



# TECHNISCHER NEWSLETTER FÜR RELEASE

Q3 –2008 (September 2008)



## AVIRA ANTIVIR WINDOWS

Produkt	Funktion	Beschreibung
Avira AntiVir Sharepoint	Support für Microsoft Office SharePoint 2007 und SharePoint Services 3.0	<p>Avira AntiVir SharePoint unterstützt jetzt den Microsoft Office SharePoint Server 2007 und die entsprechenden SharePoint Services 3.0.</p> <p>Das Produkt ist in deutscher und englischer Sprache verfügbar.</p> <p><b>Bitte beachten Sie:</b></p> <p>Diese Version von Avira AntiVir SharePoint läuft nur auf dem Microsoft Office SharePoint Server 2007 (x86), d.h. auf der 32 Bit Version des SharePoint Servers.</p> <p>Eine Version von Avira AntiVir SharePoint, die auf der 64 Bit Version des Microsoft Office SharePoint Servers 2007 läuft, wird im Dezember 2008 verfügbar sein.</p> <p><b>Bitte beachten Sie ebenfalls:</b></p> <p>Der Avira AntiVir SharePoint kann nicht remote konfiguriert werden. Ursache hierfür ist die Verwendung des AVIPC Protokolls für die Interprozesskommunikation (AVIPC weist Verbindungsanfragen anderer Hosts zurück). Zur Remote Konfiguration sollte daher das Microsoft RDP (=remote desktop protocol) verwendet werden.</p>
	Neue MMC-basierte GUI	Microsoft Office SharePoint Server 2007 und die SharePoint Services 3.0 verwenden beide geänderte Template Architekturen. Daher konnte die vorhandene HTML-basierte GUI nicht länger verwendet werden.

		<p>Eine neue GUI wurde entwickelt. Für diese neue GUI wurde ein MMC Snap-In verwendet, das auf dem existierenden Avira MMC Framework beruht. Bitte beachten Sie die folgenden Merkmale dieser GUI:</p> <p><u>Status</u></p> <p>Der Status Knoten zeigt den verbundenen Knoten an und ob es mit dieser Verbindung Probleme gibt.</p> <p><u>Übersicht</u></p> <p>Der Übersichtsknoten zeigt den aktuellen Status des Dienstes an, den Status des Scanners, den Update Status, Lizenzinformationen und zusätzliche Warnungen und Hinweise.</p> <p><u>Statistiken</u></p> <p>Der Statistiknoten zeigt statistische Daten in Form einer HTML Seite an:</p> <ul style="list-style-type: none"><li>○ Letzte geprüfte Datei</li><li>○ Letzte gefundene Malware</li><li>○ Gesamtzahl geprüfter Dateien</li><li>○ Gesamtzahl gefundener infizierter Dateien</li></ul> <p><u>Einstellungen</u></p> <p>Der Einstellungenknoten ermöglicht die Konfiguration der beiden Avira AntiVir Sha-</p>
--	--	---

		<p>rePoint Komponenten:</p> <ul style="list-style-type: none"> <li>○ AntiVir (Scanning):             <ul style="list-style-type: none"> <li>○ Die Scan-Einstellungen sind die von der Savapi 2 (die vom Produkt verwendet wird) angebotenen Konfigurationseinstellungen, u.a. im Bereich Archivbehandlung und Heuristik.</li> </ul> </li> <li>○ Updater             <ul style="list-style-type: none"> <li>○ Die Updater-Konfiguration erlaubt Netzwerkkonfiguration (= Festlegen der Update URL), Konfiguration eines Proxyservers und Festlegung der Benachrichtigungsoptionen.</li> </ul> </li> </ul> <p><u>Infos über</u></p> <p>Der "Infos über..." Knoten zeigt allgemeine Produktinformationen auf einer HTML Seite an:</p> <ul style="list-style-type: none"> <li>○ Produktinformation: (Kontakt Daten, Links, Internet)</li> <li>○ Supportinformationen: (Email, Internet)</li> <li>○ Lizenzinformation: (Laufzeitende der Lizenz, Seriennummer, Lizenznehmer)</li> </ul>
	Systemanforderungen	<p>Bitte beachten Sie die folgenden Systemanforderungen</p> <ul style="list-style-type: none"> <li>○ Microsoft Office SharePoint Server 2007 oder SharePoint Services 3.0 (32 Bit) oder</li> <li>○ Microsoft Office SharePoint Portal Server 2003 oder SharePoint Services 2.0</li> </ul>

