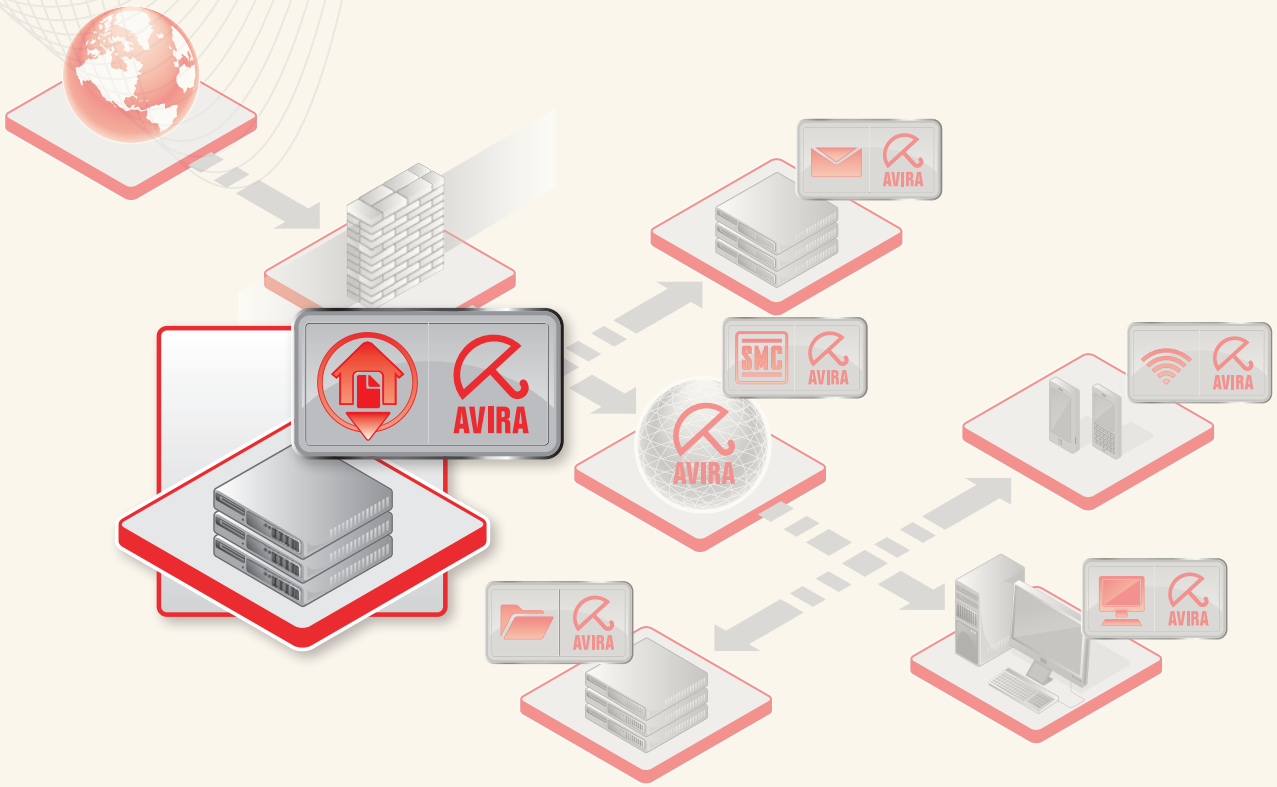
AVIRA
More Than Security

User Manual

Avira AntiVir SharePoint



www.avira.com

Trademarks and Copyright

Trademarks

AntiVir is a registered trademark of Avira GmbH.
Windows is a registered trademark of the Microsoft Corporation in the United States and other countries.
All other brand and product names are trademarks or registered trademarks of their respective owners.
Protected trademarks are not marked as such in this manual. This does not mean, however that they may be used freely.

Copyright information

A code provided by a third party has been used for Avira AntiVir SharePoint. We thank the copyright owners for making the code available to us. For detailed information on copyright, please refer to in the help of Avira AntiVir SharePoint under the Third Party Licenses.

Table of Contents

1 Introduction

Avira AntiVir SharePoint protects your SharePoint systems against viruses, malware, adware and spyware, unwanted programs and other dangers. This manual deals with viruses and software in brief.

Note
The program's full name is Avira AntiVir SharePoint. For greater readability, this name is abbreviated to AntiVir SharePoint.

Please go to our website at http://www.avira.com to download the Avira AntiVir SharePoint handbook in PDF form, update Avira AntiVir SharePoint or renew your license.

You will also find information on our website such as telephone numbers for technical support and information on how to subscribe to our newsletter.

2 Icons and emphases

The following icons are used:

Icon	Explanation
✓	Placed before a condition which must be fulfilled prior to implementation.
▸	Placed before an action step that you implement.
→	Placed before an event that follows the previous action.
Note	Placed before a link to particularly important information or a tip that makes AntiVir for Sharepoint easier to use.
Warning	This precedes a warning. Please observe the warnings in order to ensure that the Antivir for SharePoint virus protection function takes full effect.

