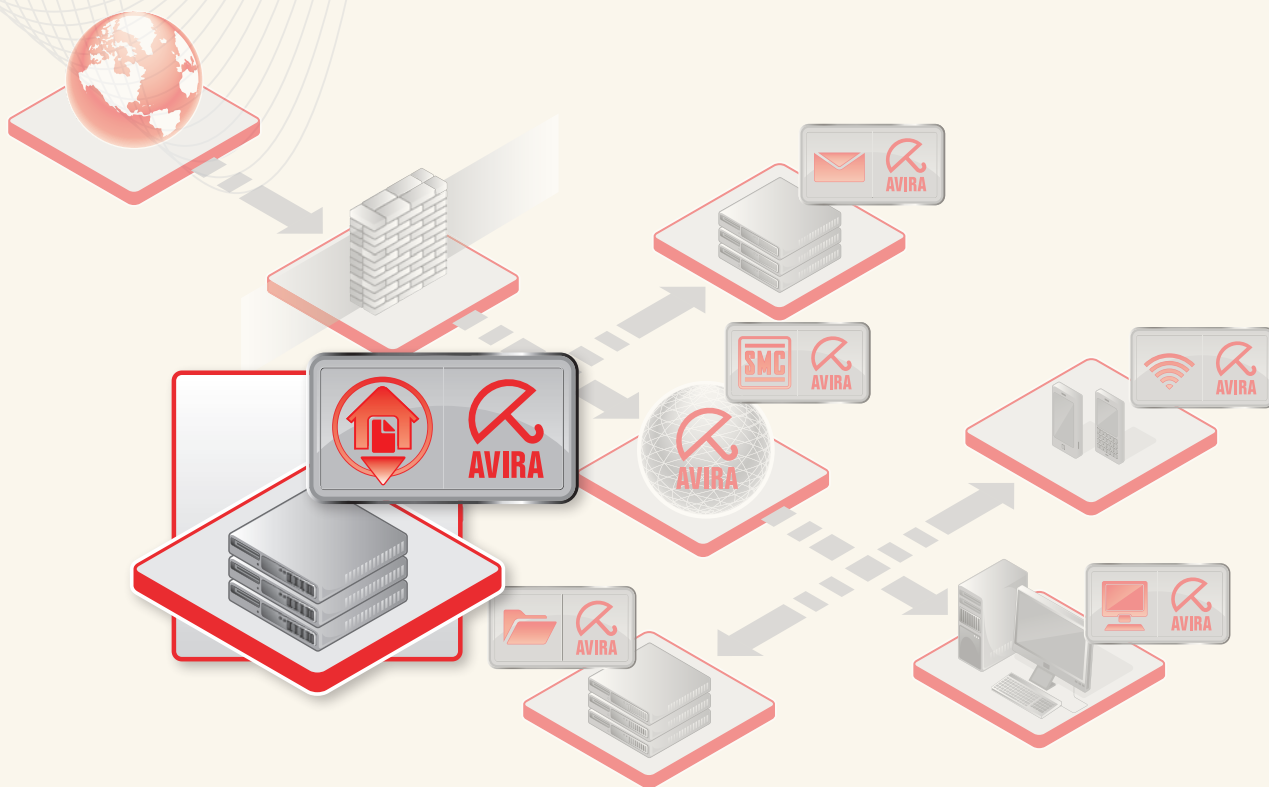


Handbuch für Anwender

# Avira AntiVir SharePoint



## Warenzeichen und Copyright

### Warenzeichen

AntiVir ist ein registriertes Warenzeichen der Avira GmbH.

Windows ist ein registriertes Warenzeichen der Microsoft Corporation in den Vereinigten Staaten und anderen Ländern.

Alle anderen Marken- und Produktnamen sind Warenzeichen oder eingetragene Warenzeichen ihrer entsprechenden Besitzer.

Geschützte Warenzeichen sind in diesem Handbuch nicht als solche gekennzeichnet. Dies bedeutet jedoch nicht, dass sie frei verwendet werden dürfen.

### Hinweise zum Copyright

Für Avira AntiVir SharePoint wurde Code von Drittanbietern verwendet. Wir bedanken uns bei den Copyright-Inhabern dafür, dass sie uns ihren Code zur Verfügung gestellt haben. Detaillierte Informationen zum Copyright finden Sie in der Hilfe von Avira AntiVir SharePoint unter Third Party Licenses.

# Inhaltsverzeichnis

<b>1</b>	<b>Einführung .....</b>	<b>1</b>
<b>2</b>	<b>Symbole und Hervorhebungen .....</b>	<b>2</b>
<b>3</b>	<b>Produktinformation .....</b>	<b>3</b>
	3.1 Funktionsübersicht .....	3
	3.2 Leistungsumfang .....	5
	3.3 Systemvoraussetzungen .....	5
	3.4 Lizenzierung .....	6
<b>4</b>	<b>Installation und Deinstallation .....</b>	<b>7</b>
	4.1 Installation .....	7
	4.2 Deinstallation .....	8
<b>5</b>	<b>Oberfläche und Bedienung .....</b>	<b>9</b>
<b>6</b>	<b>Virenfund .....</b>	<b>11</b>
<b>7</b>	<b>Updates .....</b>	<b>12</b>
<b>8</b>	<b>Viren und mehr .....</b>	<b>13</b>
	8.1 Erweiterte Gefahrenkategorien .....	13
	8.2 Viren sowie sonstige Malware .....	15
<b>9</b>	<b>Info und Service .....</b>	<b>20</b>
<b>10</b>	<b>Konfigurationsoptionen .....</b>	<b>21</b>
	10.1 Konfigurationsoptionen .....	21
	10.2 AntiVir konfigurieren .....	21
	10.2.1 AntiVir konfigurieren .....	21
	10.2.2 Suche .....	21
	10.2.3 Archive .....	22
	10.2.4 Report .....	23
	10.2.5 Erweiterte Gefahrenkategorien .....	24
	10.3 Update konfigurieren .....	25
	10.3.1 Update konfigurieren .....	25
	10.3.2 Netzwerk .....	26
	10.3.3 Proxy .....	26
	10.3.4 Email .....	27

# 1 Einführung

Avira AntiVir SharePoint schützt SharePoint Systeme vor Viren, Malware, Ad- und Spyware, unerwünschten Programmen und sonstigen Gefahren. Verkürzend wird in diesem Handbuch von Viren und Malware gesprochen.

---

**Hinweis**

Der vollständige Name des Programms lautet Avira AntiVir SharePoint. Zur besseren Lesbarkeit wird dieser Name auf AntiVir SharePoint verkürzt.

Auf unserer Webseite <http://www.avira.de> können Sie das Handbuch zu AntiVir SharePoint als PDF herunterladen, Avira AntiVir SharePoint aktualisieren oder Ihre Lizenz erneuern.

Zudem finden Sie auf unserer Webseite Informationen wie beispielsweise die Telefonnummer des technischen Supports sowie unseren Newsletter, den Sie dort abonnieren können.

## 2 Symbole und Hervorhebungen

Folgende Symbole werden verwendet:

<b>Symbol</b>	<b>Erläuterung</b>
✓	Steht vor einer Voraussetzung, die vor dem Ausführen einer Handlung erfüllt sein muss.
▶	Steht vor einem Handlungsschritt, den Sie ausführen.
→	Steht vor einem Ergebnis, das aus der vorangehenden Handlung folgt.
<b>Hinweis</b>	Steht vor einem Hinweis mit besonders wichtigen Informationen oder vor einem Tipp, der das Verständnis und die Nutzung von AntiVir for Sharepoint erleichtert.
<b>Warnung</b>	Steht vor einem Warnhinweis. Beachten Sie Warnhinweise, um die Virenschutzfunktion von Antivir for SharePoint voll zu gewährleisten.

Folgende Hervorhebungen werden verwendet:

<b>Hervorhebung</b>	<b>Erläuterung</b>
<i>Kursiv</i>	Dateiname oder Pfadangabe. Elemente der Software-Oberfläche, die angezeigt werden (z.B. Fenstertitel, Fensterbereich oder Optionsfeld).
<b>Fett</b>	Elemente der Software-Oberfläche, die angeklickt werden (z.B. Menüpunkt, Registerkarte oder Schaltfläche).

