



TECHNISCHER NEWSLETTER ZUM RELEASE

Q1 – 2010 (März 2010)

AVIRA ANTIVIR WINDOWS

Produkt	Funktion	Beschreibung
Avira AntiVir, Version 10 (alle Produkte)	Neue Oberfläche	Avira AntiVir, Version 10, wird mit einer neuen Benutzeroberfläche auf den Markt kommen, die komplett neue Icons wie auch eine Navigation in 3D und ein durchgehendes Hintergrundbild beinhaltet.
Avira AntiVir, Version 10 (alle Produkte außer Avira AntiVir Personal)	Avira AntiVir ProActiv	<p>Avira AntiVir, Version 10, ist jetzt mit einer verhaltensbasiert arbeitenden Komponente ausgestattet, genannt Avira AntiVir ProActiv.</p> <p>AntiVir ProActiv überwacht ständig das Verhalten des Systems in Echtzeit und sucht nach ungewöhnlichen Ereignissen.</p> <p>Das integrierte Regelwerk ist dazu in der Lage, frühzeitig zu entscheiden, ob ein bestimmtes Ereignis (oder eine Kombination von Ereignissen) anzeigt, dass das System gerade von neuer oder unbekannter Malware (Schadsoftware) attackiert wird.</p> <p>Wenn eine Regel zutrifft, kann der Nutzer entscheiden, was mit der verdächtigen Datei geschehen soll, beispielsweise sie einmal zu blockieren, sie immer zu blockieren oder den Vorgang zu ignorieren.</p> <p>Teil dieser neuen Technologie ist die Avira AntiVir ProActiv Community, die es jedem Nutzer erlaubt, eine aktive Rolle in Aviras globalem Kampf gegen Viren und Malware einzunehmen, indem automatisch Daten zu ausgeführten Programmaktionen zu Avira</p>

		<p>geschickt werden. Diese Daten werden dann analysiert und die Ergebnisse werden wieder in das ProActiv-Modul eingespeist.</p> <p>Avira AntiVir ProActiv wird nur mittels einer benutzerdefinierten Installation bzw. einer Änderungsinstallation installiert. Wenn ein Nutzer von der AV 9 ein Upgrade auf die AV 10 vornimmt, wird er per Slide-Up informiert, dass das neue Modul AntiVir ProActiv-Modul verfügbar ist. Er kann das Modul dann installieren, in dem er eine Änderungsinstallation durchführt.</p> <p>Die Teilnahme an der Avira AntiVir ProActiv Community muss separat aktiviert werden. Wenn die AV 10 Professional mittels SMC administriert wird, kann AntiVir ProActiv und die Teilnahme an der AntiVir ProActiv Community entweder durch die GUI oder mittels eines Silent Setups separat aktiviert werden.</p> <p>Bitte beachten::</p> <p>Avira AntiVir ProActiv ist für Avira AntiVir Personal zum Q1 2010 nicht verfügbar.</p>
<p>Avira AntiVir, Version 10 (alle Produkte)</p>	<p>On-Access Scanner mit One-Click Removal, Reparatur und Slide-Up-Information</p>	<p>Der Avira AntiVir Guard (On Access-Scanner) bietet jetzt einen automatischen und einen interaktiven Modus.</p> <p>Der interaktive Modus des Avira AntiVir Guard ist verbessert worden und bietet jetzt eine viel einfachere Möglichkeit, mit gefundener Malware umzugehen. Im Falle eines Malware-Fundes wird der Zugang zu der entsprechenden Datei jetzt standardmäßig blockiert. Dies verhindert, dass der Kunde aus Versehen die Datei öffnet und sein System infiziert.</p> <p>Die Information, dass Malware gefunden wurde, wird jetzt in einem Slide-Up angezeigt und nicht mehr in einem separaten Fenster. Das Slide-Up bietet ein One-Click Removal</p>