		<ul style="list-style-type: none"> <li>○ ab Intel Pentium III kompatibel</li> <li>○ mindestens 512 MB Arbeitsspeicher</li> <li>○ mindestens 100 MB freier Speicherplatz auf der Festplatte, mehr für temporäre Files</li> </ul>
<b>Avira AntiVir Mobile (Pocket PC)</b>	Unterstützung von Softkeys und Menüsystem	<p>Die alte Kommando-Toolbar wurde entfernt. Avira AntiVir Mobile (Pocket PC) kann jetzt vom Anwender vollständig nur mit Hilfe des rechten und linken Softkeys bedient werden.</p> <p>Auf Geräten, die nicht über Softkeys verfügen kann das Menü über den normalen Stick bedient werden.</p> <p><b>Bitte beachten Sie:</b></p> <p>Die meisten Dialoge sind jetzt vollständige Bildschirmdialoge. Dies trifft insbesondere für den „About“ und den „Lizenzdialog“, die Konfigurationsdialoge, Scannermeldungen, Malwaremeldungen, Statistiken und das Updatesystem zu.</p>
	Anzeige des SIP Button Controls nach MS Standard	In Übereinstimmung mit den MS Designrichtlinien befindet sich das SIP Control (=software based input panel, d.h. der Zugang zu einem softwarebasierten Keyboard, über das das Gerät gesteuert werden kann – bei Geräten, die selbst nicht über eine Tastatur verfügen) jetzt in der Mitte der Taskleiste des Fensters.
	Support für den Standard „Warten“ Mauszeiger	Das Produkt unterstützt jetzt den „Warten“ Mauszeiger des Systems (farbiges Rädchen), der angezeigt wird, wenn ein Kommando ausgeführt wird, das das aktuelle Fenster rendert oder wenn das System als Ganzes auf eine Eingabe des Anwenders

		nach 0,5 Sekunden noch nicht reagiert hat.
	Verbesserte Stabilität des Guard	Der AV Guard wurde optimiert, um Deadlocks, die ab und an auf Windows Mobile 6 und Mobile 5 auftraten, zu verhindern.
	Lizenz-Blacklisting	Das Produkt erlaubt jetzt das Blacklisting von Lizenzen. D.h. Seriennummern, die illegal verwendet werden, können jetzt gesperrt werden. Mit einer Lizenz, die gesperrt wurde, kann das Produkt nicht mehr betrieben werden, da diese Lizenz wie eine ungültige Lizenz behandelt wird.
	Neue Kommandos zur Verwendung in der Kommandozeile	Eine Reihe von Kommandozeilen Kommandos wurden zum Programm hinzugefügt: <ul style="list-style-type: none"> <li>○ Kommando “/CFG_GUARD” start die Guard Konfiguration</li> <li>○ Kommando “/CFG_SCANNER” startet die Scanner Konfiguration</li> <li>○ Kommando “/CFG_GENERAL” startet die allgemeine Konfiguration</li> </ul>
	Geänderter Guard Startup Dialog	Der Dialog, der es dem Anwender ermöglicht, den Guard nach einem Soft-Reset zu beenden, wird jetzt nur eingeblendet, wenn der Guard tatsächlich aktiviert war. Die erneute Aktivierung des Guard kann über die normalen Konfigurationseinstellungen vorgenommen werden.

## AVIRA ANTIVIR UNIX

Produkt	Funktion	Beschreibung
<p><b>Avira AntiVir MailGate /Avira MailGate Suite</b></p>	<p>Neue Version 3.0 von Avira AntiVir MailGate basierend auf der SAVAPI 3</p>	<p>Die neue Version 3.0 von Avira AntiVir MailGate und MailGate Suite beruht jetzt auf der neuen SAVAPI 3.</p> <p>Einer der wesentlichen Vorzüge der SAVAPI 3 ist die native Einbindung der neuen Avira AntiVir Engine. Die Engine selbst bietet dem Kunden eine ganze Reihe von Vorteilen:</p> <ul style="list-style-type: none"> <li>○ 15 % bis 20 % schnellerer Scan</li> <li>○ Die modulare Struktur erlaubt ein sehr schnelles Update einzelner Engine Komponenten, um schnell auf neue Gefahren zu reagieren</li> <li>○ Sie prüft auch Dateien, die größer sind als 4 GB</li> </ul> <p>Die SAVAPI 3 unterstützt das Single File Update einzelner Engine Komponenten als auch der VDF und SAVAPI 3 Komponenten und liefert damit ein höheres Sicherheitslevel, da das gesamte System im Falle neuer Gefahren sehr schnell aktualisiert werden kann.</p> <p><b>Bitte beachten Sie:</b></p> <p>Installationen von MailGate/MailGate Suite in der Version 2.x können nicht direkt auf die Version 3.0 aktualisiert werden. Sie müssen entfernt werden, bevor die neue Versi-</p>

