.
- Limit the direct access to data or database.
- Test and document all application access controls and access groups.

Conclusion

Preservation of confidentiality, integrity and availability of information is the most challenging issue in the Internet world. Although the above security measures address some major security threats, it is good to establish and implement security standards, guidelines, and procedures for each network elements.