		<p>der Malware. Dies bedeutet, dass die Malware mit einem Klick entfernt werden kann. Außerdem wird die Malware nicht mehr nur vom System entfernt. Das System selber wird ebenfalls repariert und der Schaden, der von der Malware angerichtet wurde, wird behoben.</p>
<p>Avira AntiVir, Version 10 (alle Produkte)</p>	<p>Generische Reparatur</p>	<p>Malware entdecken und entfernen ist eine Sache, Schäden zu reparieren, die die Malware möglicherweise verursacht hat, eine ganz andere. Avira bietet jetzt eine neue Art, das System zu reparieren und es in seinen früheren Zustand zu versetzen. Was normalerweise gemacht wird, ist Reparaturskripte zu nutzen, um das System zu reparieren. Avira macht dies auch. Aber zusätzlich zu diesem Skript-basierten Ansatz bietet Avira jetzt auch eine generische Reparatur. Diese generische Reparatur kann das System selbst dann reparieren, wenn kein Reparaturskript zur Verfügung steht.</p>
<p>Avira AntiVir, Version 10 (alle Produkte)</p>	<p>Mehrfachauswahl in der Quarantäne</p>	<p>In der Quarantäne ist es mit der neuen Version möglich, mehrere Objekte auf einmal auszuwählen und diese beispielsweise zu prüfen oder wieder herzustellen.</p>
<p>Avira AntiVir, Version 10 (alle Produkte außer Avira AntiVir Personal)</p>	<p>SMTP-Fußzeile</p>	<p>Kunden können jetzt zu jeder unverschlüsselten Email, die per SMTP (ausgehend) verschickt wird und vom MailGuard geprüft wurde, eine Fußzeile (Footer) hinzufügen.</p> <p>Mit dieser Option kann eine Standard-Fußzeile von MailGuard eingefügt werden. Diese sagt hauptsächlich, dass die entsprechende Email von AntiVir MailGuard gescannt wurde. Ebenso sind die Version der Engine und der VDF enthalten, mit denen die Mail gescannt wurde. Der Nutzer kann auch einen selbstdefinierten Text einfügen. Wenn beide Optionen aktiviert sind, wird die selbstdefinierte Fußzeile vor die Fußzeile des MailGuards gesetzt.</p>

<p>Avira AntiVir, Version 10 (alle Produkte)</p>	<p>Update ist jetzt ein separater Eintrag in der Konfiguration</p>	<p>Um sicherzustellen, dass das System ein sehr hohes Sicherheitsniveau behält, ist es für den Nutzer am wichtigsten, regelmäßig Updates für das Produkt wie auch die Engine und Virendefinitionsdateien durchzuführen.</p> <p>Deswegen ist das Update jetzt ein separater Eintrag im Konfigurationsmenü und der vormals verfügbare standardmäßige Update-Job im Planer wurde entfernt.</p> <p>Standardmäßig lädt das Produkt jetzt alle Updates herunter und installiert diese. Der Nutzer wird alle 120 Sekunden daran erinnert, wenn ein Neustart des Systems notwendig ist. Das Update nutzt eine bestehende Netzwerkverbindung, um sich mit dem Webserver zu verbinden. Diese Einstellungen können vom Nutzer geändert werden, wenn er beispielsweise ein Update übers Intranet durchführen will.</p>
<p>Avira AntiVir, Version 10 (alle Produkte)</p>	<p>Auszulassende Prozesse beim Guard: Nutzung des Wildcard-Zeichens (*) und Namen mit mehr als 15 Buchstaben</p>	<p>Beim Guard ist es jetzt möglich, bestimmte Prozesse und Dateiobjekte vom Prüfen auszunehmen. Mit der Version 10 können Prozess- / Datenobjekte mit mehr als 15 Buchstaben hinzugefügt werden. Es ist jetzt ebenso möglich, Wildcards (*) zu benutzen und die Prozess- / Dateinamen mit dem kompletten Pfad.</p>
<p>Avira AntiVir, Version 10 (alle Produkte 64-Bit)</p>	<p>Rootkit-Erkennung jetzt auch für 64-Bit-Systeme verfügbar</p>	<p>Die Erkennung von Rootkits, die bis jetzt nur für 32-Bit-Systeme verfügbar war, ist jetzt in der Version 10 ebenfalls für 64-Bit-Systeme verfügbar.</p>
<p>Avira AntiVir, Version 10</p>	<p>Mehr Konfigurationsmöglichkeiten im Standard-</p>	<p>In der Version 10 der AntiVir-Produkte wurde eine Reihe von Konfigurationsoptionen von der Expertenkonfiguration in die Standardkonfiguration verschoben. Es ist jetzt</p>