		<p>on 3.0 installiert werden kann.</p> <p>Es gibt eine Migrationsperiode bis zum 31.10.2009, in der die Version 2.x weiterhin mit Updates für Engine und VDF versorgt wird. Kunden können daher frei wählen, wann sie auf die Version 3.0 aktualisieren möchten.</p> <p><b>Bitte beachten Sie ebenfalls:</b></p> <p>MailGate und MailGate Suite in der Version 3.0 können nicht mehr über die GUI administriert werden. Installation, Konfiguration und Administration sind nur noch über Skripts oder die Kommandozeile möglich.</p> <p><b>Verfügbarkeit:</b></p> <p>Bitte beachten Sie, dass das Produkt für die folgenden Plattformen verfügbar ist:</p> <ul style="list-style-type: none"><li>○ Red Hat Enterprise Linux 5 Server</li><li>○ Red Hat Enterprise Linux 4 Server</li><li>○ Novell SUSE Linux Enterprise Server 10 - 10.2</li><li>○ Novell SUSE Linux Enterprise Server 9</li><li>○ Debian GNU/Linux 4 (stable)</li><li>○ Ubuntu Server Edition 8</li><li>○ Sun Solaris 10 (SPARC)</li><li>○ Sun Solaris 9 (SPARC)</li></ul>
--	--	--

<p><b>Avira MailGate Suite</b></p>	<p>Integration der neuen AntiSpam Version</p>	<p>In die MailGate Suite wurde die neue, auf dem eXpurgate SDK, Version 3.0, beruhende AntiSpam Version eingefügt.</p>
<p><b>Avira AntiVir WebGate / Avira WebGate Suite</b></p>	<p>Neue Version 3.0 von Avira AntiVir WebGate / WebGate Suite basierend auf der SAVAPI 3</p>	<p>Die neue Version 3.0 von Avira AntiVir WebGate und WebGate Suite beruht jetzt auf der neuen SAVAPI 3.</p> <p>Einer der wesentlichen Vorzüge der SAVAPI 3 ist die native Einbindung der neuen Avira AntiVir Engine. Die Engine selbst bietet dem Kunden eine ganze Reihe von Vorteilen:</p> <ul style="list-style-type: none"> <li>○ 15 % bis 20 % schnellerer Scan</li> <li>○ Die modulare Struktur erlaubt ein sehr schnelles Update einzelner Engine Komponenten, um schnell auf neue Gefahren zu reagieren</li> <li>○ Sie prüft auch Dateien, die größer sind als 4 GB</li> </ul> <p>Die SAVAPI 3 unterstützt das Single File Update einzelner Engine Komponenten als auch der VDF und SAVAPI 3 Komponenten und liefert damit ein höheres Sicherheitslevel, da das gesamte System im Falle neuer Gefahren sehr schnell aktualisiert werden kann.</p> <p><b>Bitte beachten Sie:</b></p> <p>Installationen von WebGate/WebGate Suite in der Version 2.x können nicht direkt auf die Version 3.0 aktualisiert werden. Sie müssen entfernt werden, bevor die neue Version 3.0 installiert werden kann.</p> <p>Es gibt eine Migrationsperiode bis zum 31.10.2009, in der die Version 2.x weiterhin</p>

		<p>mit Updates für Engine und VDF versorgt wird. Kunden können daher frei wählen, wann sie auf die Version 3.0 aktualisieren möchten.</p> <p><b>Bitte beachten Sie ebenfalls:</b></p> <p>WebGate und WebGate Suite in der Version 3.0 können nicht mehr über die GUI administriert werden. Installation, Konfiguration und Administration sind nur noch über Skripts oder die Kommandozeile möglich.</p> <p><b>Verfügbarkeit:</b></p> <p>Bitte beachten Sie, dass das Produkt für die folgenden Plattformen verfügbar ist:</p> <ul style="list-style-type: none"><li>○ Red Hat Enterprise Linux 5 Server</li><li>○ Red Hat Enterprise Linux 4 Server</li><li>○ Novell SUSE Linux Enterprise Server 10 - 10.2</li><li>○ Novell SUSE Linux Enterprise Server 9</li><li>○ Debian GNU/Linux 4 (stable)</li><li>○ Ubuntu Server Edition 8</li><li>○ Sun Solaris 10 (SPARC)</li><li>○ Sun Solaris 9 (SPARC)</li></ul>
--	--	---

