The trojan horse virus: an overview

Another type of malware that is not technically a virus because there is usually no auto-replication is a Trojan horse program, which seems to be something useful, as a free utility, but actually contains some kind of malware. The unhappy about a Trojan program that is running the software users willingly and still do not know what is causing problems on their systems. Rootkits are a form of Trojan horse programs that can monitor the traffic from a computer, monitor keystrokes and capturing passwords. Are the most modern backdoor on one system and are between the most insidious Trojan horse software because they can mask that the system has been compromised by changing the file system and drivers needed for the normal operation of the computer.

Viruses

A virus is a program that spreads, replicating it in other programs or documents. Its only purpose is to interrupt the operation of your computer or network by deleting or corrupting files, disk formatting or by using large quantities of computer resources. Viruses and worms that spread through e-mail attachments were common place for years. They are simple to avoid; just don’t open any attachments from emails sent by someone who you aren’t expecting a message. Even if you know the sender, careful; malware programs may use address book from an e-mail program to send messages, causing you to believe that the message is safe. In fact, most virus scanners detect a virus or worm contained in an e-mail message and often excludes the annex before it ever reaches your Inbox, but if the virus is very new, it cannot be detected.

Worm

A worm is similar to a virus that replicates automatically, but a worm does not attach to another program; indeed, it is a standalone program. Worms are now more common than viruses, because with the Internet and network connectivity, worms in general do not need help to spread. Whereas a virus requires a user to run the program that contains the virus to operate and then copy this file to spread a worm can do their work without any help and can propagate through a network connection available. Some insidious actions that a worm can commit include using the network bandwidth, deleting files, send e-mails and creating backdoors in computers.

NETWORK SECURITY POLICY

Without a security policy, the availability of your network can be compromised. The policy begins with the assessment of risk to network and build a team to respond. Continuation of the policy requires the practical implementation of change management and monitoring of network security for breaches of security. Finally, the review process modifies the existing policy and adapts the lessons learned.

The last area of responsibility is the answer. While often network monitoring identifies a security violation, the security team members that are the real solution and fixing of such violation. Each Member of the security team should know in detail the security features provided by the equipment in its operational area.

While we define the responsibilities of the team as a whole, you must define the individual roles and responsibilities of the security team members in your security policy.

Approving Security Changes

Security changes are defined as changes to network equipment that can have an impact on overall network security. Your security policy must identify the requirements of specific security configuration in non-technical terms. In other words, instead of setting a requirement as “ no outside sources FTP connections will be allowed through the firewall”, set the requirement as “ outside connections should not be able to retrieve files from inside the network”. You need to define a unique set of requirements for your organization.

The security team should review the list of simple language requirements to identify issues of design requirements or specific network configuration. After the team created the network configuration changes necessary to implement the security policy, you can apply these possible future configuration changes. Although it is possible for the security team review all changes, this process enables them to only review the changes that risk sufficient to justify special treatment.

We recommend that the security team to review the following types of changes:

- Any change in the firewall configuration.
- Any amendment (ACL) of access control lists.
- Any changes to the configuration of the simple network management protocol (SNMP).
- Any change or update software that differs from the list of approved software revision.

We recommend that you also meet the following guidelines:

- Change passwords for network devices on a routine basis.
- To restrict access to network devices to a list of approved personnel.
- Ensure that the current revision levels of environments software network servers and equipment are in accordance with the security configuration requirements.

Monitoring Security of Your Network

Security monitoring is similar for network monitoring, except focuses on the detection of network changes that indicate a security breach. The starting point for security monitoring is to determine what constitutes a violation. Conduct a risk analysis, we identify the level of monitoring required based on the threat to the system. By adopting security changes, we identify specific threats to the network. Looking at both of these parameters, I will develop a clear picture of what you need to monitor and frequency.

In risk analysis matrix, the firewall is considered a high-risk network, indicating that he should follow. In approving security changes section, you'll find that you must monitor for changes to the firewall. This means that the SNMP polling agent should monitor things such as failed login attempts, unusual traffic, changes to the firewall, access granted to the firewall and configuration of connections through the firewall.

Following this example, create a monitoring policy to each area identified in your risk analysis. We recommend that the equipment of low risk, medium risk equipment weekly and daily monitoring equipment high-risk per hour. If you need more rapid detection, monitor in a short time interval.

Finally, your security policy should address how to notify the security team of security breaches. Often, your network monitoring software will be the first to discover the breach. It should trigger a notification to the operations centre, which in turn shall notify the security team using a pager number, if necessary.