Anti-Malware/Anti-Virus Programs

by Sophia

WHAT'S COVERED

In this lesson, we will continue to learn about a number of common considerations that should typically be incorporated into an enterprise security policy. We will then discuss common security procedures and conclude with a review of considerations for deploying anti-malware solutions in an enterprise network.

Specifically, this lesson will cover the following:

1. Security Policies
   - 1a. Downloading Patches and Hotfixes
   - 1b. Firmware Updates
   - 1c. Device Driver Updates
   - 1d. Asset Disposal
2. Security Procedures
   - 2a. Host-Based Anti-Malware
   - 2b. Cloud-/Server-Based Anti-Malware
   - 2c. Configuration Backups
   - 2d. Updating Antivirus Components
   - 2e. Heuristic Scanning
   - 2f. Upgrading an Antivirus Engine
   - 2g. Updating Definition Files
   - 2h. Scanning for Viruses
   - 2i. On-Demand Scan
   - 2j. On-Access Scan
   - 2k. Emergency Scan
   - 2l. Fixing an Infected Computer

1. Security Policies

As you learned in the previous tutorial, a security policy should define how security is to be implemented within an organization and include physical security, document security, and network security. Let's continue our introduction of common security policy considerations.

We will continue to explore these in the terms and concepts we will discuss in this lesson.

1a. Downloading Patches and Hotfixes

If you do not have automatic updates set up, you can download patches and hotfixes manually. A **hotfix** is just like a **patch** that updates software, but the term hotfix is reserved for a solution to potentially serious issues that could compromise your network and hosts.

TERMS TO KNOW

Hotfix

A code that fixes a bug in a product.

Patch

A file that describes changes to be made to a computer file or files, usually changes made to a computer program that fix a programming bug.

1b. Firmware Updates

While keeping operating system and application patches up to date gets most of the attention, there are devices on your network that may require firmware updates from time to time. **Firmware** is a form of program code and related data that is stored in persistent memory of some sort, such as non-volatile RAM (NVRAM).

TERM TO KNOW

Firmware

Something in between hardware and software. Like software, it is created from source code, but it is closely tied to the hardware it runs on.

1c. Device Driver Updates

Device Drivers are files that allow a peripheral or component to talk to the hardware layer of the hosting device. In most cases, the drivers you need for a device will already be present in the drive cache that is installed with the operating system, but in some cases, especially with new devices, this will not be the case. In those instances, you may need to download the latest driver from the manufacturer's website.

TERM TO KNOW

Device Driver

A program that acts as an interface between an application and hardware, written specifically for the device it controls.

1d. Asset Disposal

When the time comes to decommission an asset such as a server or a hard drive, the handling of any data that remains is a big security issue. Whenever data is erased or removed from a storage medium, residual data can be left behind. This can allow for the data to be reconstructed when the organization disposes of the medium, resulting in unauthorized individuals or groups gaining access to the data. Media that security professionals must consider include magnetic hard disk drives, solid-state drives, magnetic tapes, and optical media, such as CDs and DVDs.

KEY CONCEPT

When considering data remanence, security professionals must understand three countermeasures: clearing, purging, and destruction.

- Clearing includes removing data from the media so that the data cannot be reconstructed using normal file recovery techniques and tools. With this method, the data is only recoverable using special forensic techniques.
- Purging, also referred to as sanitization, makes the data unreadable even with advanced forensic techniques. With this technique, data should be unrecoverable.
- Destruction involves destroying the media on which the data resides.
  - Overwriting is a destruction technique that writes data patterns over the entire media, thereby eliminating any trace data.
  - **Degaussing**, another destruction technique, exposes the media to a powerful, alternating magnetic field, removing any previously written data and leaving the media in a magnetically randomized (blank) state. A degaussed disk cannot be reused.
  - Encryption scrambles the data on the media, thereby rendering it unreadable without the encryption key. It does not destroy the data; anyone with the encryption key can unlock it.
  - Physical destruction involves physically breaking the media apart, drilling holes in it, or chemically altering it. For magnetic media, physical destruction can also involve exposure to high temperatures.

TERM TO KNOW

Degauss

To reduce or eliminate the magnetic field.

2. Security Procedures

A **security procedure** defines how to respond to any security event that happens on your network.