The following emphases are used:

Emphasis	Explanation
Cursive	File name or path data.
	Displayed software interface elements (e.g. window heading, window field or options box).
Bold	Clicked software interface elements (e.g. menu item, tab or button)

3 Product information

3.1 Function overview

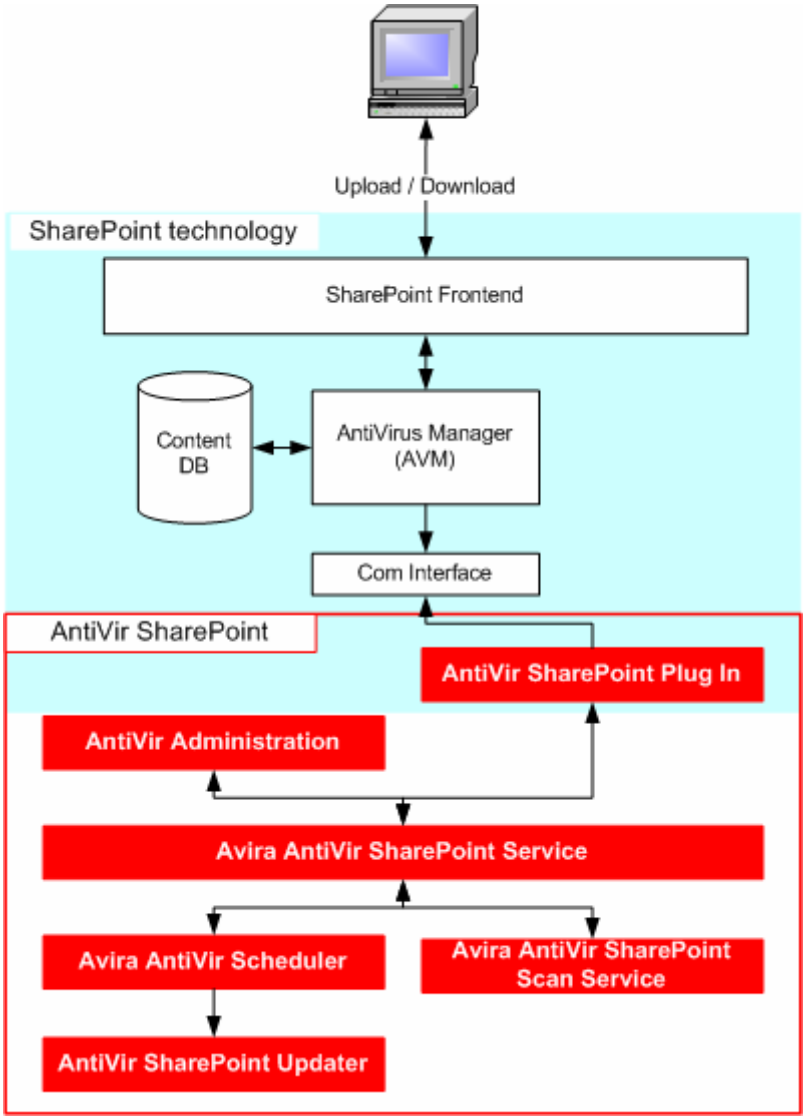
AntiVir SharePoint is an antivirus solution developed specially for Microsoft SharePoint and supports the following SharePoint technology:

- Microsoft Office SharePoint Server 2007
- Microsoft Windows SharePoint Services 3.0
- Microsoft Office SharePoint Portal Server 2003
- Microsoft Windows SharePoint Services 2.0

Microsoft SharePoint technology enables a company's documents to be made available to users at a central point and manages these documents with a version control. Documents are accessed by means of a web interface - the SharePoint team pages - by uploading and downloading. The documents and files are saved in a central MS SQL database. This is a serious problem for security because the data cannot be protected against virus attacks using a conventional antivirus solution such as an on-demand or on-access virus scanner: On-demand and on-access virus scanners require that the data to be scanned should exist as files in the file system.

Depending on the configuration, AntiVir SharePoint scans documents for viruses and malware at every upload and downloaded to/from the SharePoint team pages. If a virus is found, transfer is prevented if the document cannot be repaired.

Architecture:



The use of external antivirus programs is controlled by means of the Antivirus Manager (AVM) in SharePoint technology. Antivirus functions can be enabled in the SharePoint Antivirus settings. If the virus protection functions are enabled, the AVM transfers the data transferred by users for uploading or requested by users for downloading to an external antivirus program.

AntiVir is integrated in the SharePoint technology by means of a plug-in: The AntiVir SharePoint plug-in processes SharePoint requests for virus scans and forwards these to the Avira AntiVir SharePoint service. Avira AntiVir SharePoint service forwards requests for virus scans to the Avira AntiVir SharePoint scan service and processes the Avira Administration settings. The Avira AntiVir Scheduler service starts the update component in order to perform regular updates. AntiVir Administration is a snap-in of the Microsoft Management Console (MMC). The Avira AntiVir SharePoint scan service scans for viruses and malware.

3.2 Delivery scope

AntiVir SharePoint offers extensive antivirus protection for corporate data that you manage and provide using SharePoint technology. This also protects the computer systems used for SharePoint. AntiVir SharePoint is easy to install and has the following configuration options:

Settings for scanning for viruses and malware:

- OLE heuristics and Win32 file heuristics.
- Archive scan

Settings in relation to the automatic update (update of the scanning engine and virus definition file):

- Webserver or fileserver can be updated
- A proxy server can be used for updates
- Email notification function

3.3 System requirements

Avira AntiVir SharePoint supports the following SharePoint technologies:

- Microsoft Office SharePoint Server 2007
- Microsoft Windows SharePoint Services 3.0
- Microsoft Office SharePoint Portal Server 2003
- Microsoft Windows SharePoint Services 2.0

The following system requirements and specifications are required:

- Executable SharePoint technology: SharePoint Server 2007 or SharePoint Services 3.0 or SharePoint Portal Server 2003 or Windows SharePoint Services 2.0
- Server computers with processor speed 2.5 GHz (Gigahertz) or higher, 32 or 64 bit processor
- At least 1 GB RAM, 2 GB recommended
- 130 MB free memory space on the hard disk
- At least 100 MB temporary memory on the hard disk

3.4 Licensing

You require a license to use Avira AntiVir SharePoint. The license is issued in the form of a digital license key in the file hbedv.key. You can obtain the license file by email from Avira GmbH. The license file contains the license for all products that you have ordered in one order process.