(alle Produkte)	Modus	also möglich, das Produkt zu einem großen Teil in der Standardkonfiguration einzurichten. So bleibt die Expertenkonfiguration für die Situationen, in denen eine sehr spezifische Einstellung des Produktes notwendig ist.
Avira AntiVir, Version 10 (alle Produkte)	<input checked="" type="checkbox"/> Expressinstallation	Avira AntiVir bietet jetzt eine neue Expressinstallation, die es ermöglicht, die Produkte sehr schnell zu installieren. Wenn die „Expressinstallation“ ausgewählt wird, braucht es nur noch drei weitere Klicks, um das Produkt zu installieren.
Avira AntiVir, Version 10 (alle Produkte)	Produkt empfehlen	Nutzer, die ihre Freunde, Verwandte oder andere Leute auch an der Avira Familie teilhaben und sie so von einer der besten Sicherheitslösungen profitieren lassen wollen, können dies jetzt sehr einfach tun und daraus sogar noch Nutzen ziehen. Avira AntiVir ermöglicht es jetzt, anderen Nutzern ein Produkt zu empfehlen. Dazu müssen Nutzer nur auf den Eintrag „Produkt empfehlen“ im Menü klicken, und sich in ihrem Avira Kundenkonto anmelden.
Avira AntiVir, Version 10 (alle Produkte)	Verbessertes Slide-Up-System <input checked="" type="checkbox"/>	Die Slide-Ups, die das Produkt zeitweise auslöst, wurden verbessert und haben jetzt einen Schließen- wie auch Minimier-Button in der rechten oberen Ecke integriert. Wenn das Slide-Up minimiert wird, gibt es ein zusätzliches Icon in der Taskleiste, mit dem das Slide-Up wieder vergrößert werden kann.
Avira Premium Security Suite, Version 10	Kinderschutz mit Begrenzung der Internetnutzung	Avira AntiVir Premium Security Suite bietet einen Kinderschutz, um Kinder davor zu schützen, auf Webseiten zu surfen, die für Kinder oder Jugendliche nicht geeignet sind. Der Kinderschutz bietet jetzt auch die Möglichkeit, Gesamtzeiten zu definieren, in denen Kinder das Internet nutzen können. Die Nutzungszeit kann auf monatlicher, wöchentlicher oder täglicher Basis begrenzt werden. Die täglichen Einstellungen erlauben ebenfalls unterschiedliche Nutzungszeiten für Wochenenden oder unter der Wo-