# 3 Produktinformation

## 3.1 Funktionsübersicht

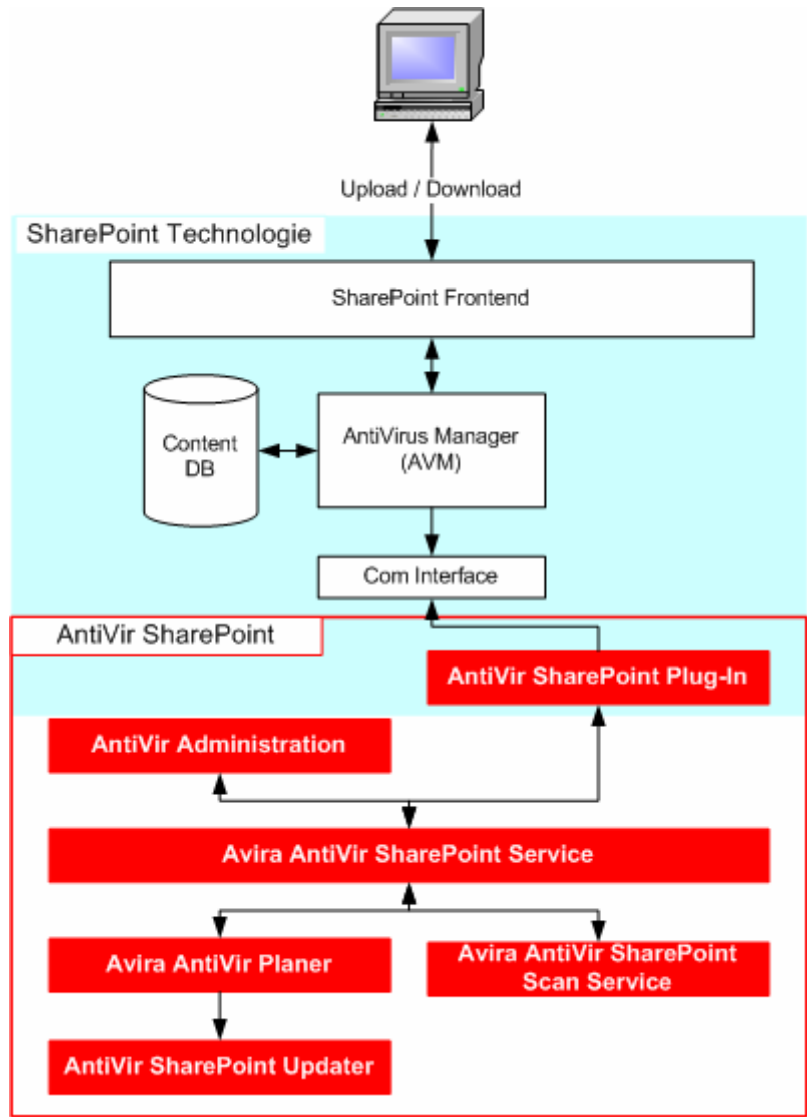
AntiVir SharePoint ist eine speziell für Microsoft SharePoint entwickelte Antivirenlösung und unterstützt die folgenden SharePoint- Technologien:

- 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-Technologien stellen Dokumente eines Unternehmens für Benutzer an zentraler Stelle zur Verfügung und verwalten diese mit einer Versionskontrolle. Der Zugriff auf Dokumente erfolgt über eine Weboberfläche - den SharePoint Teamseiten - per Up- und Download. Die Dokumente bzw. Dateien sind zentral in einer MS SQL-Datenbank gespeichert. Dies stellt für die Sicherheit ein ernst zu nehmendes Problem dar, da die Daten nicht mit einer herkömmlichen Antivirenlösung wie einem On-Demand oder einem On-Access Virens Scanner vor Virenbefall geschützt werden können: On-Demand und On-Access Virens Scanner erfordern ein Vorliegen der zu durchsuchenden Daten als Dateien im Dateisystem.

AntiVir SharePoint durchsucht je nach Konfiguration bei jedem Upload und Download zu und von den SharePoint Teamseiten Dokumente nach Viren und Malware. Bei einem Virenfund wird der Transfer unterbunden, falls eine Reparatur des Dokuments nicht möglich ist.

**Architektur:**



In den SharePoint-Technologien wird der Einsatz von externen Antivirenprogrammen über den Antivirus Manager (AVM) gesteuert. Virenschutzfunktionen können in den SharePoint Antivireneinstellungen aktiviert werden. Sind die Virenschutzfunktionen aktiviert, übergibt AVM die von Benutzern zum Upload übergebenen oder zum Download angeforderten Daten einem externen Antivirenprogramm.

AntiVir ist über ein Plug-In in die Sharepoint-Technologien integriert. Das AntiVir SharePoint-Plug-In bearbeitet Anfragen zur Suche nach Viren von SharePoint und leitet diese an den Dienst Avira AntiVir SharePoint Service weiter. Avira AntiVir SharePoint Service gibt Anfragen zur Suche an den Dienst Avira AntiVir SharePoint Scan Service weiter und verarbeitet die Einstellungen der AntiVir Administration. Der Dienst Avira AntiVir Planer startet zur Ausführung von regelmäßigen Updates die Update-Komponente. Die AntiVir Administration ist ein Snap-In der Microsoft Management Konsole (MMC). Die Suche nach Viren und Malware wird vom Avira AntiVir SharePoint Scan Service ausgeführt.

## 3.2 Leistungsumfang

AntiVir SharePoint bietet einen umfassenden Antivirenschutz für Unternehmensdaten, die Sie mit SharePoint-Technologien verwalten und zur Verfügung stellen. So schützen Sie auch die für SharePoint eingesetzten Computersysteme. AntiVir SharePoint ist einfach zu installieren und verfügt über folgende Konfigurationsmöglichkeiten:

### **Einstellungen zur Suche nach Viren und Malware:**

- OLE Heuristik und Win32 Dateiheuristik
- Archivsuche

### **Einstellungen zum automatischen Update (Aktualisierung der Suchengine und der Virendefinitionsdatei):**

- Update von Webserver oder Fileserver möglich
- Update über Proxyserver möglich
- Email-Benachrichtigungsfunktion

## 3.3 Systemvoraussetzungen

Avira AntiVir SharePoint unterstützt die SharePoint-Technologien:

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

Es bestehen die folgenden Systemvoraussetzungen und Anforderungen:

- Lauffähige SharePoint-Technologie: SharePoint Server 2007 oder SharePoint Services 3.0 oder SharePoint Portal Server 2003 oder Windows SharePoint Services 2.0
- Servercomputer mit Prozessorgeschwindigkeit 2,5 GHz (Gigahertz) oder höher, 32 oder 64 Bit Prozessor
- Mindestens 1 GB Arbeitsspeicher, 2 GB empfohlen
- 130 MB freier Speicherplatz auf der Festplatte
- Mindestens 100 MB temporärer Speicherplatz auf der Festplatte

## 3.4 Lizenzierung

Um Avira AntiVir SharePoint zu nutzen, benötigen Sie eine Lizenz. Die Lizenz liegt in Form eines digitalen Lizenzschlüssels, der Datei hbedv.key, vor. Die Lizenzdatei erhalten Sie von der Avira GmbH per Email. Die Lizenzdatei enthält die Lizenz für alle Produkte, die Sie bei einem Bestellvorgang bestellt haben.

Mit der Lizenzdatei hbedv.key aktivieren Sie Ihre Lizenz für Avira AntiVir SharePoint. Während der Installation werden Sie aufgefordert, diese Lizenzdatei zu laden. Um Ihre Lizenz zu verlängern oder die Lizenz nach der Installation zu laden, legen Sie die Lizenzdatei im Installationsverzeichnis ab.

## 4 Installation und Deinstallation

### 4.1 Installation

Vor der Installation von AntiVir SharePoint prüfen Sie folgende Voraussetzungen:

- ✓ Stellen Sie sicher, dass die Systemvoraussetzungen erfüllt sind (siehe Systemvoraussetzungen).
- ✓ Stellen Sie sicher, dass Sie am Rechner als Administrator oder als Benutzer mit Administrator-Rechten angemeldet sind.
- ✓ Stellen Sie sicher, dass zur Aktualisierung von AntiVir SharePoint eine Internetverbindung oder eine Netzwerkverbindung zu einem Downloadserver vorhanden ist. Wenn Sie einen Fileserver nutzen, benötigen Sie ggf. einen Benutzernamen und ein Kennwort für das Server-Login.
- ✓ Stellen Sie sicher, dass eine gültige Lizenzdatei hbedv.key vorhanden und in einem lokalen Verzeichnis auf dem Server gespeichert ist.

#### Installationsarten

##### Vollständig

Es kann kein Zielordner für die zu installierenden Programmdateien gewählt werden.

##### Benutzerdefiniert

Es kann ein Zielordner für die zu installierenden Programmdateien gewählt werden.