Activate your license for the Avira AntiVir SharePoint with the license file hbedv.key. During the installation process you will be asked to load the license file. To extend your license or load the license after installation, save the license file to the installation directory.

4 Installation and uninstallation

4.1 Installation

Before installing AntiVir SharePoint, check the following requirements:

✓ Ensure that the system requirements are met (see System requirements).

✓ Ensure that you are logged in to the computer as an administrator or as a user with administrator rights.

✓ Ensure that an Internet connection or network connection to a download server exists for updating AntiVir SharePoint. If you use a fileserver, you may require a user name and a password for server login.

✓ Ensure that a valid license file hbedv.key exists and is stored in a local directory on the server.

Installation types

Full

No destination folder can be selected for the program files to be installed.

User-defined

A target folder can be selected for the program files to be installed.

Performing installation

Avira AntiVir SharePoint is installed as follows:

▶ Start the installation program by double-clicking on the installation file you have downloaded from the Internet or insert the program CD.

→ After a safety message, which acknowledges the producer of the software, the installation file will be decompressed.

▶ Click **Next**.

→ The setup program is started and a message appears allowing you to confirm the pausing of the WWW publishing service. The WWW publishing service must be stopped before AntiVir SharePoint can be installed. The websites hosted on this server are unavailable during setup.

▶ Confirm that you want to pause the WWW publishing service with **Yes.**

→ The Avira AntiVir SharePoint installation wizard opens up. Follow the instructions of the installation wizard. Complete the following installation steps:

▶ Where appropriate, install Microsoft Visual C++ 2008 - Redistributable Kit, if the kit has not already been installed.

Note
Avira AntiVir SharePoint uses the runtime libraries of the Microsoft Visual C++ 2008 - Redistributable Kit. To use AntiVir SharePoint, Microsoft Visual C++ 2008 - Redistributable Kit must therefore be installed.

- Confirmation of license agreements
- Selection of setup type (complete installation or custom installation)
- Licensing of the AntiVir Server: Loading of the license file or selection of the 30-day evaluation license
- Installation of the components of Avira AntiVir SharePoint.

After installation, the antivirus function of the SharePoint AntiVirus Manager is enabled, AntiVir SharePoint is configured with default settings.

Update

After installation, AntiVir SharePoint should be updated: Ensure that AntiVir SharePoint can receive data from the Internet. A proxy server through which AntiVir SharePoint receives updates can be specified in the AntiVir SharePoint configuration:

Specify a proxy server for receiving updates under Settings :: Configure Update :: Proxy.

Note
You can change settings in the SharePoint AntiVirus Manager in SharePoint central administration under **SharePoint central administration :: Security configuration :: Configure Antivirus settings**.

Warning
Please note the following when making settings in SharePoint central administration: Antivirus protection must be enabled when uploading and downloading documents so that Avira AntiVir SharePoint checks documents that are uploaded or downloaded to or from SharePoint team pages.

Note
You can change the AntiVir SharePoint default settings and implement other settings in AntiVir Administration. Configuration of the update by means of a proxy server or fileserver, configuration of the email notification function.

4.2 Uninstallation

Uninstallation is carried out via the control panel of the operating system:

- Under **System Controller :: Software**, find the Avira AntiVir SharePoint and click the **Remove** option.
- Confirm uninstallation.

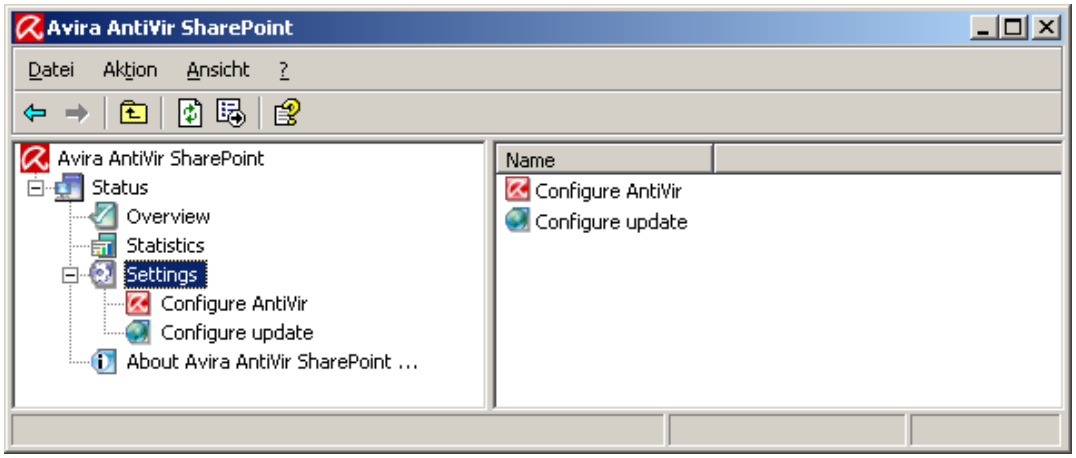
During uninstallation, AntiVir services are stopped and all program files and report files are deleted.