		<p>che (Schultage). Mehrere Perioden für einen Tag können auch festgelegt werden. Der Kinderschutz ist jetzt auch wesentlich prominenter im Produkt platziert und steht als separates Modul in der Konfiguration und im Control Center zur Verfügung.</p>
	Kinderschutz jetzt als separates Modul	<p>Der Kinderschutz wird jetzt als separates Modul im Control Center und in der Konfiguration dargestellt.</p>
Avira AntiVir Professional, Version 10	Integrierte Desktop-Firewall	<p>Avira Antivir Professional, Version 10, kommt mit einer integrierten Desktop-Firewall, die es ermöglicht, den ein- und ausgehenden Netzwerkverkehr zu überprüfen und zu steuern.</p> <p>Bei einer Neuinstallation muss eine benutzerdefinierte Installation gewählt und die Firewall explizit zu den Modulen hinzugefügt werden, die installiert werden sollen. Die Firewall wird nicht installiert, wenn die voreingestellte Expressinstallation durchgeführt wird.</p> <p>Wenn ein Produkt-Upgrade von einer Vorgänger-Version durchgeführt wird muss die Installation über die Windows Änderungsinstallation durchgeführt werden.</p> <p>Die Avira Firewall ist eine regelbasierte Firewall mit unterschiedlichen Regeln für Adapter und Applikationen. Applikationsregeln können pro User definiert werden. Sie können mit „Erlauben“, „Fragen“ und „Ablehnen“ als mögliche Aktionen als Grundeinstellungen definiert werden. Es gibt für die Applikationsregeln ebenfalls erweiterte Einstellungen, die eine detaillierte Definition der Regeln für den Typ „Verkehr“ oder „Abhören“ erlauben.</p> <p>Die Firewall ist ein selbstlernendes Modul – immer wenn keine Regel für eine Applikation definiert ist, fragt ein Pop-Up nach, wie mit der Applikation verfahren werden soll (Erlauben oder Ablehnen). Es ist auch möglich, direkt aus dem Pop-Up eine Regel ein-</p>

		<p>zurichten. Um die Anzahl an Pop-Ups zu minieren, gibt es eine Liste von vertrauenswürdigen Herstellern, deren Applikationen nicht von der Firewall überwacht werden. Diese Hersteller können aus der Liste entfernt werden, wenn die Firewall ihre Applikationen überwachen soll. Es ist auch möglich, einer Applikation einen sogenannten privilegierten Modus zu erteilen, so dass diese nicht mehr von der Firewall überwacht wird. Benachrichtigungen werden versandt, wenn die Firewall Portscan oder Flooding entdeckt, oder wenn eine Applikation oder IP blockiert wurde. Die Firewall bietet ebenfalls einen automatischen Game-Mode (in dem Pop-Ups verhindert werden wenn gespielt wird).</p> <p>Es ist ebenfalls möglich, für jeden Adapter separat Regeln einzurichten. Es können Regeln für den eingehenden wie auch ausgehenden Netzwerkverkehr eingerichtet werden. Eine große Anzahl von vordefinierten Regeln und Templates macht es einfach, neue Regeln hinzuzufügen, wie zum Beispiel eine bestimmte IP-Adresse zu blockieren, VPN-Verbindungen zu erlauben oder ähnliches.</p> <p>Die einfachste Möglichkeit, ein Sicherheitsniveau für die Firewall zu definieren ist den Schieberegler im Firewall-Tab des Control Centers zu benutzen und diesen auf das benötigte Sicherheitsniveau zu setzen.</p> <p>Die Firewall kann ebenfalls über das Avira Security Management Center zentral verwaltet werden. Firewall-Einstellungen können entweder für die gesamte Sicherheitsumgebung oder für bestimmte Gruppen innerhalb der Sicherheitsumgebung definiert werden. Applikationen können zentral blockiert oder erlaubt werden. Generische Adapterregeln für bestimmte Arten von Adaptern wie zum Beispiel „Drahtlos“ oder „Einwahl“ können ebenfalls definiert werden. Die Firewall berichtet natürlich über alle Ereignisse und Zwischenfälle an die SMC, so dass eine kontinuierliche Überwachung</p>
--	--	---