#### Installation ausführen

So installieren Sie Avira AntiVir SharePoint:

- ▶ Starten Sie das Installationsprogramm mit einem Doppelklick auf die Installationsdatei, die Sie aus dem Internet heruntergeladen haben, oder legen Sie die Programm-CD ein.
- Nach einer Sicherheitsmeldung, die den Herausgeber der Software bestätigt, wird die Installationsdatei dekomprimiert.
- ▶ Klicken Sie auf **Weiter**.
- Das Setup-Programm wird gestartet, es erscheint eine Meldung, mit der Sie das Anhalten des WWW-Publishingdienstes bestätigen. Zur Installation von AntiVir SharePoint ist das Stoppen des WWW-Publishingdienstes erforderlich. Während des Setups sind die Webseiten, die auf diesem Server gehostet werden, nicht erreichbar.
- ▶ Bestätigen Sie das Anhalten des WWW-Publishingdienstes mit **Ja**.
- Der Installationsassistent von Avira AntiVir SharePoint öffnet sich. Folgen Sie den Anweisungen des Installationsassistenten. Folgende Installationsschritte werden ausgeführt:
  - ▶ Ggf. Installation des Microsoft Visual C++ 2008 - Redistributable Kit, wenn das Kit nicht bereits installiert wurde.

### Hinweis

Avira AntiVir SharePoint verwendet Runtime Libraries des Microsoft Visual C++ 2008 - Redistributable Kit. Zur Nutzung von AntiVir SharePoint ist daher eine Installation von Microsoft Visual C++ 2008 - Redistributable Kit zwingend erforderlich.

- ▶ Bestätigung der Lizenzvereinbarungen
- ▶ Auswahl des Setup-Typs (Vollständige Installation oder benutzerdefinierte Installation)
- ▶ Lizenzierung von AntiVir Server: Laden der Lizenzdatei oder Auswahl der 30-Tage-Evaluationslizenz
- ▶ Installation der Komponenten von Avira AntiVir SharePoint.

Nach der Installation ist die Antivirenfunktion des SharePoint AntiVirus Managers aktiviert, AntiVir SharePoint ist mit Standardeinstellungen konfiguriert.

### Update

Nach der Installation sollte AntiVir SharePoint aktualisiert werden: Gewährleisten Sie, dass AntiVir SharePoint Daten aus dem Internet empfangen kann. Es kann in der Konfiguration von AntiVir SharePoint ein Proxyserver angegeben werden, über den AntiVir SharePoint Updates bezieht:

Geben Sie unter Einstellungen :: Update konfigurieren:: Proxy einen Proxyserver für die Ausführung von Updates an.

### Hinweis

Sie können Einstellungen im SharePoint AntiVirus Manager in der SharePoint Zentraladministration ändern unter **SharePoint Zentraladministration :: Sicherheitskonfiguration :: Antiviruseinstellungen konfigurieren**.

### Warnung

Beachten Sie bei Einstellungen in der SharePoint Zentraladministration: Der Antivirenschutz beim Upload und Download von Dokumenten muss aktiviert sein, damit Avira AntiVir SharePoint Dokumente prüft, die zu SharePoint Teamseiten hochgeladen oder von SharePoint Teamseiten heruntergeladen werden.

### Hinweis

In der AntiVir Administration können Sie die Standardeinstellungen von AntiVir SharePoint ändern sowie weitere Einstellungen vornehmen: Konfiguration des Updates über einen Proxy- oder Fileserver, Konfiguration der Email-Benachrichtigungsfunktion.

## 4.2 Deinstallation

Die Deinstallation führen Sie über die Systemsteuerung des Betriebssystems durch:

- Unter **Systemsteuerung :: Software** suchen Sie nach Avira AntiVir SharePoint und klicken auf die Option **Entfernen**.
- Bestätigen Sie die Deinstallation.

Bei der Deinstallation werden die AntiVir-Dienste gestoppt, alle Programm- und Reportdateien werden gelöscht.

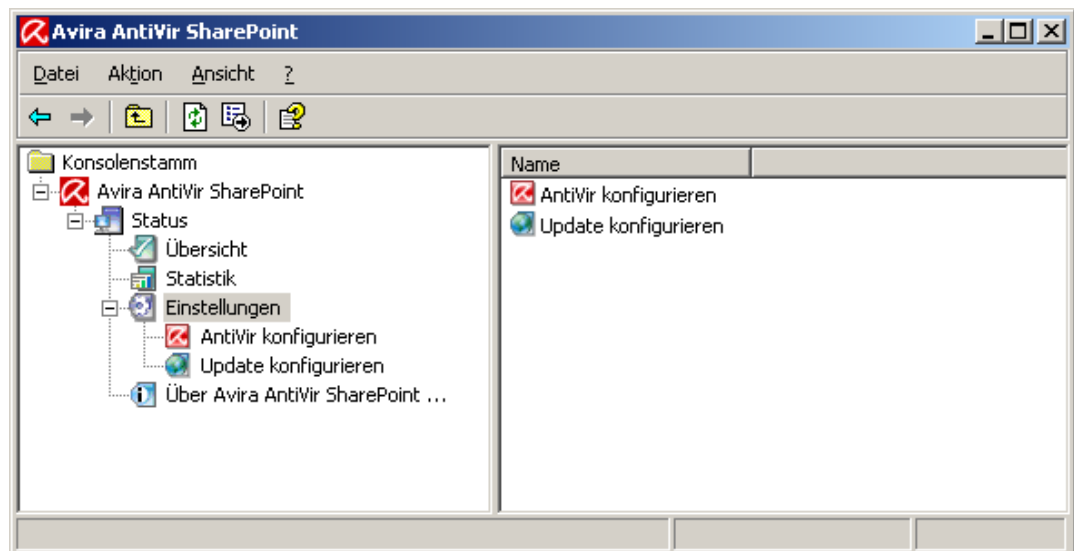
## 5 Oberfläche und Bedienung

Die Virenschutzfunktion von Avira AntiVir SharePoint kann über den SharePoint AntiVirus Manager gesteuert, d.h. aktiviert oder deaktiviert werden. Sie finden die Einstellungen des SharePoint AntiVirus Manager in der SharePoint Zentraladministration unter **Sicherheitskonfiguration :: Antiviruseinstellungen konfigurieren**. Nach der Installation ist die Antivirenfunktion standardmäßig aktiviert.

### Warnung

Beachten Sie bei Einstellungen in der SharePoint Zentraladministration: Der Antivirenschutz beim Upload und Download von Dokumenten muss aktiviert sein, damit Avira AntiVir SharePoint Dokumente prüft, die zu SharePoint Teamseiten hochgeladen oder von SharePoint Teamseiten heruntergeladen werden.

Die Konfiguration von AntiVir SharePoint erfolgt über die AntiVir Administration. Die AntiVir Administration ist ein Snap-In der Microsoft Management Konsole (MMC).



### Hinweis

Beachten Sie, dass in dieser Hilfe nur die proprietären Elemente der AntiVir Administration dokumentiert sind. Informationen zur MMC und zur manuellen Einbindung eines Snap-In entnehmen Sie dem Benutzerhandbuch oder der Online-Hilfe des Betriebssystems.

### Starten und Beenden der AntiVir Administration

Sie starten die AntiVir Administration über die Verknüpfung unter Programme::Avira::AntiVir SharePoint::Avira AntiVir SharePoint Benutzeroberfläche. Sie können die AntiVir Administration auch direkt in der MMC laden. Sie finden die AntiVir Konsolendatei im Installationsverzeichnis von AntiVir SharePoint. Um die AntiVir Administration zu beenden, müssen Sie MMC schließen.

### Bedienung

- Navigieren Sie über die Konsolenstruktur im linken Fenster der MMC. Navigationselemente werden auch als Objekte im rechten Detailfenster der MMC angezeigt. Sie öffnen diese Objekte im Detailfenster mit Doppelklick. Die AntiVir SharePoint Konfiguration befindet sich unter dem Knoten **Einstellungen**. Sie können im Detailfenster verschiedene Konfigurationsrubriken anwählen: Es öffnet sich das Fenster *AntiVir konfigurieren*, in dem Sie die angewählte Rubrik konfigurieren können.
- Befehle und Aktionen sind über Links im Detailfenster verfügbar.
- Bei der Konfiguration von AntiVir SharePoint müssen Sie Ihre Angaben im Fenster *AntiVir konfigurieren* mit der Schaltfläche **OK** bestätigen, um die neuen Einstellungen zu übernehmen. Mit der Schaltfläche **Abbrechen** werden Ihre Angaben verworfen.

### Produktversion von AntiVir SharePoint abrufen

Die Produktversion von AntiVir SharePoint können Sie im Hilfemenü der MMC unter **Info über Avira AntiVir SharePoint...** abrufen.

### Hilfe aufrufen

Sie können die Hilfe über das Hilfe-Icon in der MMC oder mit F1 aufrufen.