5 User interface and operation

The antivirus function of Avira AntiVir SharePoint can be controlled, i.e. enabled or disabled, by the SharePoint AntiVirus Manager. You will find the settings for the SharePoint AntiVirus Manager in SharePoint central administration under **Security configuration :: Configure Antivirus settings**. After installation, the antivirus function is enabled by default.

Warning
Please note the following when making settings in SharePoint central administration: Antivirus protection must be enabled when uploading and downloading documents so that Avira AntiVir SharePoint checks documents that are uploaded or downloaded to or from SharePoint team pages.

AntiVir Sharepoint is configured in AntiVir Administration. AntiVir Administration is a snap-in of the Microsoft Management Console (MMC).



Note
Please note that only the proprietary elements of AntiVir Administration are documented in this help. For information on the MMC and on manual integration of a snap-in, please refer to the user manual or the online help of the operating system.

Starting and stopping AntiVir Administration

Start AntiVir Administration via the link under Programs::Avira::AntiVir SharePoint::Avira AntiVir SharePoint user interface. You can also load AntiVir Administration directly in the MMC. You will find the AntiVir console file in the installation directory of AntiVir SharePoint. To end AntiVir Administration, you must close MMC.

Operation

– Navigate via the console structure in the left-hand window of the MMC. Navigation elements are also displayed as objects in the right-hand detail window of the MMC. Open these objects in the detail window by double-clicking. The AntiVir SharePoint configuration can be found under the **Settings** node. You can select various configuration sections in the detail window: The *Configure AntiVir* window is opened in which you can configure the selected section.

- Commands and actions are available in the details window via links.
- When configuring AntiVir SharePoint , you must confirm information in the *Configure AntiVir* window with the button **OK** in order to apply the new settings. Your settings are cancelled with the button **Cancel**.

Get the AntiVir SharePoint product version

You can get the product version of AntiVir SharePoint in the MMC help menu under **About Avira AntiVir SharePoint...**.

Accessing help

You can also access the help via the Help icon in MMC or with F1.

Overview of AntiVir Administration

Avira AntiVir SharePoint

Status

- Display the connection status of AntiVir Administration for the AntiVir SharePoint services
- Actions: **Connect servers** when a connection to the AntiVir SharePoint services is disconnected

Overview

- Display the status of AntiVir SharePoint services: AntiVir SharePoint Service and AntiVir SharePoint Scan Service
- Display system status: Last update, VDF and engine version
- Actions: Start update (VDF/engine)

Statistics

- Display the statistical data of the virus scan
- Actions: Reset statistics

Settings

- **Configure AntiVir**: Options for heuristics and archive scanning
- **Configure update**: Download method (via webserver or fileserver), configuration of connection to the download server, email notification function

About Avira AntiVir SharePoint...

- Display contact and support information

6 Virus detection

When documents are uploaded to or downloaded from SharePoint Team pages, Avira AntiVir SharePoint scans these documents for viruses and malware. If AntiVir finds viruses or malware in a document, this is reported to SharePoint. SharePoint prevents the transfer of the document. The SharePoint team page user receives a message:

Note
You can specify what is to happen when a virus is found in SharePoint central administration under **Security configuration :: Configure antivirus settings**. This means, for example, that you can allow infected files to be downloaded to allow users to check infected documents for viruses and malware on their own computer system.

Warning
Please note the following when making settings in SharePoint central administration: Antivirus protection must be enabled when uploading and downloading documents so that Avira AntiVir SharePoint checks documents that are uploaded or downloaded to or from SharePoint team pages.

7 Updates

The effectiveness of antivirus software depends entirely on the scanning engine and the virus definitions being up to date. For this reason, you should regularly download updates for Avira SharePoint from our download servers. To enable regular updates to be carried out, the AntiVir SharePoint Updater component is integrated in AntiVir SharePoint. The component updates the following program components:

- Virus definition file
- Scanning engine

In AntiVir Administration under *Configure Update* you can set up the update orders which are started by the Avira AntiVir planner service and which are executed by the update component. With every update order, the status of the virus definition files and the scanning engine is checked and updated if necessary. You can activate an update manually in AntiVir Administration under **Overview :: Last Update**. After an update AntiVir SharePoint does not have to be restarted.

You can obtain updates via the following servers:

- directly from the Internet via a webserver of Avira GmbH. The following update webservers are available:
  http://professional.avira-update.com/update
  http://professional.avira-update.net/update
  http://62.146.210.32/update

- via a webserver or fileserver in the Intranet, which downloads the update files from the Internet and supplies them to other systems in the network. This is useful if you want to update AntiVir SharePoint on more than one computer in a network. This ensures that AntiVir SharePoint is kept up to date on the computer systems to be protected in a resource-saving way.

When a webserver is used, the HTTP protocol is used for the download. When using a fileserver, access to the update file is provided via the network. You can the update to AntiVir Administration under the update configuration.

Note
You can use AntiVir Internet Update Manager (fileserver or webserver in Windows) as a webserver or fileserver in the intranet. This program mirrors the download servers of AntiVir products (including AntiVirShare Point) and is available on the Internet at http://www.avira.com.

