Local Area Network / Wide Area Network Security Threat Analysis

A Guide for Non-Technical Managers responsible for a corporate network

Top Network Security Risks

1. Un-patched servers

Server systems used within the corporate network, both ones exposed to the internet, and internal servers that have no direct connection to the internet represent a potential major security risk.

While most IT departments would claim that they are diligent about applying patches as soon as they are available, this risk has to be taken very seriously as even large companies (Microsoft for example) have failed to patch all servers in a timely manner, leading to disruption of internal network traffic by Worms like Code Red and its variants. (Particularly at risk are internal servers that may be neglected because they don't connect directly to the internet)

2. Un-patched client software

Many common and freely available internet client applications, in particular Internet Explorer, Outlook Express, and Outlook contain security vulnerabilities that may be exploited by a large number of variations on Worm or Viral code. Many of the variations will slip past anti-virus software for several days before anti-virus software makers add their signatures to their software.

Many of these threats can be negated by making sure that all web browsing and e-mail software is regularly updated with all available security patches.

In the particular case of e-mail attachments, the single most dangerous and common security threat today, Using Microsoft Outlook 2000 patched to at least service release 2 and having the extended attachment security option installed completely blocks all executable content in email attachments. Microsoft Office XP includes the dangerous attachment blocking automatically.

It should be noted that no version of Microsoft's free Outlook Express offers effective blocking of dangerous attachments and users of Outlook Express should therefore have an up to date anti-virus utility installed on their system in addition to training on what attachments are safe to open.

3. Insecure peer to peer file sharing

Individual user's computers often have file and printer sharing turned on, allowing files to be copied directly between computers within an office. While this is very convenient and often essential to workgroup productivity, care must be taken when deciding what folders to share.

Workstation computer operating systems generally offer much less security than server operating systems. Network aware worms and viruses may take advantage of unprotected shared folders to spread from machine within a LAN. To prevent the possible spread of viruses between computers the root folder, program folders, and operating system folders should never be shared.

Only folders containing data files should be shared, and confidential data that must be shared should be stored on a server where more security is available.

4. Insecure passwords

When possible, any resources shared on a network should be protected by allowing access only with a valid user name and password combination. Passwords should be difficult to guess, and not shared or left in plain sight (i.e. stuck to the monitor.)

A strong password policy allows access to resources to be restricted as needed, to working hours, and an individual's access to confidential data can be disabled immediately upon termination.

5. Dial-up connections

Anyone with a dial-up internet account for personal use at home can easily configure a suitable computer within the corporate network to use the dial up connection, bypassing any safeguards implemented at the server level, exposing the corporate network to e-mail borne worms, Trojans, and viruses.

Keeping client and server software patched minimises the risks of uncontrolled dial-up internet connections, but providing a secured high speed internet connection eliminates the need for dial-up connections.

6. Residential high speed internet connections

Cable and ADSL high speed connections are very popular for residential internet connection. High speed residential internet connections suffer the same risks as dial-up internet connections but their tendency to be always-on and more often targeted for hacking makes them more at risk if not protected.

If employees have a fast internet connection at home and a slow connection at work, many will be tempted to download at home using little security precaution and then bring the downloads into the corporate network on CD-R or floppy disks.

As with dial-up connections, offering a fast internet connection in the workplace will reduce the likelihood that dangerous programs will be brought into the corporate network from home.

7. Corporate owned laptops

The portable nature of laptops leads them to often be connected to a multitude of network environments, (including client's networks) and often require the use of one or more different dial-up internet connections in addition to connection to the corporate network.

Additionally, disk space, speed and memory limitations often make keeping laptops up to date with security patches difficult.

8. Employee owned laptops

Employee's personal laptops suffer all of the same vulnerabilities as corporate owned laptops with the additional risk that there is no control over personal software that may be installed or the employee's dial-up or residential high speed internet connection.

Also it may be difficult or impossible to make sure that personal laptop or desktop computers have security patches installed as an employee may be well within his/her rights to disallow access to the personal equipment.

Protecting the Network

Being aware of the above threats and following the guidelines above will provide a reasonable level of safety for a corporate network, but additional steps are usually taken to further reduce security risks.

Firewalls and Network Address Translation

Most networks have the added security of a hardware or software firewall that blocks and discards any traffic coming into the network that is not expected. Computers behind the firewall usually are assigned special IP (Internet Protocol) addresses that can not be routed over the internet.

Network address translation is performed by a gateway router or proxy server (often integrated with the firewall) that allows computers with non-routable addresses to make requests from the internet.

There is no way that unsolicited traffic from the internet can de directed to a computer with a non-routable address unless the firewall/router etc. has been specifically programmed to pass traffic to a particular server (a web or mail server for example) behind the firewall.

Unfortunately a firewall can not prevent hostile applications running on individual workstations (such as Trojans, Viruses, and Worms) from opening security holes from inside a network, as the traffic can appear to be perfectly normal.

Programs like ZoneAlarm (which has a free version) try to identify suspicious outgoing traffic, but these need to be installed on each individual workstation and may be of limited usefulness because of a large number of false alarms.

The Bottom Line

Even If all of the above suggestions are followed to the extreme, there is still the chance that something can get past even the best planned network security; the internet will never be completely safe.

These suggestions should in most cases limit potential damage to a single computer. The failure to follow these suggestions, in particular allowing unsafe peer to peer file sharing with inadequate or non-existent passwords could allow a hostile application to spread to a large number of computers.