### AntiVir Administration im Überblick

#### Avira AntiVir SharePoint

##### Status

- Anzeige des Verbindungsstatus der AntiVir Administration zu den AntiVir SharePoint Diensten
- Aktionen: **Server verbinden** bei getrennter Verbindung zu den AntiVir SharePoint Diensten

##### Übersicht

- Anzeige des Status der AntiVir SharePoint Dienste: AntiVir SharePoint Service und AntiVir SharePoint Scan Service
- Anzeige des Systemstatus: Letztes Update, VDF- und Engine-Version
- Aktionen: Update (VDF/Engine) starten

##### Statistik

- Anzeige der statistischen Daten der Virensuche
- Aktionen: Statistik zurücksetzen

##### Einstellungen

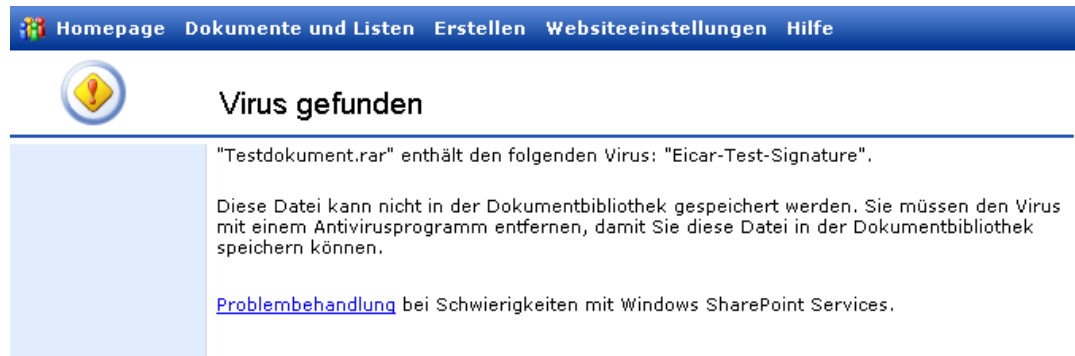
- **AntiVir konfigurieren**: Optionen zur Heuristik und zur Archivsuche
- **Update konfigurieren**: Downloadmethode (via Webserver oder Fileserver), Konfiguration der Verbindung zum Downloadserver, Email-Benachrichtigungsfunktion

##### Über Avira AntiVir SharePoint...

- Anzeige von Kontakt- und Supportinformationen

## 6 Virenfund

Beim Upload oder Download von Dokumenten zu bzw. von SharePoint Teamseiten durchsucht AntiVir SharePoint diese Dokumente nach Viren und Malware. Wenn AntiVir in einem Dokument Viren oder Malware findet, wird dies SharePoint gemeldet. Der Transfer des Dokuments wird von SharePoint unterbunden. Der Nutzer der SharePoint Teamseite erhält eine Meldung:



The screenshot shows a SharePoint navigation bar with links: Homepage, Dokumente und Listen, Erstellen, Websiteeinstellungen, and Hilfe. Below the bar is a warning icon (a yellow triangle with an exclamation mark) and the heading "Virus gefunden". The main content area contains the following text:

"Testdokument.rar" enthält den folgenden Virus: "Eicar-Test-Signature".

Diese Datei kann nicht in der Dokumentbibliothek gespeichert werden. Sie müssen den Virus mit einem Antivirusprogramm entfernen, damit Sie diese Datei in der Dokumentbibliothek speichern können.

[Problembehandlung](#) bei Schwierigkeiten mit Windows SharePoint Services.

### Hinweis

In der SharePoint Zentraladministration unter **Sicherheitskonfiguration :: Antiviruseinstellungen konfigurieren** können Sie das Verhalten beim Virenfund spezifizieren. So können Sie z.B. den Download infizierter Dateien zulassen, um den Nutzern die Möglichkeit zu geben, infizierte Dokumente auf dem eigenen Computersystem auf Viren und Malware zu prüfen.

### Warnung

Beachten Sie bei Einstellungen in der SharePoint Zentraladministration: Der Antivirenschutz beim Upload und Download von Dokumenten muss aktiviert sein, damit Avira AntiVir SharePoint Dokumente prüft, die zu SharePoint Teamseiten hochgeladen oder von SharePoint Teamseiten heruntergeladen werden.

## 7 Updates

Die Wirksamkeit einer Antivirensoftware steht und fällt mit der Aktualität der Suchengine und der Virendefinitionen. Laden Sie deshalb regelmäßig Updates für Avira AntiVir SharePoint von unseren Downloadservern herunter. Zur Ausführung von regelmäßigen Updates ist die Komponente AntiVir SharePoint Updater in AntiVir SharePoint integriert. Die Komponente aktualisiert die folgenden Programmkomponenten:

- Virendefinitionsdatei
- Suchengine

In der AntiVir Administration unter *Update konfigurieren* richten Sie Update-Aufträge ein, die in den angegebenen Intervallen vom Dienst Avira AntiVir Planer gestartet und von der Update-Komponente ausgeführt werden. Bei jedem Update-Auftrag werden die Virendefinitionsdatei und die Suchengine auf Aktualität geprüft und ggf. aktualisiert. In der AntiVir Administration unter **Übersicht :: Letztes Update** können Sie ein Update manuell anstoßen. Nach einem Update muss AntiVir SharePoint nicht neu gestartet werden.

Sie können Updates über folgende Server beziehen:

- direkt aus dem Internet über einen Webserver der Avira GmbH. Folgende Update-Webserver sind verfügbar:  
<http://professional.avira-update.com/update>  
<http://professional.avira-update.net/update>  
<http://62.146.210.32/update>
- über einen Web- oder Fileserver im Intranet, der die Update-Dateien aus dem Internet herunterlädt und sie anderen Rechnern im Netz zur Verfügung stellt. Dies ist sinnvoll, wenn Sie AntiVir SharePoint auf mehreren Computern in einem Netzwerk aktualisieren wollen. So kann die Aktualität von AntiVir SharePoint auf den zu schützenden Computersystemen ressourcenschonend gewährleistet werden.

Bei der Nutzung eines Webservers erfolgt der Download per HTTP-Protokoll. Bei der Nutzung eines File-Servers erfolgt ein Zugriff auf die Update-Dateien über das Netzwerk. Sie konfigurieren das Update auf der AntiVir Administration unter der Update-Konfiguration.

### **Hinweis**

Als Web- oder Fileserver im Intranet können Sie AntiVir Internet Update Manager (File- oder Webserver unter Windows) nutzen. Das Programm spiegelt Downloadserver von AntiVir Produkten (u.a. AntiVir SharePoint) und ist im Internet auf <http://www.avira.com> beziehbar.

## 8 Viren und mehr

### 8.1 Erweiterte Gefahrenkategorien

#### **Kostenverursachende Einwahlprogramme (DIALER)**

Bestimmte im Internet angebotene Dienstleistungen sind kostenpflichtig. Die Abrechnung erfolgt in Deutschland über Einwahlprogramme mit 0190/0900-Nummern (in Österreich und der Schweiz über 09x0-Nummern; in Deutschland wird mittelfristig auf 09x0 umgestellt). Auf dem Rechner installiert, gewährleisten diese Programme - kurz Dialer genannt - den Verbindungsaufbau über eine entsprechende Premium-Rate-Nummer, deren Tarifgestaltung ein breites Spektrum umfassen kann.

Die Vermarktung von Online-Inhalten über den Weg der Telefonrechnung ist legal und kann für den Nutzer vorteilhaft sein. Seriöse Dialer lassen deshalb keinen Zweifel daran aufkommen, dass sie vom Kunden bewusst und mit Bedacht eingesetzt werden. Sie installieren sich nur dann auf dem Anwender-Rechner, wenn der Nutzer dazu seine Zustimmung abgibt, wobei diese Zustimmung aufgrund einer völlig eindeutigen und klar erkennbaren Etikettierung bzw. Aufforderung erfolgt sein muss. Der Verbindungsaufbau seriöser Dialer-Programme wird unmissverständlich angezeigt. Außerdem informieren seriöse Dialer exakt und augenfällig über die Höhe der dabei entstehenden Kosten.

Leider jedoch gibt es Dialer, die sich unauffällig, auf fragwürdige Weise oder gar in betrügerischer Absicht auf Rechnern installieren. Sie ersetzen z.B. die Standard-DFÜ-Verbindung des Internet-Nutzers zum ISP (Internet-Service-Provider) und rufen bei jeder Verbindung eine kostenverursachende, oft horrend überteuerte 0190/0900-Nummer an. Der betroffene Anwender merkt mitunter erst mit der nächsten Telefonrechnung, dass ein unerwünschtes 0190/0900-Dialer-Programm auf seinem Rechner bei jedem Verbindungsaufbau zum Internet eine Premium-Rate-Nummer gewählt hat - mit der Folge drastisch hoher Gebühren.

