Godot Content Services
Website: content.godotmedia.com
Email: content@godotmedia.com

SAMPLE – Network Security Plan for ABC Corporation - Paper Excerpt

Potential Threats Faced by ABC Corporation's Network

A network attack can disrupt operations, integrity, functioning and even the availability of the whole network or some systems. Here are some of the major threats that the organization should identify and be prepared to combat.

Viruses

A virus is a malicious computer program that attaches itself to an executable file. There are multiple ways in which a virus can find its way into a computer system (a) as an e-mail attachment (b) file downloads through FTP or (c) along with a software program. Opening and running this program on a computer can damage files, the system's software or hardware. A virus can leave a trail of infection through file sharing and email forwarding.

Depending on the type of virus, the consequences the organization's systems face can be different. From annoying messages on the screen, a reduction in memory space and data modification to damaged or overwritten files and a complete erasing of the hard drive, a virus can operate in many destructive ways.

Worms

Like a virus, a worm is also a malicious computer program with the difference that it is capable of replicating itself and spreading through network connections on its own. For instance, a worm can send several copies of itself to all the contacts in the organization's email address book.

A worm consumes a lot of network bandwidth or system memory, and stops individual computer systems, as well as network and web servers, from responding. In extreme cases, worms may allow their malicious creators (and senders) to control the organization's systems remotely.

Trojan Horse

Masquerading as useful software, a Trojan horse is yet another malicious program that causes damage to computer systems on which it is run or installed. A Trojan does not replicate or infect other files. It deletes files and allows hackers to remotely access the organization's systems.

Some of the attacks that the organization's servers and clients can fall prey to include:

- Web server malfunctions caused by bugs in the web server software
- Information overload caused by sending a parameter that is outside the bounds of the system's programs. This causes crashes or gives hackers administrative access to the system.
- DoS (Denial of Service) attacks accomplished by flooding the web server with requests. This prevents other users from accessing the system.
- FTP server attacks because of bugs in FTP server software
- Clients can be infected when they connect to the web server affected by worms that are transmitted through normal HTTP communications.

The devices on the organization's networks (firewalls, switches, routers, remote access equipment) can suffer direct attacks. Weak account and password security, firmware and software vulnerabilities are the main reasons why these devices fall prey to attacks.

Network Security Measures to be Implemented

The organization should establish security baselines and policy templates that can be applied to its systems. The administrator should be aware of the different varieties of security software that can be installed on the organization's systems to protect them from the various kinds of attacks.

A combination of software firewalls and anti-virus programs on the organization's systems is a good way to combat viruses, worms and Trojans. An anti-virus program scans e-mail attachments for viruses while a software firewall prevents unauthorized access to the systems. It is advisable to keep the anti-virus as well as the systems' OS (operating system) updated, and to also run full disk scans on a periodic basis. A basic precaution against these malicious programs is to advise employees never to click an e-mail attachment from unknown senders. As far as application security is concerned, the administrator should block P2P and IM application types that do not deliver any value in a work environment.

Creation of network security zones, which also require very less administrative overhead, is highly recommended. Such topologies can be created using NAT (network address translation), VLANs (virtual local area networks) and NAC (network access control) protection schemes.

OS Hardening

OS hardening refers to keeping the organization's operating systems and software patches updated and doing away with unnecessary services from the systems. As the OS is the most critical part of any organization's computer system, the administrator should ensure that all the measures related to the security of the server and workstation operating systems are implemented.

As part of OS hardening, the administrator should ensure that the latest versions of software or bug fixes and patches are installed on the systems. He should examine other areas of the OS for security

vulnerabilities, including setting configuration options, examining available running devices and securing file systems. Other steps the administrator should take include:

- Ensure that the OS software of all the computers and servers are updated to the latest release versions with the most recent security patches applied
- Enable automatic operating system updates on all workstations to allow automatic updates through the network
- Establish clear security policies and baseline plans to ensure that all workstations are running a minimum level of software versions
- Install or enable only the necessary security and administrative-related options. The administrator should also take a close look at services that are not required, but installed by default, on all the systems.
- Set up user access restrictions for sensitive OS files

The organization's employees can also do their bit to help prevent external or internal attacks. This includes following password management best practices such as creating strong passwords and changing them on a periodic basis. They should adhere to the network security policies established by the organization, such as not interfering with the anti-virus scanning or automatic software download process.

Protecting Web Servers: The organization's web servers can be attacked in a number of ways. These include malformed requests (bugs in the web server software that cause it to malfunction), buffer overflow (an overflow of the system's data buffer causing crashes or providing administrative access to the system), worms, DoS (prevents users from accessing the organization's website). These attacks can be prevented by installing current web server and browser software, and applying the most recent security patches.

Protecting Email Servers: As worms and viruses are most often transmitted via e-mails, the security of e-mail servers (that store messages, and allow users to send and retrieve e-mail) assumes a lot of importance. E-mail servers should be secured to prevent spam e-mails from being sent to thousands of users. The administrator can secure the e-mail servers by ensuring that the e-mail software is current, with the latest service patches and revisions.

Protecting File Servers: The organization's file server should be configured such that access through the network is possible only with an authentication, using a user name and password. Also, the various files and directories should be secured with access permissions. The departmental directories should be set up such that only those who belong/work in that particular department can access their directory's files. A more common directory, like a directory of company policies and benefits that employees may need to access, should have a read-only permission.

User access permissions should also be set up for the organization's print servers. Setting up more granular security-access permissions for the print server will disallow users from deleting or modifying jobs after they have been sent to the printer.

In the case of database servers, the database software or query function should be configured or programmed correctly to prevent malicious users from bypassing built-in security. Keeping application and database software current is important to avoid such security vulnerabilities. Access permissions and authentication should be set up for the database server. While creating user accounts, it should be ensured that the passwords are complex and meet the minimum length requirements. The default database accounts (administrator or supervisor account) should have secure passwords.