8 Viruses and more

8.1 Extended threat categories

Dialers (DIALERS)

Certain services available in the Internet have to be paid for. They are invoiced in Germany via dialers with 0190/0900 numbers (or via 09x0 numbers in Austria and Switzerland; in Germany, the number is set to change to 09x0 in the medium term). Once installed on the computer, these programs guarantee a connection via a suitable premium rate number whose scale of charges can vary widely.

The marketing of online content via your telephone bill is legal and can be of advantage to the user. Genuine dialers leave no room for doubt that they are used deliberately and intentionally by the user. They are only installed on the user's computer subject to the user's consent, which must be given via a completely unambiguous and clearly visible labeling or request. The dial-up process of genuine dialers is clearly displayed. Moreover, genuine dialers tell you the incurred costs exactly and unmistakably.

Unfortunately there are also dialers which install themselves on computers unnoticed, by dubious means or even with deceptive intent. For example they replace the Internet user's default data communication link to the ISP (Internet Service Provider) and dial a cost-incurring and often horrendously expensive 0190/0900 number every time a connection is made. The affected user will probably not notice until his next phone bill that an unwanted 0190/0900 dialer program on his computer has dialed a premium rate number with every connection, resulting in dramatically increased costs.

We recommend that you ask directly your telephone provider to block this number range to be immediately protected against undesired dialers (0190/0900 dialers).

Games (GAMES)

There is a place for computer games - but it is not necessarily at work (except perhaps in the lunch hour). Nevertheless, with the wealth of games downloadable from the Internet, a fair bit of mine sweeping and Patience playing goes on among company employees and civil servants. You can download a whole array of games via the Internet. Email games have also become more popular: numerous variants are circulating, ranging from simple chess to "fleet exercises" (including torpedo combats): The corresponding moves are sent to partners via email programs, who answer them.

Studies have shown that the number of working hours devoted to computer games has long reached economically significant proportions. It is therefore not surprising that more and more companies are considering ways of banning computer games from workplace computers.

Jokes (JOKES)

Jokes are merely intended to give someone a fright or provide general amusement without causing harm or reproducing. When a joke program is loaded, the computer will usually start at some point to play a tune or display something unusual on the screen. Examples of jokes are the washing machine in the disk drive (DRAIN.COM) or the screen eater (BUGSRES.COM).

But beware! All symptoms of joke programs may also originate from a virus or Trojan. At the very least users will get quite a shock or be thrown into such a panic that they themselves may cause real damage.

Security Privacy Risk (SPR)

Software that maybe is able to compromise the security of your system, initiate unwanted program activities, damage your privacy or spy out your user behavior and might therefore be unwanted.

Backdoor Clients (BDC)

In order to steal data or manipulate computers, a "backdoor" server program is smuggled in unknown to the user. This program can be controlled by a third party using backdoor control software (client) via the Internet or a network.

Adware/Spyware (ADSPY)

Software that displays advertising or software that sends the user's personal data to a third party, often without their knowledge or consent, and for this reason may be unwanted.

Unusual Runtime Compression Tools (PCK)

Files that have been compressed with an unusual runtime compression tool and that can therefore be classified as possibly suspicious.

Double Extension Files (HEUR-DBLEXT)

Executable files that hide their real file extension in a suspicious way. This camouflage method is often used by malware.

Phishing

Phishing, also known as *brand spoofing* is a clever form of data theft aimed at customers or potential customers of Internet service providers, banks, online banking services, registration authorities.
When submitting your email address on the Internet, filling in online forms, accessing newsgroups or websites, your data can be stolen by "Internet crawling spiders" and then used without your permission to commit fraud or other crimes.

Application (APPL)

The term APPL refers to an application which may involve a risk when used or is of dubious origin.

Possible Fake Software (PFS)

The designation PFS ("Possible Fake Software") indicates software that usually comes at a charge but that contains no functions or that installs dubious components.

Adware (ADWARE)

This software or components installed by it will display advertisements on your system.

8.2 Viruses and other malware

Adware

Adware is software that presents banner ads or in pop-up windows through a bar that appears on a computer screen. These advertisements usually cannot be removed and are consequently always visible. The connection data allow many conclusions on the usage behavior and are problematic in terms of data security.

Backdoors

A backdoor can gain access to a computer by going around the computer access security mechanisms.

A program that is being executed in the background generally enables the attacker almost unlimited rights. User's personal data can be spied with the backdoor's help, but are mainly used to install further computer viruses or worms on the relevant system. The connection data allow many conclusions on the usage behavior and are problematic in terms of data security.

Boot viruses

The boot or master boot sector of hard disks is mainly infected by boot sector viruses. They overwrite important information necessary for the system execution. One of the awkward consequences: the computer system cannot be loaded any more...

Bot-Net

A Bot-Net is defined as a remote network of PCs (on the Internet), which is composed of bots that communicate with each other. A Bot-Net can comprise a collection of cracked machines running programs (usually referred to as worms, Trojans) under a common command and control infrastructure. Bot-Nets serve various purposes, including Denial-of-Service attacks etc., partly without the affected PC user's knowledge. The main potential of Bot-Nets is that the networks can achieve dimensions on thousands of computers and its bandwidth sum bursts most conventional Internet accesses.

Exploit

An exploit (security gap) is a computer program or script that takes advantage of a bug, glitch or vulnerability leading to privilege escalation or denial of service on a computer system. One form of exploitation for example is an attack from the Internet with the help of manipulated data packages. Programs can be infiltrated in order to obtain higher access.