Um sich generell vor unerwünschten kostenverursachenden Einwahlprogrammen (0190/0900-Dialern) zu schützen, empfehlen wir Ihnen, sich direkt bei Ihrem Telefon-Anbieter für diesen Nummernkreis sperren zu lassen.

#### **Spiele (GAMES)**

Computerspiele müssen sein - aber sie gehören nicht unbedingt an den Arbeitsplatz (die Mittagspause vielleicht einmal ausgenommen). Dennoch wird von Mitarbeitern in Unternehmen und Behörden so manches Moorhuhn erlegt und so mancher Karobube doppelgeklickt. Über das Internet kann eine Fülle von Spielen heruntergeladen werden. Auch Email-Games erfreuen sich wachsender Verbreitung: Vom simplen Schach bis zum "Flottenmanöver" (inklusive Torpedogefecht) sind zahlreiche Varianten in Umlauf: Die jeweiligen Spielzüge werden über Mailprogramme an Partner gesendet und von diesen beantwortet.

Untersuchungen haben ergeben, dass die zum Computerspielen verwendete Arbeitszeit längst wirtschaftlich relevante Größenordnungen erreicht hat. Umso verständlicher ist, dass immer mehr Unternehmen Möglichkeiten in Betracht ziehen, Computerspiele von Arbeitsplatzrechnern fern zu halten.

### Witzprogramme (JOKES)

Die Witzprogramme sollen lediglich jemanden erschrecken oder zur allgemeinen Belustigung dienen, ohne schädlich zu sein oder sich selbst zu vermehren. Meist fängt der Computer nach dem Aufruf eines Witzprogramms irgendwann an, eine Melodie zu spielen oder etwas Ungewohntes auf dem Bildschirm zu zeigen. Beispiele für Witzprogramme sind die Waschmaschine im Diskettenlaufwerk (DRAIN.COM) und der Bildschirmfresser (BUGSRES.COM).

Aber Vorsicht! Alle Symptome von Witzprogrammen könnten auch von einem Virus oder einem Trojaner stammen. Zumindest bekommt man aber einen gehörigen Schreck oder richtet in Panik hinterher sogar selbst tatsächlichen Schaden an.

### Security Privacy Risk (SPR)

Software, die die Sicherheit Ihres Systems beeinträchtigen, nicht gewünschte Programmaktivitäten auslösen, Ihre Privatsphäre verletzen oder Ihr Benutzerverhalten ausspähen kann und daher möglicherweise unerwünscht ist.

### Backdoor-Steuersoftware (BDC)

Um Daten zu stehlen oder Rechner zu manipulieren, wird "durch die Hintertür" ein Backdoor-Server-Programm eingeschleust, ohne dass der Anwender es merkt. Über Internet oder Netzwerk kann dieses Programm über eine Backdoor Steuersoftware (Client) von Dritten gesteuert werden.

### Adware/Spyware (ADSPY)

Software, die Werbung einblendet oder Software, die persönliche Daten des Anwenders häufig ohne dessen Wissen oder Zustimmung an Dritte versendet und daher möglicherweise unerwünscht ist.

### Ungewöhnliche Laufzeitpacker (PCK)

Dateien, die mit einem ungewöhnlichen Laufzeitpacker komprimiert wurden und daher als möglicherweise verdächtig eingestuft werden können.

### Dateien mit verschleierte Dateieindungen (HEUR-DBLEXT)

Ausführbare Dateien, die ihre wahre Dateieindung in verdächtiger Weise verschleiern. Diese Methode der Verschleierung wird häufig von Malware benutzt.

### Phishing

Phishing, auch bekannt als *brand spoofing* ist eine raffinierte Form des Datendiebstahls, der auf Kunden bzw. potenzielle Kunden von Internet Service Providern, Banken, Online-Banking Diensten, Registrierungsbehörden abzielt.

Durch eine Weitergabe der eigenen Email-Adresse im Internet, das Ausfüllen von Online-Formularen, dem Beitritt von Newsgroups oder Webseiten ist es möglich, dass Ihre Daten von sog. "Internet crawling spiders" gestohlen und ohne Ihre Erlaubnis dazu verwendet werden einen Betrug oder andere Verbrechen zu begehen.

### **Anwendung (APPL)**

Bei der Bezeichnung APPL handelt es sich um eine Applikation, deren Nutzung mit einem Risiko verbunden sein kann oder die von fragwürdiger Herkunft ist.

### **Possible Fake Software (PFS)**

Bei der Bezeichnung PFS ("Possible Fake Software") handelt es sich um Software, die in der Regel kostenpflichtig ist, aber keine Funktionalität beinhaltet oder die fragwürdige Komponenten installiert.

### **Adware (ADWARE)**

Diese Software oder von ihr installierte Komponenten zeigen auf Ihrem System Werbung an.

## 8.2 Viren sowie sonstige Malware

### **Adware**

Als Adware wird Software bezeichnet, die dem Benutzer zusätzlich zur eigentlichen Funktionalität Werbe-Banner oder Werbe-Popups zeigt. Diese Werbeeinblendungen lassen sich in der Regel nicht abschalten und sind meist immer sichtbar. Hier erlauben die Verbindungsdaten bereits vielfältige Rückschlüsse auf das Nutzungsverhalten und sind aus Datenschutzgründen problematisch.

### **Backdoors**

Einem Backdoor (deutsch: Hintertür) ist es möglich, unter Umgehung der Zugriffssicherung, Zugriff auf einen Computer zu erlangen.

Ein versteckt laufendes Programm ermöglicht einem Angreifer meist fast uneingeschränkte Rechte. Mit Hilfe des Backdoors können persönliche Daten des Anwenders ausspioniert werden. Aber Sie werden meist dazu benutzt, weitere Computerviren oder Würmer auf dem betroffenen System zu installieren.

### **Bootviren**

Der Boot- bzw. Masterbootsektor von Festplatten wird mit Vorliebe von Bootsektorviren infiziert. Sie überschreiben wichtige Informationen zum Systemstart. Eine der unangenehmen Folgen: das Betriebssystem kann nicht mehr geladen werden...

### **Bot-Net**

Unter einem Bot-Net versteht man ein fernsteuerbares Netzwerk (im Internet) von PCs, welches aus untereinander kommunizierenden Bots besteht. Diese Kontrolle wird durch Viren bzw. Trojaner erreicht, die den Computer infizieren und dann auf Anweisungen warten, ohne auf dem infizierten Rechner Schaden anzurichten. Diese Netzwerke können für Spam-Verbreitung, DDoS Attacken, usw. verwendet werden, z.T. ohne dass die betroffenen PC-Nutzer etwas merken. Das Hauptpotenzial von Bot-Nets besteht darin, dass die Netzwerke Größen von tausenden Rechnern erreichen können, deren Bandbreitensumme die der meisten herkömmlichen Internetzugänge sprengt.

### **Exploit**

Ein Exploit (Sicherheitslücke) ist ein Computerprogramm oder Script, welches spezifische Schwächen oder Fehlfunktionen eines Betriebssystems oder Programms ausnutzt. Eine Form des Exploits sind Angriffe aus dem Internet mit Hilfe von manipulierten Datenpaketen, die Schwachstellen in der Netzwerksoftware ausnutzen. Hier können Programme eingeschleust werden, mit denen ein größerer Zugriff erlangt werden kann.

### **Hoaxes (engl.: hoax - Scherz, Schabernack, Ulk)**

Seit ein paar Jahren erhalten die User im Internet und in anderen Netzen Warnungen vor Viren, die sich angeblich per Email verbreiten sollen. Diese Warnungen werden über Email mit der Aufforderung verbreitet, sie an möglichst viele Kollegen und andere Benutzer weiter zu senden, um alle vor der "Gefahr" zu warnen.

### **Honeypot**

Ein Honeypot (Honigtopf) ist ein in einem Netzwerk installierter Dienst (Programm oder Server). Dieser hat die Aufgabe, ein Netzwerk zu überwachen und Angriffe zu protokollieren. Dieser Dienst ist dem legitimen Nutzer unbekannt und wird daher niemals angesprochen. Wenn nun ein Angreifer ein Netzwerk auf Schwachstellen untersucht und dabei die von einem Honeypot angebotenen Dienste in Anspruch nimmt, wird er protokolliert und ein Alarm ausgelöst.

### **Makroviren**

Makroviren sind kleine Programme, die in der Makrosprache einer Anwendung (z.B. WordBasic unter WinWord 6.0) geschrieben sind und sich normalerweise auch nur innerhalb von Dokumenten dieser Anwendung verbreiten können. Sie werden deshalb auch Dokumentviren genannt. Damit sie aktiv werden, sind sie immer darauf angewiesen, dass die entsprechende Applikation gestartet und eines der infizierten Makros ausgeführt wird. Im Unterschied zu "normalen" Viren befallen Makroviren also keine ausführbaren Dateien sondern die Dokumente der jeweiligen Wirts-Applikation.