		der Firewall-Aktivitäten auf allen administrierten Clients möglich ist.
Avira AntiVir Professional, Version 10	Umstrukturierung der Konfiguration von Emailbenachrichtigungen	<p>Die Konfiguration von Email-Benachrichtungen wurde jetzt vom Knoten „Email“ der allgemeinen Konfiguration in den Bereich Warnungen verschoben.</p> <p>Emailwarnungen können jetzt für den Guard, Scanner und den Updater separat konfiguriert werden.</p> <p>Der Inhalt dieser Warn-Emails kann individuell festgelegt werden. Das Produkt bietet eine Reihe von Variablen, wie zum Beispiel Engine- und VDF-Version, die ausgeführte Aktion nach der Erkennung oder die Anzahl der geprüften Dateien und so weiter, die in den Vorlagen benutzt werden können. Das Produkt wird diese dann mit den tatsächlichen Werten ersetzen, wenn solche Warnungen versandt werden.</p> <p>Optional kann auch das Logfile an jede dieser Warnemails angehängt werden.</p>
Avira AntiVir Professional, Version 10	Konfigurationsprofile <input type="checkbox"/>	<p>Konfigurationsprofile wurden um eine neue Regel erweitert, die es dem User jetzt ermöglicht, eine Regel basierend auf der IP-Adresse und Netzwerkmaske zu definieren.</p> <p>Diese Regel greift immer dann, wenn der standardmäßige Gateway die IP-Adresse und Netzwerkmaske hat, die in der Regel definiert wurde.</p>
Avira AntiVir Server Windows, Version 10	Alle Ereignisse löschen	<p>Es ist jetzt möglich, alle ausgewählten oder alle Ereignisse aus der Ereignisdatenbank zu löschen. Dazu muss nur zum Ereignisknoten gegangen werden, bestimmte oder alle Events markiert werden und dann auf das „Löschen“-Icon in der Symbolleiste geklickt werden. alternativ kann auch die „Löschen“-Aktion vom Menü ausgewählt werden, das über die rechte Maustaste erscheint.</p>

	Shell Extension Support	Avira AntiVir Server ermöglicht es jetzt, Dateien oder Verzeichnisse direkt aus dem Windows Explorer heraus zu prüfen, in dem einfach der Eintrag markiert wird und per Rechtsklick der Prüflauf des Servers angestoßen wird.
	Offline Scanner für VMWare Images	<p>Avira AntiVir Server Windows bietet jetzt die Möglichkeit, auch VMWare Images, die offline sind, auf mögliche Infizierungen mit Viren zu prüfen.</p> <p>Die Prüfung der VMWare Images, die offline sind, wird über ein besonderes Profil im Produkt geregelt. Hierzu muss nur das entsprechende Icon in der Navigationsleiste ausgewählt werden und per rechtem Mausklick den Menüeintrag „neues VMWare-Profil erstellen“ ausgewählt werden.</p> <p>Im folgenden Dialog können die entsprechende VMX-Datei ausgewählt werden. Die VMX-Datei enthält die Information über die VMDK-Datei (die das Image selber ist), die dann gescannt wird.</p> <p>Es ist ebenfalls möglich, Aktionen vor oder nach dem Prüfen auszuwählen. Diese Aktionen werden dadurch definiert, dass ein VB-Skript benutzt wird oder eine .exe-Datei eingefügt wird.</p> <p>Es gibt ebenfalls die Möglichkeit, VMWare Images als nur lesbare Dateien einzurichten, was bedeutet, dass diese Images nur geprüft, aber nicht repariert werden.</p>
	Benutzerdefinierte oder Expressinstallation	<p>Wie auch die AV 10 Professional, bietet jetzt der AV 10 Server die Möglichkeit, zwischen einer Express- oder benutzerdefinierten Installation zu wählen.</p> <p>Wenn der Nutzer die Expressinstallation ausgewählt hat, benötigt er nur noch drei weitere Klicks, um die Installation abzuschließen. Der Expressinstallation schließt sich ein Konfigurationsassistent an, der es ermöglicht, grundlegende Einstellungen wie</p>