## AVIRA SECURITY MANAGEMENT CENTER

Produkt	Funktion	Beschreibung
<p><b>Avira Security Management Center</b></p>	<p>Pull Mechanismus als neue Methode zur Kommunikation von SMC Server und Client.</p>	<p>Die Kommunikation zwischen SMC-Server und Clients beruhte bislang auf dem PUSH-Verfahren. Diese Verfahren wurde jetzt um ein PULL-Verfahren ergänzt.</p> <p>Der Unterschied besteht darin, dass die Clients jetzt neue Operationen vom SMC-Server abfordern (=pull) wohingegen beim PUSH-Mechanismus der SMC-Server die Operationen auf die Clienten schiebt (=push)</p> <p>Dies scheint nur eine kleine Änderung zu sein aber tatsächlich ist diese Änderung eine Voraussetzung, um die SMC als Verwaltungstool in größeren Netzwerken mit zehntausenden von Clienten einsetzbar zu machen.</p> <p>Mit dem PUSH-Mechanismus schiebt der SMC-Server Kommandos direkt zu den Agenten. Dies kann gerade in größeren Netzwerken lange Wartezeiten hervorrufen, da alle Klienten, auch die, die gerade offline sind, kontaktiert werden.</p> <p>Beim dem PULL Mechanismus erzeugt der SMC-Server so genannte „pending operations“, die die Aktionen darstellen, die auf der Client-Seite ausgeführt werden müssen. Die 2.3 Version des Agents kontaktiert in einem konfigurierbaren Zeitintervall den SMC-Server und prüft, ob neue „pending operations“ für ihn vorhanden sind und falls ja, führt diese aus.</p> <p>Bitte beachten Sie, dass die Standard Kommunikationsmethode zwischen SMC-Server</p>

		<p>und Agents immer noch "PUSH" ist. Dies trifft sowohl für neue SMC Installationen als auch für Upgrade Installationen von der vorherigen Version zu.</p> <p>Der "PULL"-Modus muss optional über die Agent-Konfiguration eingestellt werden. Daher ist es möglich, SMC-Agents im „PULL“-Modus und gleichzeitig andere Agenten im „PUSH“-Modus zu betreiben.</p> <p>Da der SMC Server in der Lage ist, mit Agents in beiden Modi zu arbeiten, sollte es keine Kompatibilitätsprobleme mit Agenten geben, deren Version kleiner als 2.3 ist.</p> <p>Die folgenden Funktionen, bei denen eine Client-Kommunikation involviert ist, können als PULL Operationen konfiguriert werden:</p> <ul style="list-style-type: none"> <li>○ Produktinstallation /-deinstallation (mit Ausnahme der Agent Installation, wenn sie remote über das entsprechende Feature der SMC erfolgt)</li> <li>○ Produkt-Konfiguration</li> <li>○ Produkt-Kommandos</li> <li>○ Task Management</li> <li>○ Rechner-Status-Anzeige</li> </ul> <p>Aus technischen Gründen basieren andere Funktionen wie das Holen und Anzeigen von Logdateien immer noch auf dem Push-Mechanismus.</p> <p><b>Wie es funktioniert:</b></p> <p>Zunächst einmal muss der Anwender entscheiden, ob er die Kommunikationsmethode zwischen SMC-Server und SMC-Agents auf PULL umstellen möchte. Dies ist über die</p>
--	--	---