Hoaxes

For several years, Internet and other network users have received alerts about viruses that are purportedly spread via email. These alerts are spread per email with the request that they should be sent to the highest possible number of colleagues and to other users, in order to warn everyone against the "danger".

Honeypots

A honeypot is a service (program or server) installed in a network. Its function is to monitor a network and log attacks. This service is unknown to the legitimate user - because of this reason he is never addressed. If an attacker examines a network for the weak points and uses the services which are offered by a Honeypot, it is logged and an alert is triggered.

Macro viruses

Macro viruses are small programs that are written in the macro language of an application (e.g. WordBasic under WinWord 6.0) and that can normally only spread within documents of this application. Because of this, they are also called document viruses. In order to be active, they need that the corresponding applications are activated and that one of the infected macros has been executed. Unlike "normal" viruses, macro viruses consequently do not attack executable files but they do attack the documents of the corresponding host-application.

Pharming

Pharming is a manipulation of the host file of web browsers to divert enquiries to spoofed websites. This is a further development of classic phishing. Pharming fraudsters operate their own large server farms on which fake websites are stored. Pharming has established itself as an umbrella term for various types of DNS attacks. In the case of a manipulation of the host file, a specific manipulation of a system is carried out with the aid of a Trojan or virus. The result is that the system can now only access fake websites, even if the correct web address is entered.

Phishing

Phishing means angling for personal details of the Internet user. Phishers generally send their victims apparently official letters such as emails that are intended to induce them to reveal confidential information to the culprits in good faith, in particular user names and passwords or PINs and TANs of online banking accounts. With the stolen access details, the phishers can assume the identities of the victims and carry out transactions in their name. What is clear is that banks and insurance companies never ask for credit card numbers, PINs, TANs or other access details by email, SMS or telephone.

Polymorph viruses

Polymorph viruses are the real masters of disguise. They change their own programming codes - and are therefore very hard to detect.

Program viruses

A computer virus is a program that is capable of attaching itself to other programs after being executed and cause an infection. Viruses multiply themselves unlike logic bombs and Trojans. In contrast to a worm, a virus always requires a program as host, where the virus deposits its virulent code. The program execution of the host itself is not changed as a rule.

Rootkit

A rootkit is a collection of software tools that are installed after a computer system has been infiltrated to conceal logins of the infiltrator, hide processes and record data - generally speaking: to make themselves invisible. They attempt to update already installed spy programs and reinstall deleted spyware.

Script viruses and worms

Such viruses are extremely easy to program and they can spread - if the required technology is on hand - within a few hours via email round the globe.

Script viruses and worms use one of the script languages, such as Javascript, VBScript etc., to insert themselves in other, new scripts or to spread themselves by calling operating system functions. This frequently happens via email or through the exchange of files (documents).

A worm is a program that multiplies itself but that does not infect the host. Worms can consequently not form part of other program sequences. Worms are often the only possibility to infiltrate any kind of damaging programs on systems with restrictive security measures.

Spyware

Spyware are so called spy programs that intercept or take partial control of a computer's operation without the user's informed consent. Spyware is designed to exploit infected computers for commercial gain.

Trojan horses (short Trojans)

Trojans are pretty common nowadays. We are talking about programs that pretend to have a particular function, but that show their real image after execution and carry out a different function that, in most cases, is destructive. Trojan horses cannot multiply themselves, which differentiates them from viruses and worms. Most of them have an interesting name (SEX.EXE or STARTME.EXE) with the intention to induce the user to start the Trojan. Immediately after execution they become active and can, for example, format the hard disk. A dropper is a special form of Trojan that 'drops' viruses, i.e. embeds viruses on the computer system.

Zombies

A Zombie-PC is a computer that is infected with malware programs and that enables hackers to abuse computers via remote control for criminal purposes. On command, the affected PC starts denial-of-service (DoS) attacks, for example, or sends spam and phishing emails.

9 Info and Service

In AntiVir Administration under *About...* you will find the information about our contact and support addresses. We are always happy to receive your suggestions about how our products could be improved. In the case of undetected suspect files in particular, and in the event of false alarms, you can help us to optimize the virus protection provided by AntiVir products.

Suspicious files

Viruses that may not yet be detected or removed by our products or suspect files can be sent to us. We provide you with several ways of doing this.

- Send the required file packed (WinZIP, PKZip, Arj etc.) in the attachment of an email to virus@avira.com. As some email gateways work with anti-virus software, you should also provide the file(s) with a password (please remember to tell us the password).
- You can also send us the suspicious file via our website.

False positive

If you believe that AntiVir is reporting a detection in a file that is most likely "clean", send the relevant file with information about the false positive in compressed form (WinZIP, PKZIP, Arj etc.) to virus@avira.com. As some email gateways work with anti-virus software, you should also provide the file(s) with a password (please remember to tell us the password).

10 Configuration options

10.1 Configuration options

Avira AntiVir Sharepoint is configured in AntiVir Administration under *Settings*. The following configuration options are available:

- **Configure AntiVir**: Options for heuristics, archive scanning and the logging function
- **Configure update**: Download method (via webserver or fileserver), configuration of connection to the download server, email notification function

10.2 Configure AntiVir

10.2.1 Configure AntiVir

Under **Configure AntiVir** you can configure the heuristic scan and the logging function of AntiVir SharePoint.

