Computer parts 17917

Technology, Computer

The world of computers has changed dramatically over the past 25 years. Twenty-five years ago, most computers were centralized and managed in data centers. Computers were kept in locked rooms and links outside a site were unusual. Computer security threats were rare, and were basically concerned with insiders. These threats were well understood and dealt with using standard techniques: computers behind locked doors and accounting for all resources. Twenty-five years later, many systems are connected to the Internet. The Internet is a huge network and has no boundaries. Businesses find an increasing need to connect to the internet to take advantage of the business opportunities.

The security framework for systems with internet connections is however very different. Information on the internet can be accessed from anywhere in the world in real time. While this is good for the spread of information, it has also allowed for the proliferation of malicious information . Hacker tools are now widely available on the internet. Some web sites even provides tutorials on how to hack into a system, giving details of the vulnerabilities of the different kinds of systems. It does not take an expert programmer to break into a system. Anyone with malicious intentions can search the internet for programs to break into a system which is not properly secured.

It is hence vital for businesses with connections to the internet to ensure that their networks are secure. This is important to minimize the risk of intrusions both from insiders and outsiders. Although a network cannot be 100% safe, a secure network will keep everyone but the most determined hacker out of the network. A network with a good accounting and auditing system will

ensure that all activities are logged thereby enabling malicious activity to be detected.

There are basically three overlapping types of security risks:

1. Bugs or misconfiguration problems in the Web server that allow unauthorized remote users to:

o Steal confidential documents not intended for their eyes.

o Execute commands on the server host machine, allowing them to modify the system.

o Gain information about the Web server's host machine that will allow them to break into the system.

o Launch denial-of-service attacks, rendering the machine temporarily unusable.

2. Browser-side risks, including:

o Active content that crashes the browser, damages the user's system, breaches the user's privacy, or merely creates an annoyance.

o The misuse of personal information knowingly or unkowingly provided by the end-user.

3. Interception of network data sent from browser to server or vice versa via network eavesdropping. Eavesdroppers can operate from any point on the pathway between browser and server including:

o The network on the browser's side of the connection.

o The network on the server's side of the connection (including intranets).

o The end-user's Internet service provider (ISP).

o The server's ISP.

o Either ISP s regional access provider.

It's important to realize that " secure" browsers and servers are only designed to protect confidential information against network eavesdropping. Without system security on browser and server sides, confidential documents are vulnerable to interception.

Before a network can be secured, a network security policy has to be established. A network security policy defines the organization s expectations of proper computer and network use and the procedures to prevent and respond to security incidents. A network security policy is the foundation of security because it outlines what assets are worth protecting and what actions or inactions threaten the assets. The policy will weigh possible threats against the value of personal productivity and efficiency and identify the different corporate assets, which need different levels of protection. Without a network security policy, a proper security framework cannot be established. Employees cannot refer to any established standards and security controls would be circumvented for the sake of increasing efficiency. A network security policy should be communicated to everyone who uses the computer network, whether employee or contractor.

Before a network security policy can be established, a risk analysis has to be studied. Risk analysis is the process of identifying what you need to protect, what you need to protect it from, and how to protect it. It is the process of examining all of your risks, and ranking those risks by level of severity.

Another way to protect the network is by installing firewall. Firewalls are tools that can be used to enhance the security of computers connected to a network, such as a LAN or the Internet. A firewall separates a computer from the Internet, inspecting packets of data as they arrive at either side of the firewall inbound to, or outbound from, your computer to determine whether it should be allowed to pass or be blocked. Firewalls act as guards at the computer s entry ports, where the computer exchanges data with other devices on the network. Firewalls ensure that packets that are requesting permission to enter the computer meet certain rules that are established by the user of the computer. Firewalls operate in two ways, by either denying or accepting all messages based on a list of designated acceptable or unacceptable sources, or by allowing or denying all messages based on a list of designated acceptable or unacceptable destination ports.

A good way of assessing the risks of network connectivity is to first evaluate the network to determine which assets are worth protecting and the extent to which these assets should be protected. In principle, the cost of protecting a particular asset should not be more than the asset itself. A detailed list of all assets, which include both tangible objects, such as servers and workstations, and intangible objects, such as software and data should be made. Directories that hold confidential or mission-critical files must be

identified. After identifying the assets, a determination of how much it cost to replace each asset must be made to prioritize the list of assets.

Although network security policies are subjective and can be very different for different organizations, there are certain issues that are relevant in most policies.

Physical Security - Network security interacts with physical security because the size or shape of the network " machine" or entity can span a building, campus, country or the world due to interconnections and trust relationships. Without physical security, the other issues of network security like confidentiality, availability and integrity will be greatly threatened. The physical security section states how facilities and hardware should be protected. This section will also define which employees should be granted access to restricted areas such as server rooms and wiring closets.

Network Security - The network security section states how assets stored on the network will be protected. This section might include security measures regarding access controls, firewalls, network auditing, remote access, directory services, Internet services, and file system directory structures.

Access Control - Access control determines who has access to what. There must be a proper procedure to ensure that only the right people have access to the right information or services. Good access control includes managing remote access and enabling administrators to be efficient in their work. It should not be so complex that it becomes easy to commit errors.

Authentication - Authentication is how users tell the network who they are. The type of authentication used varies depending on from where users are authenticating. From their desk, a simple user id and password may be sufficient because of the accompanying physical security. When connecting from the Internet, a more secure 2-factor authentication (token-based authentication) may be necessary.

Encryption - Encryption can ensure data integrity or protect sensitive information sent over insecure lines. Such protection is usually essential for remote access to important assets or as an extra protection when using the organization s intranet.

Developing a network security policy is not something, which can be done in a day or two. It is also not merely a technical issue, which can be left to the technical personnel. Success of the policy will depend largely on the support of the upper management and the awareness of employees of the organization.

Going through the whole process of developing a security policy is not enough. Threats change, vulnerabilities change, business requirements change and the available counter-measures change. All of these must be periodically and routinely re-evaluated to achieve a network security policy that is feasible, practical, enforceable and at the same time protects the network.

The diagram illustrates some common topologies for a modern enterprise network. The number and type of computer users on the network are

growing rapidly. And the number of wide area network services employed by the company to reach its network users is also expanding.

In this typical 3Com Security solution, secure tunneling ensures that proper security levels are maintained from wireless LANs and connections made over the public Internet. With 3Com's firewall and encryption protection prevents external intrusion while giving remote offices, telecommuters and mobile users full access to corporate resources.