		<p>SMC-Agent Konfiguration möglich. Hier kann auch das PULL-Intervall festgelegt werden (die Standardeinstellung beträgt 60 Sekunden)</p> <p>Tasks, die jetzt erstellt werden, werden automatisch als server-verwaltete Tasks gespeichert, d.h. als Tasks, die auf dem Server gespeichert werden, aber über den internen Task-Planer des Agents ausgeführt werden.</p> <p><b>Bitte beachten Sie:</b></p> <p>Die Konfigurationsoption, die es ermöglichte, einen Task als agent-basierten Task zu speichern wurde entfernt. Alle Tasks werden jetzt automatisch auf dem SMC-Server gespeichert. SMC-Agents 2.3 speichern diese Tasks als server-verwaltete Tasks, d.h. sie werden nicht vom Server ausgeführt, sondern vom Agent. SMC Agents kleiner 2.3 (d.h. Agents, die den PULL Mechanismus nicht unterstützen) speichern sie als server-basierte Tasks, d.h. sie werden vom Server ausgeführt.</p>
	<p>Filternde Gruppen (=gefilterte Sicherheitsumgebung)</p>	<p>Insbesondere in Sicherheitsumgebungen, die tausende oder zehntausende von Clients verwalten, benötigt der Administrator einen schnellen Überblick über alle Klienten, die in irgendeiner Form seine Aufmerksamkeit erfordern</p> <p>Für diese Anforderung stellt die SMC jetzt eine Funktion zur Verfügung, die es erlaubt, die Computer in der Sicherheitsumgebung nach bestimmten Kriterien zu filtern und das Ergebnis in einer oder mehreren speziellen virtuellen Gruppen, so genannten „gefilterten Sicherheitsumgebungen“ darzustellen.</p> <p>Folgende Filter können zur Erzeugung virtueller Gruppen oder gefilterter Sicherheitsumgebungen verwendet werden:</p>

		<ul style="list-style-type: none"> <li>○ Rechner, die einen Fehlerstatus melden</li> <li>○ Rechner, die einen Produkt-Fehler-Status melden:             <ul style="list-style-type: none"> <li>○ Modul veraltet</li> <li>○ Allgemeiner Modulfehler</li> </ul> </li> <li>○ Rechner, auf denen ein bestimmtes Produkt nicht installiert ist             <ul style="list-style-type: none"> <li>○ (Alle Produkte im Software Repository befinden, können ausgewählt werden)</li> </ul> </li> </ul> <p><b>Bitte beachten Sie:</b></p> <p>Eine filternde Gruppe liefern lediglich eine bestimmte Sicht auf alle Clients dar, die dem gewählten Filterkriterium entsprechen, d.h. die Clients werden nicht permanent in diese Gruppe verschoben, sondern bleiben in ihrer Originalgruppe.</p> <p>Alle Aktionen, die für diesen Client in der filternden Gruppe ausgeführt werden, werden jedoch tatsächlich auf dem realen Client ausgeführt.</p>
	Aktivieren des Planers für den integrierten IUM während der Installation	In der Vergangenheit war der Planer für den Integrierten Internet Update Manager nach der Installation deaktiviert. Der Anwender musste daher nach der Installation das SMC Frontend öffnen und den IUM Planer separat konfigurieren. Dies wurde nun geändert, so dass der Anwender nun bereits während der Installation den IUM Updater aktivieren und konfigurieren kann.
<b>Avira Internet Update Manager</b>	Neue IUM Status Anzeige	Die IUM Benutzeroberfläche stellt jetzt einige Realtime Status Informationen zur Verfügung. Diese Infos werden in drei TABS im Anzeigebereich neben der Navigationsleiste gezeigt. Jeder Server, der im IUM verwaltet wird, erhält seine eigene Status Anzeige.

		<p>Angezeigt werden:</p> <ul style="list-style-type: none"> <li>○ Server Info</li> <li>○ Server Status</li> <li>○ Log Datei</li> </ul> <p>Die Status Infos sind nur bei geöffnetem IUM Frontend verfügbar. Daten werden nicht persistent gespeichert.</p> <p>Ältere Daten sind über die Logdatei zugänglich. Die maximale Größe der Logdatei und die maximale Anzahl an Backups kann über die ium.conf konfiguriert werden.</p>
	Aktivieren des Planers für den integrierten IUM während der Installation	In der Vergangenheit war der Planer für den Internet Update Manager nach der Installation deaktiviert. Der Anwender musste daher nach der Installation das SMC Frontend öffnen und den IUM Planer separat konfigurieren. Dies wurde nun geändert, so dass der Anwender nun bereits während der Installation den IUM Updater aktivieren und konfigurieren kann.
	Neuer Knoten "Einstellungen" im IUM Frontend	Alle Einstellungen, die das Selbst-Update des IUM Frontends, Proxy-Server Einstellungen und Update Server betreffen, sind jetzt in einem neuen Knoten „Einstellungen“ zusammengefasst worden, der sich unter dem MMC Rootknoten befindet.