### **Pharming**

Pharming ist eine Manipulation der Hostdatei von Webbrowsern, um Anfragen auf gefälschte Webseiten umzuleiten. Es handelt sich um eine Weiterentwicklung des klassischen Phishings. Pharming-Betrüger unterhalten eigene große Server-Farmen, auf denen gefälschte Webseiten abgelegt sind. Pharming hat sich auch als Oberbegriff für verschiedene Arten von DNS-Angriffen etabliert. Bei einer Manipulation der Host-Datei wird unter Zuhilfenahme eines Trojaners oder eines Virus eine gezielte Manipulation des Systems vorgenommen. Die Folge davon ist, dass von diesem System nur noch gefälschte Websites abrufbar sind, selbst wenn die Web-Adresse korrekt eingegeben wurde.

### Phishing

Phishing bedeutet ins Deutsche übersetzt das Fischen nach persönlichen Daten des Internetnutzers. Der Phisher schickt seinem Opfer in der Regel offiziell wirkende Schreiben, wie beispielsweise Emails, die es verleiten sollen, vertrauliche Informationen, vor allem Benutzernamen und Passwörter oder PIN und TAN von Online-Banking-Zugängen, im guten Glauben dem Täter preiszugeben. Mit den gestohlenen Zugangsdaten kann der Phisher die Identität seines Opfers übernehmen und in dessen Namen Handlungen ausführen. Klar ist: Banken und Versicherungen bitten niemals um die Zusendung von Kreditkartennummern, PIN, TAN oder anderen Zugangsdaten per Email, per SMS oder telefonisch.

### Polymorphe Viren

Wahre Meister der Tarnung und Verkleidung sind polymorphe Viren. Sie verändern ihre eigenen Programmiercodes - und sind deshalb besonders schwer zu erkennen.

### Programmviren

Ein Computervirus ist ein Programm, welches die Fähigkeit besitzt, sich nach seinem Aufruf selbsttätig an andere Programme auf irgendeine Weise anzuhängen und dadurch zu infizieren. Viren vervielfältigen sich also im Gegensatz zu logischen Bomben und Trojanern selber. Im Gegensatz zu einem Wurm benötigt der Virus immer ein fremdes Programm als Wirt, in dem er seinen virulenten Code ablegt. Im Normalfall wird aber der eigentliche Programmablauf des Wirtes selber nicht geändert.

### Rootkit

Ein Rootkit ist eine Sammlung von Softwarewerkzeugen, die nach dem Einbruch in ein Computersystem installiert werden, um Logins des Eindringlings zu verbergen, Prozesse zu verstecken und Daten mitzuschneiden - generell gesagt: sich unsichtbar zu machen. Sie versuchen bereits installierte Spionageprogramme zu aktualisieren und gelöschte Spyware erneut zu installieren.

### Skriptviren und Würmer

Diese Viren sind extrem einfach zu programmieren und verbreiten sich - entsprechende Techniken vorausgesetzt - innerhalb weniger Stunden per Email um den ganzen Erdball. Skriptviren und -würmer benutzen eine der Script-Sprachen, wie beispielsweise Javascript, VBScript etc., um sich selbst in andere, neue Skripte einzufügen oder sich selber durch den Aufruf von Betriebssystemfunktionen zu verbreiten. Häufig geschieht dies per Email oder durch den Austausch von Dateien (Dokumenten).

Als Wurm wird ein Programm bezeichnet, das sich selber vervielfältigt jedoch keinen Wirt infiziert. Würmer können also nicht Bestandteil anderer Programmabläufe werden. Würmer sind auf Systemen mit restriktiveren Sicherheitsvorkehrungen oft die einzige Möglichkeit irgendwelche Schadensprogramme einzuschleusen.

### **Spyware**

Spyware sind sogenannte Spionageprogramme, die persönliche Daten des Benutzers ohne dessen Wissen oder gar Zustimmung an den Hersteller der Software oder an Dritte sendet. Meist dienen Spyware-Programme dazu, das Surf-Verhalten im Internet zu analysieren und gezielte Werbe-Banner oder Werbe-Popups einzublenden.

### **Trojanische Pferde (kurz Trojaner)**

Trojaner sind in letzter Zeit recht häufig anzutreffen. So bezeichnet man Programme, die vorgeben, eine bestimmte Funktion zu haben, nach ihrem Start aber ihr wahres Gesicht zeigen und irgendeine andere Funktion ausführen, die zumeist zerstörerisch ist. Trojanische Pferde können sich nicht selber vermehren, was sie von Viren und Würmern unterscheidet. Die meisten haben einen interessanten Namen (SEX.EXE oder STARTME.EXE), der den Anwender zur Ausführung des Trojaners verleiten soll. Unmittelbar nach der Ausführung werden diese dann aktiv und formatieren z.B. die Festplatte. Eine spezielle Art eines Trojaners ist ein Dropper, der Viren 'droppt', d.h. in das Computersystem einpflanzt.

### **Zombie**

Ein Zombie-PC ist ein Rechner, welcher mit Malwareprogrammen infiziert ist und es den Hackern erlaubt, Rechner per Fernsteuerung für ihre kriminellen Zwecke zu missbrauchen. Der betroffene PC startet auf Befehl beispielsweise Denial-of-Service-(DoS) Attacken oder versendet Spam und Phishing Emails.



## 9 Info und Service

Auf der AntiVir Administration unter dem Knoten *Info über...* erhalten Sie Informationen zu unseren Kontakt- und Supportadressen. Gerne nehmen wir Ihre Anregungen auf, unsere Produkte zu verbessern. Insbesondere bei nicht erkannten verdächtigen Dateien und bei Fehlalarmen können Sie dazu beitragen, den Virenschutz der AntiVir Produkte zu optimieren.

### Verdächtige Dateien

Viren, die gegebenenfalls von unseren Produkten noch nicht erkannt bzw. entfernt werden können oder verdächtige Dateien können Sie an uns senden. Dafür stellen wir Ihnen mehrere Wege zur Verfügung.

- Senden Sie die gewünschte Datei gepackt (WinZIP, PKZip, Arj etc.) im Anhang einer Email an [virus@avira.de](mailto:virus@avira.de). Da einige Email-Gateways mit Antivirensoftware arbeiten, sollten Sie die Datei(en) zusätzlich mit einem Kennwort versehen (bitte nicht vergessen, uns das Kennwort mitzuteilen).
- Alternativ haben Sie die Möglichkeit, die verdächtige Datei über unsere Webseite an uns zu senden.

### Fehlalarm

Sind Sie der Meinung AntiVir meldet einen Fund in einer Datei, die jedoch mit hoher Wahrscheinlichkeit "sauber" ist, so senden Sie diese Datei mit einem Hinweis auf einen Fehlalarm, gepackt (WinZIP, PKZIP, Arj etc.) im Anhang einer Email, an [virus@avira.de](mailto:virus@avira.de). Da einige Email-Gateways mit Antivirensoftware arbeiten, sollten Sie die Datei(en) zusätzlich mit einem Kennwort versehen (bitte nicht vergessen, uns das Kennwort mitzuteilen).

# 10 Konfigurationsoptionen

## 10.1 Konfigurationsoptionen

Sie konfigurieren Avira AntiVir Sharepoint in der AntiVir Administration unter *Einstellungen*. Es sind folgende Konfigurationsoptionen verfügbar:

- **AntiVir konfigurieren:** Optionen zur Heuristik, zur Archivsuche und zur Protokollierfunktion
- **Update konfigurieren:** Downloadmethode (via Webserver oder Fileserver), Konfiguration der Verbindung zum Downloadserver, Email-Benachrichtigungsfunktion

## 10.2 AntiVir konfigurieren

### 10.2.1 AntiVir konfigurieren

Unter **AntiVir konfigurieren** können Sie die heuristische Suche, die Archivsuche und die Protokollierfunktion von AntiVir SharePoint einstellen.

### 10.2.2 Suche

Unter **Suche** können Sie Optionen zur Heuristik aktivieren. Avira AntiVir SharePoint enthält sehr leistungsfähige Heuristiken, mit denen unbekannte Malware proaktiv erkannt werden kann, das heißt bevor eine spezielle Virensignatur gegen den Schädling erstellt und ein Virenschutz-Update dazu versandt wurde. Die Virenerkennung erfolgt durch eine aufwendige Analyse und Untersuchung des betreffenden Codes nach Funktionen, die für Malware typisch sind. Erfüllt der untersuchte Code diese charakteristischen Merkmale, wird er als verdächtig gemeldet (heuristischer Treffer). Dies bedeutet aber nicht zwingend, dass es sich bei dem Code tatsächlich um Malware handelt; es können auch Fehlmeldungen vorkommen. Heuristische Treffer werden wie Viren, die aufgrund einer bekannten Virensignatur erkannt wurden, behandelt: Der Transfer der betroffenen Dateien wird unterbunden.