10.2.2 Scan

Under **Scan** you can activate options for heuristic purposes. Avira AntiVir SharePoint contains very powerful heuristics that can proactively uncover unknown malware, i.e. before a special virus signature to combat the damaging element has been created and before a virus guard update has been sent. Virus detection involves an extensive analysis and investigation of the affected codes for functions typical of malware. If the code being scanned exhibits these characteristic features, it is reported as being suspicious (heuristic hits). This does not necessarily mean that the code is in fact malware. False positives do sometimes occur. Heuristic hits are treated like viruses that have been detected from a known virus signature: The transfer of the affected files is stopped.

Macrovirus heuristics

Activate macrovirus heuristics

AntiVir contains a highly powerful macro virus heuristic. If this option is enabled, documents are scanned for unknown macroviruses. All macros are deleted in an affected document in the possible event of repairs.

Advanced Heuristic Analysis and Detection (AHeAD)

Advanced Heuristic Analysis and Detection (AHeAD)

If this option is enabled, the heuristic scan for viruses using AntiVir AHeAD technology is enabled. For heuristic hits, the affected data is treated as viruses. You can define how 'sharp' you want the heuristics to be. The option is enabled as the default setting.

Low detection level

If this option is enabled, AntiVir SharePoint detects slightly less unknown malware, the risk of false alerts is low in this case.

Medium detection level

This setting optimizes the ratio of detection performance to false positives: If the detection rate of unknown malware is relatively high, relatively few false positives are received. This option is enabled as the default setting and is recommended.

High detection level

If this option is enabled, AntiVir SharePoint identifies far more unknown malware, but you must also accept that there are likely to be false positives.

10.2.3 Archives

You can configure the scan in archives under **Archives**. Because archive scanning can require considerable computer capacity, you have the option of limiting scanning in archives or configuring the scanning pattern in archives.

Archive settings

Scan archives

If this option is enabled, then archives will be scanned. Archives will be unpacked and scanned. Archive scanning is enabled as the default setting and is recommended.

Smart extensions

If this option is enabled, the AntiVir SharePoint detects whether a file is a packed file format (archive), even if the file extension differs from the usual extensions, and scans the archive. Each file must be opened to check the file format. This slows down the scanning speed. This setting is activated by default and is recommended.

Exceptions

Under *Exceptions* you have the option of limiting the archive scan. The purpose of archive scan exceptions is to prevent possible system overloads due to archive bombs. The options for limiting the archive scan are automatically disabled as soon as you disable the option *Scan archives*.

Warning
You should limit the archive scan to a reasonable degree, taking the recommended standard values as your guide. Archives that are excluded from the scan for viruses and malware are transferred to Sharepoint team pages without being checked and are downloaded from there to the computer systems of the Sharepoint users. This is how malware can be spread through archives. If you restrict the scanning of archives, you should strongly recommend that SharePoint users check archives using a conventional anti-virus scanner before uploading them or after downloading them.

Maximum recursion depth

When scanning archives, the AntiVir SharePoint uses a recursive scan: Archives within archives are unpacked and scanned for viruses and unwanted programs. If this option is enabled, the recursive scan is restricted to the specified maximum recursion depth value. The option is disabled as the default setting. Archives that exceed the specified maximum value are not scanned for viruses or malware.

You can define the maximum recursion depth for the recursive scan. The recommended standard value is 20: An archive is unpacked up to 19 times and scanned for viruses and malware.

Maximum compression rate (ratio)

If this option is enabled, the archive scan is restricted to a maximum compression rate. The compression rate is defined as the ratio of the original file size to the compressed file size. Archives that exceed the specified maximum value are not scanned for viruses or malware. The option is disabled as the default setting. If this option is enabled, the recommended standard compression rate is 9

Maximum size of archives to be scanned

You can specify a maximum archive size in MB up to which the archives should be scanned. If this option is enabled, archives that exceed the specified maximum value are not scanned for viruses or malware. The option is disabled as the default setting. If this option is enabled, the recommended standard compression rate is 100 MB.

10.2.4 Report

Under Report you can enable or disable the AntiVir SharePoint logging function (logger) and define the scope of the logger. The log file avesvc.log is saved in the following directory:

C:\Documents and Settings\All Users\Application data\Avira\AntiVir SharePoint\logfiles

Note
The logger of the Update module is limited to 1500 log files and cannot be configured. If the maximum of 1500 log files is reached, each new update deletes the oldest log file.

Logging

Off

If this option is enabled, no AntiVir SharePoint actions are logged.

Default

If this option is enabled, only error messages from the AntiVir SharePoint are logged.

Extended

If this option is enabled, error messages and warning messages from the AntiVir SharePoint are logged.

Full

If this option is enabled, all messages and actions of the AntiVir SharePoint are logged.

The log function of AntiVir SharePoint is set to the **Standard** option as standard.

Limit report file

Limit size to n KB

If this option is enabled, the report file can be limited to a specific size. This option is activated by default with a value of 1024 KB. If the log file exceeds the specified size, the report file entries are backed up in a backup report file and the report file is reset. When the log entries are saved in the backup log file, the entries of the previous backup are overwritten.