KEY CONCEPT

Here's a short list of items you might include:

- What to do when someone has locked themselves out of their account
- How to properly install or remove software on servers
- What to do if files on the servers suddenly appear to be deleted or altered

- How to respond when a network computer has a virus
- Actions to take if it appears that a hacker has broken into the network
- Actions to take if there is a physical emergency such as a fire or flood

Of all the update types that need to be maintained, anti-malware updates are the most critical to the organization. You must maintain updates to the malware definitions as well as updates to the malware engine itself. When choosing an anti-malware solution, there are two approaches: host based and cloud based. In the following sections, we will examine both.

TERM TO KNOW

Security Procedure

An action in response to any security event that happens on your network.

2a. Host-Based Anti-Malware

Host-based anti-malware is a solution that you install and run on each PC in your network. It has the advantage of giving you total control over the process but also requires you to stay on top of updates. It also requires the deployment of some hardware to hold the engine and the definition files.

2b. Cloud-/Server-Based Anti-Malware

Cloud antivirus products do not run on local computers but run in the cloud, creating a smaller footprint on the client and utilizing processing power in the cloud.

KEY CONCEPT

They have the following advantages:

- They allow access to the latest malware data within minutes of the cloud antivirus service learning about it.
- They eliminate the need to continually update your antivirus software.
- The client is small, and it requires little processing power.

Cloud antivirus products have the following disadvantages:

- There is a client-to-cloud relationship, which means they cannot run in the background.
- They may scan only the core Windows files for viruses and not the whole computer.
- They are highly dependent on an internet connection.

IN CONTEXT

Should you install host-based or cloud-/server-based anti-malware for your network?

Imagine that you manage a very large enterprise network and need to keep a close eye on the most common attacks today: malware. You should ideally install a next-generation intrusion prevention system (IPS) device, but you do not have the money for that type of equipment and the necessary

training. You need something that will stop zero-day attacks if possible and do not want to add much processing or even more software on the hosts in the network than you already have. You do not want to install any new hardware, if possible, to get this done. With all this in mind, cloud/server-based anti-malware may be the best solution because it allows access to the latest malware data within minutes of the cloud antivirus service learning about it, and you do not need to install any new hardware at your location. You just need a good, solid internet connection.

2c. Configuration Backups

Network professionals often create device configurations over time that can be quite complicated, and in some cases where multiple technicians have played a role, no single person has a complete understanding of the configuration. For this reason, configurations should be backed up.

HINT

Configurations may sometimes exist as text files, such as in a router or switch. Other times, such as with a Microsoft server, you will back up what is called the **system state**. This backs up only the operating system's configuration of the server (for example, the Registry if it's a Windows server) and not the data. In this case, a system-state backup and a data backup should be performed. It is also possible to back up the entire computer, which would include both data sets.

Considering the time it takes to set up a new device, install the operating system, and reconfigure it to replace a defective device, it makes great sense to keep backups of configurations so that if a device fails, you can quickly reimage a new machine and simply apply the system state to it or apply the configuration file in the case of routers and switches.

TERM TO KNOW

System State

A snapshot of a device's configuration at a specific point in time.

2d. Updating Antivirus Components

A typical antivirus program consists of two components:

- The definition files
- The engine

The definition files list the various viruses, their types, and their footprints and tell you how to remove them. More than 100 new viruses are found on the internet each month, so it is easy to see that an antivirus program would be totally useless if it did not keep up with all those emerging viruses.
The engine accesses the definition files, runs virus scans, cleans the files, and notifies the appropriate people and accounts. Eventually, viruses become so sophisticated that a new engine, or even a whole new technology, is required to combat them effectively.

2e. Heuristic Scanning

Heuristic scanning is a technology that allows an antivirus program to search for a virus even if there's no definition for it yet. The engine looks for suspicious activity of the kind that usually indicates the presence of a virus. But use such a tool with caution because if it is turned on, this scanning technique can mistake harmless or even necessary code for suspicious code.

EXAMPLE For your antivirus program to work for you, you have to upgrade, update, and scan in a specific order:

1. Upgrade the antivirus engine.
2. Update the definition files.
3. Create an antivirus emergency boot disk.
4. Configure and run a full on-demand scan.
5. Schedule monthly full on-demand scans.
6. Configure and activate on-access scans.
7. Make a new antivirus emergency boot disk every month.
8. Get the latest updates when fighting a virus outbreak.
9. Repeat all steps when you get a new engine.

EXAMPLE We are going to cover only the steps in this list that map to objectives of the Network+ exam, but looking into the others on your own will not hurt and will give you some worthwhile knowledge.

TERM TO KNOW

Heuristic Scan

A virus scan that identifies code and/or behavioral patterns common to a class or family of viruses.