#### **Makrovirenheuristik**

##### **Makrovirenheuristik aktivieren**

AntiVir enthält eine sehr leistungsfähige Makrovirenheuristik. Bei aktivierter Option werden Dokumente nach unbekanntem Makroviren durchsucht. In einem betroffenen Dokument werden bei möglicher Reparatur alle Makros gelöscht.

### Advanced Heuristic Analysis and Detection (AHeAD)

#### Advanced Heuristic Analysis and Detection (AHeAD)

Bei aktivierter Option wird die heuristische Suche nach Viren mit der AntiVir AHeAD Technologie aktiviert. Bei heuristischen Treffern werden die betroffenen Daten als Viren behandelt. Sie können einstellen, wie 'scharf' die Heuristik sein soll. Standardmäßig ist die Option aktiviert.

#### Erkennungsstufe niedrig

Bei aktivierter Option erkennt AntiVir SharePoint etwas weniger unbekannte Malware, die Gefahr von möglichen Fehlerkennungen ist hier gering.

#### Erkennungsstufe mittel

Bei dieser Einstellung ist das Verhältnis zwischen Erkennungsleistung und Fehlmeldungen optimiert: Bei relativ hohen Erkennungsraten von unbekannter Malware erfolgen relativ wenig Fehlmeldungen. Die Option ist standardmäßig aktiviert und wird empfohlen.

#### Erkennungsstufe hoch

Bei aktivierter Option erkennt AntiVir SharePoint bedeutend mehr unbekannte Malware, Sie müssen aber mit Fehlmeldungen rechnen.

## 10.2.3 Archive

Unter **Archive** können Sie die Suche in Archiven konfigurieren. Da die Archivsuche ggf. eine hohe Rechnerleistung beanspruchen kann, haben Sie Optionen zur Verfügung, um die Suche in Archiven zu beschränken oder das Verhalten der Suche in Archiven zu konfigurieren.

### Archiveinstellungen

#### Archive durchsuchen

Bei aktivierter Option werden Archive durchsucht. Die Archive werden dabei entpackt und durchsucht. Die Archivsuche ist standardmäßig aktiviert und wird empfohlen.

#### Smart Extensions

Bei aktivierter Option erkennt AntiVir SharePoint, ob es sich bei einer Datei um ein gepacktes Dateiformat (Archiv) handelt, selbst wenn die Dateiendung von den gebräuchlichen Endungen abweicht, und durchsucht das Archiv. Zur Prüfung der Dateiformate muss jede Datei geöffnet werden. Dies verlangsamt die Suchgeschwindigkeit. Diese Einstellung ist standardmäßig aktiviert und wird empfohlen.

### Ausnahmen

Unter *Ausnahmen* haben Sie die Möglichkeit, die Archivsuche einzuschränken. Die Ausnahmen der Archivsuche dienen dazu, eine mögliche Überlastung des Systems durch Archivbomben zu verhindern. Die Optionen zur Einschränkung der Archivsuche werden automatisch deaktiviert, sobald Sie die Option *Archive durchsuchen* deaktivieren.

**Warnung**

Schränken Sie die Archivsuche in einem angemessenen Rahmen ein und orientieren Sie sich dabei an den empfohlenen Standardwerten. Archive, die von der Suche nach Viren und Malware ausgenommen werden, werden ungeprüft auf Sharepoint-Teamseiten übertragen oder von diesen auf die Computersysteme der SharePoint-Nutzer heruntergeladen. So besteht die Möglichkeit, dass über Archive Malware verbreitet wird. Wenn Sie die Suche in Archiven einschränken, empfehlen Sie den SharePoint-Nutzern dringend, Archive vor dem Upload oder nach dem Download mit einem herkömmlichen Antivirens Scanner zu prüfen.

**Maximale Rekursionstiefe**

Bei der Suche in Archiven wendet AntiVir SharePoint eine rekursive Suche an: Archive in Archiven werden entpackt und auf Viren und unerwünschte Programme geprüft. Bei aktivierter Option ist die rekursive Suche mit dem angegebenen Wert für die maximale Rekursionstiefe eingeschränkt. Die Option ist standardmäßig deaktiviert. Archive, die den angegebenen Maximalwert überschreiten, werden nicht nach Viren und Malware durchsucht.

Sie können die maximale Rekursionstiefe der rekursiven Suche festlegen. Der empfohlene Standardwert ist 20: Ein Archiv wird bis zu 19 mal entpackt und auf Viren und Malware geprüft.

**Maximale Kompressionsrate (Ratio)**

Bei aktivierter Option wird die Archivsuche mit einer maximalen Kompressionsrate eingeschränkt. Die Kompressionsrate wird als das Verhältnis der Originaldateigröße zur komprimierten Dateigröße angegeben. Archive, die den angegebenen Maximalwert überschreiten, werden nicht nach Viren und Malware durchsucht. Die Option ist standardmäßig deaktiviert. Bei aktivierter Option liegt der empfohlene Standardwert bei einer Kompressionsrate von 9.

**Maximale Größe zu durchsuchender Archive**

Sie können eine maximale Größe von Archiven im MB angeben, bis zu der die Archive durchsucht werden sollen. Bei aktivierter Option werden Archive, die den angegebenen Maximalwert überschreiten, nicht nach Viren und Malware durchsucht. Die Option ist standardmäßig deaktiviert. Bei aktivierter Option liegt der empfohlene Standardwert bei 100 MB.

## 10.2.4 Report

Unter Report können Sie die Protokollierfunktion (Logger) von AntiVir SharePoint aktivieren bzw. deaktivieren und den Umfang des Loggers bestimmen. Die Logdatei `avesvc.log` wird in folgendem Verzeichnis abgelegt:

`C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\Avira\AntiVir SharePoint\logfile`s

**Hinweis**

Beim Logger des Update-Moduls besteht eine nicht konfigurierbare Beschränkung von 1500 Logdateien. Wird das Maximum von 1500 Logdateien erreicht, wird bei jedem neuen Update die älteste Logdatei gelöscht.

**Protokollierung****Aus**

Bei aktivierter Option erfolgt keine Protokollierung der Aktionen von AntiVir SharePoint.

### **Standard**

Bei aktivierter Option werden nur Fehlermeldungen von AntiVir SharePoint protokolliert.

### **Erweitert**

Bei aktivierter Option werden Fehlermeldungen und Warnmeldungen von AntiVir SharePoint protokolliert.

### **Vollständig**

Bei aktivierter Option werden alle Meldungen und Aktionen von AntiVir SharePoint protokolliert.

Standardmäßig ist die Logfunktion von AntiVir SharePoint auf die Option **Standard** gesetzt.

## **Reportdatei beschränken**

### **Größe beschränken n KB**

Bei aktivierter Option lässt sich die Reportdatei auf eine bestimmte Größe beschränken. Diese Einstellung ist standardmäßig aktiviert, mit einem Wert von 1024 KB. Übersteigt die Größe der Reportdatei die angegebene Größe, werden die Einträge der Reportdatei in eine Backup-Reportdatei zurückgesichert, die Logdatei wird zurückgesetzt. Beim Sichern der Logeinträge in der Backup-Logdatei werden die Einträge der vorangegangenen Sicherung überschrieben.

## 10.2.5 Erweiterte Gefahrenkategorien

Avira AntiVir SharePoint durchsucht Dokumente der SharePoint-Teamseiten nach Viren und Malware. Sie haben die Möglichkeit, weitere Gefahrenkategorien in die Malware-Suche einzubeziehen. Folgende Gefahrenkategorien (siehe Viren und mehr::Erweiterte Gefahrenkategorien) sind definiert:

- Adware/Spyware (ADSPY)
- Anwendung (APPL)
- Adware (ADWARE)
- Backdoor-Steuerungssoftware (BDC)
- Dialer (DIAL)
- Dateien mit verschleierte Endungen (HIDDENEXT)
- Phishing (PHISH)
- Security Privacy Risk (SPR)
- Spiele (GAME)
- Ungewöhnliche Laufzeitpacker (PCK)
- Witzprogramme (JOKE)
- Possible Fake Software (PFS)

In den Standardeinstellungen von AntiVir SharePoint sind folgende erweiterte Gefahrenkategorien in der Suche aktiviert: Adware/Spyware (ADSPY), Adware (ADWARE), Backdoor-Steuerungssoftware (BDC), Dialer (DIAL), Dateien mit verschleierte Endungen (HIDDENEXT), Phishing (PHISH).