10.2.5 Extended threat categories

Avira AntiVir SharePoint scans documents on the SharePoint team pages for viruses and malware. You have the option of incorporating other threat categories in the malware scan. The following threat categories (see Viruses and more::Extended threat categories) are defined:

- Adware/Spyware (ADSPY)
- Application (APPL)
- Adware (ADWARE)
- Backdoor Clients (BDC)
- Dialers (DIAL)
- Double Extension Files (HIDDENEXT)
- Phishing (PHISH)
- Security Privacy Risk (SPR)
- Games (GAME)
- Unusual Runtime Compression Tools (PCK)
- Jokes (JOKE)
- Possible Fake Software (PFS)

The following extended threat categories are enabled in the scan in the AntiVir SharePoint standard settings: Adware/Spyware (ADSPY), Adware (ADWARE), backdoor control software (BDC), Dialer (DIAL), double extension files (HIDDENEXT), Phishing (PHISH).

By configuring the threat categories you can activate more threat categories when scanning documents or exclude enabled threat categories from the scan as standard.

Warning
If any threat categories are disabled, files that are assigned to the threat category are not recorded as malware and are blocked. No entry is made in the report file (logger). It is recommended that none of the threat categories enabled by default should be excluded from the scan.

The threat categories must be configured in the *avwin.ini* configuration file. After a change to the *avwin.ini* file, the Avira AntiVir SharePoint Scan Service must be restarted. The configuration file can be found under:

C:\Documents and Settings\All Users\Application data\Avira\AntiVir SharePoint\config

Change the entry:

```
[COMMON]
PrefixDiff=+[category abbreviation], -[category abbreviation]
```

The plus sign enables additional threat categories , while the minus sign disables the threat categories activated by default. If you do not specify values for PrefixDiff, the standard settings will be loaded.

Examples:

```
[COMMON]
PrefixDiff=
```

The standard settings with the enabled threat categories DIAL, ADSPY, ADWARE, BDC, HIDDENEXT, PHISH are enabled.

[COMMON]
PrefixDiff= +APPL,+GAME,+JOKE,+PCK,+PFS,+SPR,-DIAL,-ADSPY,-ADWARE,-BDC,-HIDDENEXT,-PHISH

All standard threat categories are disabled: DIAL, ADSPY, ADWARE, BDC, HIDDENEXT, PHISH. All additional threat categories are enabled: APPL, GAME, JOKE, PCK, PFS, SPR.

10.3 Configure update

10.3.1 Configure update

Under **Configure Update** you can define the network settings and any proxy settings for updating AntiVir SharePoint. You can also configure an email notification via SMTP.

10.3.2 Network

Under **Network** you can configure the network settings for updating AntiVir SharePoint. You can get updates from the Internet or Intranet by means of a web server or file server / share (see section. Updates).

Network settings

Update URL

Enter the URL or IP address of the server from which you wish to download the updates. You can specify more than one Web server, separated by commas. AntiVir SharePoint uses the first available webserver for the update:

```
http://professional.avira-update.com/update,
http://professional.avira-update.net/update
```

If you wish to obtain the updates from a fileserver by means of a share directory, specify the UNC path for the share directory:

```
\\<Server name>|<IP address>\<Share name>\<Path>
```

Update interval in minutes

Enter an update interval in minutes. At the specified interval, AntiVir SharePoint checks whether there are updates for AntiVir SharePoint on the specified update server and starts the updating process as necessary. The standard setting of 120 minutes is recommended.

Network access

If you use a share directory on a file server for the update, enter a user name and a password.

Warning
The user name and password for network access are saved in encrypted form. To avoid security risks when accessing file servers, it is recommended that a user account with restricted user rights should be used. In order to execute the update, you only need reading permission for the file server.

User name

Enter a user name for authentication here.

Password

Enter a password name for authentication here.

10.3.3 Proxy

If you use a web server to update AntiVir SharePoint, you can specify a proxy server by means of which the connection to the webserver is to be created under **Proxy**.

Proxy server

Connect via proxy server

When this option is enabled, AntiVir SharePoint connects with the webserver via a proxy server which is used to update AntiVir SharePoint. This option is disabled as the default setting.

Address

Please enter the URL or the IP address of the proxy server that AntiVir SharePoint should use to connect to the webserver.

Port

Please enter the port number of the proxy server that AntiVir SharePoint should use to connect to the webserver.

User name

Enter your login name on the proxy server.

Password

Enter the relevant password for logging in on the proxy server here.

10.3.4 Email

You can specify email notification settings via SMTP under **Email**. You will be informed by email either every time an update is performed or just when an error occurs during an update. The email message contains the following information:

- The name of the computer running AntiVir SharePoint
- Date and time of the update

– Status of the update

Email messages

Enable email notifications

When this option is enabled, you will receive an email notification either every time an update is performed or just when an error occurs during an update. This option is disabled as the default setting.

Event selection

Select the event for which you require notification:

Notifications when an update has failed

An email will only be sent when an update fails.

Notify at every update

An email notification will be sent after every update in which new files were installed or when an error occurs during an update. No emails are sent of new files are not installed during an update because AntiVir SharePoint already has the latest files.

SMTP server

Enter the name of the SMTP server that you wish to use to send the notifications.

User name

Enter a user name for authentication on the SMTP server.

Password

Enter a password for authentication on the SMTP server.

Sender address

Specify a name or an email address as the sender of the email notification.

Recipient address

Enter the email address of the recipient of the email notification. You can also specify more than one recipient address, separated by commas.

Avira AntiVir SharePoint

Avira GmbH

Lindauer Str. 21
88069 Tettnang
Germany
Telephone: +49 (0) 7542-500 0
Fax: +49 (0) 7542-525 10
Internet: http://www.avira.com

Issued Q3-2009