		<p>Heuristik, Emailverbindungen, etc. vorzunehmen.</p> <p>Die benutzerdefinierte Installation ist dann notwendig, wenn der Nutzer die Avira AntiVir Rootkit-Erkennung, das Scannen von Offline VMWare Images und den Shell Extension Support (als Möglichkeit, Dateien / Verzeichnisse direkt aus dem Windows Explorer zu prüfen) mit installieren möchte. Der benutzerdefinierten Installation folgt ebenfalls ein Konfigurationsassistent.</p>
	<p>Planer: Starten / Beenden von Aufgaben; neue Intervall Option „wöchentlich“</p>	<p>Der Planer erlaubt es jetzt, Aufgaben zu starten und anzuhalten, indem sie markiert werden und eine passende Aktion aus dem Menü der rechten Maustaste ausgewählt wird.</p> <p>Die zusätzliche Planer-Option „wöchentlich“ wurde in den Planer integriert: es ist jetzt möglich, Aufgaben hinzuzufügen, die automatisch zu einer bestimmten Uhrzeit an einem bestimmten Tag oder mehreren bestimmten Tagen ausgeführt werden.</p>
	<p>Terminal Server-Unterstützung: ermöglichen von On-Demand-Prüfungen des Ordners „Eigene Dateien“ aus dem Infobereich rechts unten</p>	<p>Wenn der Server im Terminal Server-Modus ist, ist es jetzt auch möglich, direkt aus der Taskleiste heraus (Infobereich) Dateien zu prüfen.</p> <p>Diese Funktionalität ist profil-basiert: der Nutzer kann sein Profil „Eigene Dateien“ auswählen und es prüfen lassen.</p>
	<p>Integrierte WMI-Unterstützung</p>	<p>Wie auch die AV Windows-Desktop-Produkte unterstützt der Server jetzt die WMI (Windows Management Instrumentation) Datenbank.</p> <p>Die entsprechende Option ist Teil der Einstellungen des „Allgemeines“-Knotens.</p> <p>Die Windows Management Instrumentation (WMI) bietet eine starke und sehr flexible</p>

		<p>Administrationsoberfläche für Server-Administratoren.</p> <p>WMI ist praktisch eine Betriebssystemoberfläche innerhalb des Windows-Betriebssystems mittels welchem administrierte Komponente (Applikationen oder Applikationsmodule) Informationen und Benachrichtigungen liefern.</p> <p>WMI ermöglicht es Netzwerkadministratoren Informationen an Arbeitsplätzen, auf Servern, in Applikationen und Netzwerken abzufragen und festzulegen. So können diese Komponenten lokal und remote kontrolliert und verwaltet werden.</p> <p>WMI gestattet Skriptsprachen wie VBScript oder Windows PowerShell. WMI ist in Windows 2000 und neueren Betriebssystemen vorinstalliert.</p> <p>Der AV Server unterstützt jetzt WMI mit unterschiedlichen Funktionen. Er bietet eine Reihe Informationen für den WMI wie zum Beispiel Produktinformation, Statusinformation, Lizenzinformation und Information vom Guard, Scanner, Updater, von Ereignissen, vom Planer, der Konfiguration und eine Ereignisbenachrichtigung.</p> <p>Diese WMI-Information kann dann vom Administrator dazu genutzt werden, um</p> <ul style="list-style-type: none"> ▪ Statistische Informationen zu gewinnen ▪ AntiVir Server in eigene Administrationslösungen zu integrieren ▪ Ein eigenes Alarmsystem zu etablieren.
	<p>Verbesserte Email-Warnungen</p>	<p>In Version 10 von Antivir Server können Nutzer jetzt die Texte für Email-Warnungen des Guards, Scanners und Updaters bearbeiten.</p> <p>Das Produkt bietet eine Reihe von Variablen, wie zum Beispiel Engine- und VDF-Version, die ausgeführte Aktion nach der Erkennung oder die Anzahl der geprüften</p>

		<p>Dateien und so weiter, die in den Vorlagen benutzt werden können. Das Produkt wird diese dann mit den tatsächlichen Werten ersetzen, wenn solche Warnungen versandt werden.</p> <p>Optional kann für Email-Warnungen des Scanners und Updaters auch das Logfile an jede dieser Warnemails angehängt werden.</p>
	Verbesserter Updater	Die Möglichkeit, bei der Festlegung der Updater Proxy-Optionen auch die Windows Systemeinstellungen zu wählen, wurde entfernt.