2f. Upgrading an Antivirus Engine

An antivirus engine is the core program that runs the scanning process, and virus definitions are keyed to an engine version number. For example, a 3.x engine will not work with 4.x definition files. When the manufacturer releases a new engine, consider both the cost to upgrade and how much you will benefit before buying it.

2g. Updating Definition Files

We recommend that you update your list of known viruses, called the **virus definition files**, no less than weekly. You can do this manually or automatically through the vendor's website, and you can use a staging server within your company to download and distribute the updates or set up each computer to download updates individually.

TERM TO KNOW

Virus Definition File

A database of known virus signatures.

2h. Scanning for Viruses

An **antivirus scan** is the process that an antivirus program deploys to examine a computer, identify viruses, and then eliminate them. There are three types of antivirus scans, and to really make sure your system is clean, you should use a combination of the types we cover in this section.

TERM TO KNOW

Antivirus Scan

The process that an antivirus program deploys to examine a computer, identify viruses, and then eliminate them.

2i. On-Demand Scan

An **on-demand scan** is a virus scan initiated by you or an administrator that searches a file, a directory, a drive, or an entire computer but only checks the files you're currently accessing. We recommend doing this at least monthly, but you will also want to do an on-demand scan when the following occurs:

- You first install the antivirus software
- You upgrade the antivirus software engine
- You suspect a virus outbreak

TERM TO KNOW

On-Demand Scan

A virus scan that, when initiated, searches a file, a directory, a drive, or an entire computer but only checks the files currently open.

2j. On-Access Scan

An **on-access scan** runs in the background when you open a file or use a program in situations like these:

- Inserting a thumb drive or an external drive
- Downloading a file with FTP
- Receiving email messages and attachments
- Viewing a web page

This kind of scan slows down the processing speed of other programs, but it is worth the inconvenience.

TERM TO KNOW

On-Access Scan

A virus scan that runs in the background when you open a file or use a program.

2k. Emergency Scan

During an **emergency scan**, only the operating system and the antivirus program are running. You initiate one of these scans when a virus has totally invaded your system and taken control of the machine. In this situation, insert your antivirus emergency boot disk and boot the infected computer from it. Then, scan and clean the entire computer. If you do not have your boot disk, go to another, uninfected machine and create one from it.

Another possibility is to use an emergency scan website that allows you to scan your computer via high-speed internet access without using an emergency disk.

TERM TO KNOW

Emergency Scan
A virus scan performed with only the operating system and the antivirus program running.

2I. Fixing an Infected Computer

So what do you do if you know you have a virus? First, you want to make sure to scan all potentially affected hard disks and any external disks that could be infected. Establish a cleaning station, and quarantine the infected area. You will have a really hard time doing this if anyone continues to use the computer while it is infected, so make sure all users in the infected area stop using their computers.

Then, remove all external memory devices from all disk drives and perform a scan and clean at the cleaning station. Update the virus definitions of any computers that are still operational. For the ones that are not, or the ones that are still working but are infected, boot to an antivirus emergency boot disk. After you have done that, run a full scan and clean the entire system on all computers in the office space.

SUMMARY

In this lesson, you learned a number of common considerations that should typically be incorporated into an enterprise **security policy**. We discussed common **security procedures** and concluded with a review of considerations for deploying anti-malware solutions in an enterprise network.

Source: This content and supplemental material has been adapted from CompTIA Network+ Study Guide: Exam N10-007, 4th Edition. Source **Lammle: CompTIA Network+ Study Guide: Exam N10-007, 4th Edition - Instructor Companion Site (wiley.com)**

TERMS TO KNOW

Antivirus Scan
The process that an antivirus program deploys to examine a computer, identify viruses, and then eliminate them.

Degauss
To reduce or eliminate the magnetic field.

Device Driver
A program that acts as an interface between an application and hardware, written specifically for the device it controls.

Emergency Scan

A virus scan performed with only the operating system and the antivirus program running.

Firmware

Something in between hardware and software. Like software, it is created from source code, but it is closely tied to the hardware it runs on.

Heuristic Scan

A virus scan that identifies code and/or behavioral patterns common to a class or family of viruses.

Hotfix

A code that fixes a bug in a product.

On-Access Scan

A virus scan that runs in the background when you open a file or use a program.

On-Demand Scan

A virus scan that, when initiated, searches a file, a directory, a drive, or an entire computer but only checks the files currently open.

Patch

A file that describes changes to be made to a computer file or files, usually changes made to a computer program that fix a programming bug.

Security Procedure

An action in response to any security event that happens on your network.

System State

A snapshot of a device's configuration at a specific point in time.

Virus Definition File

A database of known virus signatures.