## AVIRA ANTIVIR EXCHANGE

Produkt	Funktion	Beschreibung
Avira AntiVir Exchange	Neue Version 7 für Microsoft Exchange Server 2007	<p>Die neue Avira AntiVir Exchange, Version 7, ist jetzt verfügbar. Drei verschiedene Pakete werden angeboten:</p> <ol style="list-style-type: none"> <li>1. Avira AntiVir Exchange, Version 7 (für Microsoft Exchange Server 2000/2003 32 Bit)</li> <li>2. Avira AntiVir Exchange, Version 7 (für Microsoft Exchange Server 2007 64 Bit)</li> <li>3. Avira AntiVir Exchange, Version 7 (für Microsoft Exchange Server 2007 32 Bit) → nur für Testzwecke</li> </ol> <p><b>Bitte beachten Sie:</b></p> <p>Microsoft erlaubt die Installation und Verwendung der Exchange Server 2007 32 Bit Version nur für Testzwecke. Jede Verwendung in produktiven Umgebungen ist strengsten verboten und stellt einen Bruch der Microsoft Lizenzregelungen dar.</p> <p>Die Avira AntiVir Exchange, Version 7, für Microsoft Exchange Server 2007 32 Bit wird daher <u>offiziell nicht</u> im Avira Shop oder in irgendeinem anderen Avira Vertriebskanal <u>verfügbar</u> sein. Sie wird auf Anfrage nur für Testzwecke zur Verfügung gestellt.</p>

		<p><b>Besonderer Hinweis zum Upgrade::</b></p> <p>Ein Upgrade von einer Version 6.x oder kleiner auf die Version 7 erfordert eine Deinstallation der Altversion und nachfolgende Neuinstallation der Version 7.</p> <p>Hauptgrund hierfür ist die drastische Veränderung der Verzeichnisstruktur und der Registryeinträge in der Version 7.</p> <p><b>Bitte beachten Sie:</b></p> <p>Die Veröffentlichung der Avira AntiVir Exchange, Version 7 ist für Mitte Oktober geplant.</p> <p><b>Bitte beachten Sie ebenfalls:</b></p> <p>Das Avira SmallBusiness Suite Paket wird die neue Avira AntiVir Exchange, Version 7 (für Microsoft Exchange Server 2000/2003 32 Bit) erhalten und kurz nach der Veröffentlichung von Avira AntiVir Exchange, Version 7, verfügbar sein.</p>
	<p>DCC ersetzt durch Avira SPACE</p>	<p>Das DCC (Distributed Checksum Clearinghouse) System, das für die SPAM Erkennung bislang genutzt wurde, ist durch das Avira eigenen SPACE Modul (=Spam and Phishing Cross-platform Engine) ersetzt worden.</p>

## EINE WICHTIGE INFORMATION FÜR ANWENDER DER PRODUKTE AVIRA ANTIVIR MAILGATE/MAILGATE SUITE UND WEBGATE/WEBGATE SUITE

Mit dem Q3-2008 Release veröffentlicht Avira die neue Version 3.9 der AntiVir Produkte MailGate/MailGate Suite und WebGate/WebGate Suite. Falls Sie diese Produkte einsetzen, dann erhalten Sie durch die Version 3.0 eine Vielzahl neuer Funktionen und Verbesserungen wie zum Beispiel eine neue Engine, die 15 % bis 20 % schneller prüft als die Vorgängerversion. Anwender, die auf die neue Version 3.0 wechseln möchten, müssen die vorherige Version 2.x vorher deinstallieren.

Als Anwender können Sie jedoch frei wählen, wann Sie auf die neue Version wechseln oder migrieren wollen, denn Avira wird die Version 2.x noch bis zum 31. Oktober 2009 weiter unterstützen. Das heißt, Avira wird während dieser Migrationsperiode weiterhin Updates der Engine und VDF für die 2.x Version zur Verfügung stellen.

Allerdings wird es nicht mehr möglich sein, während dieser Zeit funktionale Erweiterungen an der Vorgängerversion vorzunehmen. Falls erforderlich werden Bugfixes für Fehlfunktionen bereitgestellt, die die Verwendbarkeit dieser Produktversion ernsthaft gefährden.

Avira hat ein Migrationsportal eingerichtet, in dem Sie alle Informationen finden, die Ihnen helfen, schnell und einfach auf die Version 3.0 umzusteigen. Sie finden dieses Migrationsportal auf der Avira Homepage unter [http://www.avira.de/de/support/migration\\_avira\\_antivir\\_unix.html](http://www.avira.de/de/support/migration_avira_antivir_unix.html).