Über die Konfiguration der Gefahrenkategorien haben Sie die Möglichkeit weitere Gefahrenkategorien beim Durchsuchen von Dokumenten zu aktivieren oder standardmäßig aktivierte Gefahrenkategorien von der Suche auszunehmen.

### **Warnung**

Sind Gefahrenkategorien nicht aktiv, werden Dateien, die der Gefahrenkategorie zugeordnet sind, nicht als Malware erfasst und blockiert. Es erfolgt kein Eintrag in die Reportdatei (Logger). Es wird empfohlen, keine per default aktivierten Gefahrenkategorien von der Suche auszunehmen.

Die Konfiguration der Gefahrenkategorien muss in der Konfigurationsdatei *avwin.ini* vorgenommen werden. Nach einer Änderung der *avwin.ini* muss der Dienst Avira AntiVir SharePoint Scan Service neu gestartet werden. Sie finden die Konfigurationsdatei unter:

*C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\Avira\AntiVir  
SharePoint\config*

Ändern Sie den Eintrag:

```
[COMMON]  
PrefixDiff=+[Kategorienkürzel], -[Kategorienkürzel]
```

Mit dem Plus-Zeichen aktivieren Sie zusätzliche Gefahrenkategorien, mit dem Minus-Zeichen deaktivieren Sie die per default aktivierten Gefahrenkategorien. Wenn Sie keine Werte für den Eintrag PrefixDiff angeben, werden die Standardeinstellungen geladen.

### Beispiele:

```
[COMMON]  
PrefixDiff=
```

Die Standardeinstellungen mit den aktivierten Gefahrenkategorien DIAL, ADSPY, ADWARE, BDC, HIDDENEXT, PHISH sind aktiviert.

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

Alle Standard-Gefahrenkategorien sind deaktiviert: DIAL, ADSPY, ADWARE, BDC, HIDDENEXT, PHISH. Alle zusätzlichen Gefahrenkategorien sind aktiviert: APPL, GAME, JOKE, PCK, PFS, SPR.

## 10.3 Update konfigurieren

### 10.3.1 Update konfigurieren

Unter **Update konfigurieren** legen Sie die Netzwerkeinstellungen und ggf. Proxy-Einstellungen für das Update von AntiVir SharePoint fest. Sie können des Weiteren eine Email-Benachrichtigung per SMTP konfigurieren.

### 10.3.2 Netzwerk

Unter **Netzwerk** konfigurieren Sie die Netzwerkeinstellungen für das Update von AntiVir SharePoint. Sie können Updates über einen Webserver oder via Fileserver / Share aus dem Internet oder Intranet beziehen (siehe Kap. Updates).

#### Netzwerk Einstellungen

##### Update URL

Geben Sie die URL oder die IP-Adresse des Servers an, von dem Sie die Updates laden möchten. Sie können mehrere, durch Komma separierte Webserver angeben. AntiVir SharePoint nutzt den ersten verfügbaren Webserver zum Update:

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

Wenn Sie die Updates von einem Fileserver über ein Share-Verzeichnis beziehen möchten, geben Sie den UNC-Pfad zum Share-Verzeichnis an:

```
\\<Servername>|<IP-Adresse>\<Freigabename>\<Pfad>
```

##### Update Intervall in Minuten

Geben Sie ein Update-Intervall in Minuten an. Im angegebenen Intervall prüft AntiVir SharePoint, ob Updates für AntiVir SharePoint am angegebenen Update-Server vorliegen, und startet ggf. den Update-Vorgang. Die Standardeinstellung beträgt 120 Minuten und wird empfohlen.

#### Netzwerk Zugriff

Wenn Sie für das Update ein Share-Verzeichnis auf einem Fileserver nutzen, geben Sie einen Benutzernamen mit Passwort an.

##### **Warnung**

Der Benutzername und das Passwort für den Netzwerkzugriff werden verschlüsselt gespeichert. Um Sicherheitsrisiken auszuschließen, wird empfohlen für den Zugriff auf den Fileserver ein Benutzerkonto mit eingeschränkten Benutzerrechten zu verwenden. Zur Ausführung des Updates benötigen Sie auf dem Fileserver ausschließlich Leserechte.

##### Benutzername

Geben Sie einen Benutzernamen zur Authentifizierung ein.

##### Kennwort

Geben Sie ein Passwort zur Authentifizierung ein.

### 10.3.3 Proxy

Wenn Sie für das Update von AntiVir SharePoint einen Webserver nutzen, können Sie unter **Proxy** einen Proxyserver angeben, über den die Verbindung zum Webserver erstellt werden soll.

#### Proxyserver

##### Über Proxyserver verbinden

Bei aktivierter Option verbindet sich AntiVir SharePoint über einen Proxyserver mit dem Webserver, der für das Update von AntiVir SharePoint genutzt wird. Diese Option ist standardmäßig deaktiviert.

### Adresse

Geben Sie die URL oder IP-Adresse des Proxyservers ein, über den sich AntiVir SharePoint mit dem Webserver verbinden soll.

### Port

Geben Sie die Port-Nummer des Proxyservers ein, über den sich AntiVir SharePoint mit dem Webserver verbinden soll.

### Benutzername

Geben Sie Ihren Anmeldenamen am Proxyserver ein.

### Kennwort

Geben Sie das entsprechende Kennwort für die Anmeldung am Proxyserver ein.

## 10.3.4 Email

Unter **Email** können Sie Einstellungen für eine Email-Benachrichtigung via SMTP angeben. Sie werden wahlweise bei jedem ausgeführten Update oder nur bei einem fehlerhaften Update per Email benachrichtigt. Die Email-Nachricht enthält folgende Informationen:

- Computernamen von AntiVir SharePoint
- Datum und Zeitpunkt des Updates
- Status des Updates

### **Email-Nachrichten**

#### **Email Benachrichtigung aktivieren**

Bei aktivierter Option erfolgt wahlweise bei jedem Update oder nur bei einem fehlerhaften Update eine Email-Benachrichtigung. Diese Option ist standardmäßig deaktiviert.

#### **Ereignisauswahl**

Wählen Sie das Ereignis aus, bei dessen Eintreten Sie benachrichtigt werden möchten:

#### ***Benachrichtigen, wenn ein Update fehlgeschlagen ist***

Es wird ausschließlich nach einem fehlerhaftem Update eine Email versendet.

#### ***Bei jedem Update benachrichtigen***

Es wird nach jedem ausgeführten Update, bei dem neue Dateien installiert wurden oder ein Fehler aufgetreten ist, eine Email-Benachrichtigung versendet. Es wird keine Email versendet, wenn beim Update-Vorgang keine neuen Dateien installiert wurden, weil AntiVir SharePoint bereits über die aktuellen Dateien verfügt.

#### **SMTP-Server**

Geben Sie den Namen des SMTP-Servers, den Sie zum Versenden der Benachrichtigungen verwenden möchten ein.

#### **Benutzername**

Geben Sie einen Benutzernamen zur Authentifizierung am SMTP-Server an.

**Kennwort**

Geben Sie ein Kennwort zur Authentifizierung am SMTP-Server an.

**Absenderadresse**

Geben Sie einen Namen oder eine Email-Adresse als Absender der Email-Benachrichtigung an.

**Empfängeradresse**

Geben Sie die Email-Adresse des Empfängers der Email-Benachrichtigung an. Sie können auch mehrere, durch Komma separierte Empfänger-Adressen angeben.

## **//// Avira AntiVir SharePoint**

### **Avira GmbH**

Lindauer Str. 21  
88069 Tett nang  
Germany  
Telefon: +49 (0) 7542-500 0  
Fax: +49 (0) 7542-525 10  
Internet: <http://www.avira.de>

© Avira GmbH. Alle Rechte vorbehalten.

Dieses Handbuch wurde mit äußerster Sorgfalt erstellt. Dennoch sind Fehler in Form und Inhalt nicht ausgeschlossen. Die Vervielfältigung dieser Publikation oder von Teilen dieser Publikation in jeglicher Form ist ohne vorherige schriftliche Genehmigung durch die Avira GmbH nicht gestattet.

Irrtümer und technische Änderungen vorbehalten.

Ausgabe Q3-2009

AntiVir<sup>®</sup> ist ein registriertes Warenzeichen der Avira GmbH. Alle anderen Marken- und Produkt-namen sind Warenzeichen oder eingetragene Warenzeichen ihrer entsprechenden Besitzer. Geschützte Warenzeichen sind in diesem Handbuch nicht als solche gekennzeichnet. Dies bedeutet jedoch nicht, dass sie frei verwendet werden dürfen.