AVIRA SECURITY MANAGEMENT CENTER

Produkt	Funktion	Beschreibung
<p>Avira Security Management Center</p>	<p>SSL-Zertifikatsmanagement</p>	<p>Eine sichere Kommunikation zwischen administrierten Clients und dem Server ist essentiell für ein Managementsystem wie die SMC. Es muss sichergestellt sein, dass nur autorisierte Kommunikationsparteien Informationen lesen oder modifizieren können. Zusätzlich muss jede Kommunikationspartei die wahre Identität seines Kommunikationspartners verifizieren.</p> <p>Dies bedeutet, dass, bevor irgendeine Art von Information ausgetauscht wird, der Client die wahre Identität des Servers überprüfen muss und der Server die des Clients. Dann erst können die Kommunikationsparteien anfangen, verschlüsselte Informationen auszutauschen.</p> <p>SSL bietet eine sichere Kommunikation durch Datenverschlüsselung und Client- und Server-Authentifizierung.</p> <p>Eine sichere Kommunikation in SSL basiert auf zwei Prinzipien: die Vertraulichkeit eines persönlichen Schlüssels jeden Kommunikationspartners und Vertrauen in die Gültigkeit der ausgetauschten Zertifikate.</p> <p>Vertrauen in die Zertifikate wird durch eine vertrauenswürdige Zertifizierungsstelle (Certificate Authority (CA)) hergestellt, die die ausgestellten Zertifikate signiert und ihre Echtheit garantiert. Jede Einheit, die sich mit ihrem persönlichen Schlüssel authentifizieren will, muss gewährleisten, dass nur sie Zugang zu diesem Schlüssel hat.</p>

		<p>In der SMC kann nur der private Schlüssel des SMC-Servers an einem sicheren Ort gespeichert werden. Jeder andere Schlüssel (Agent oder Frontend) kann nicht sicher gespeichert werden, weil sie über das gesamte Netzwerk hinweg genutzt werden.</p> <p>Um eine sichere Kommunikation zwischen dem SMC Server und allen administrierten Clients zu gewährleisten, bietet die neue Version 2.5 der SMC ein Tool, das es Kunden ermöglicht, ein „certificate sign request (CSR)“ (also einen Antrag auf Erstellung eines Zertifikates) für den SMC Server zu erstellen. Zusammen mit diesem CSR kann das Tool ebenfalls einen persönlichen Schlüssel für den SMC Server erstellen. Der Kunde muss diesen persönlichen Schlüssel an einem sicheren Ort aufbewahren und den CSR zu einer vertrauenswürdigen Zertifizierungsstelle schicken, um ihn signieren zu lassen.</p> <p>Dieses Tool ist nicht Teil der SMC-Oberfläche, sondern muss über das Installationsverzeichnis des SMC Servers gestartet werden. Hier muss nach der “SSLCertRequester.exe” gesucht werden, um das Programm zu starten und um das CSR (certificate sign request) wie auch den persönlichen Schlüssel für den SMC Server zu generieren.</p> <p>Nachdem der Kunde das signierte Zertifikat von der Zertifizierungsstelle (Certificate Authority (CA)) bekommen hat, muss das Zertifikat und der persönliche Schlüssel im SSL Directory des SMC Servers gespeichert werden.</p> <p>Es ist notwendig, dass das Serverzertifikat und der persönliche Schlüssel des Servers in einer Datei sind. Dies kann auch mit der “SSLCertRequester.exe” getan werden, die die Option „Ein signiertes Zertifikat mit privatem Schlüssel importieren“ bietet.</p> <p>Das SSL-Zertifikat, das der SMC Server zu den Clients sendet, ist von der CA signiert. Teil des SSL-Authentifizierungsprozesses ist, dass der Client überprüfen muss, dass die CA, die das Zertifikat signiert hat, eine CA ist, der der Client vertraut.</p>
--	--	---

		<p>Deswegen werden die SMC Clients mit einer CA-Datei ausgestattet, die die Zertifikate der bekanntesten CA (eine CA wird ebenfalls durch ihr Zertifikat identifiziert) enthält. Wenn der User sein Zertifikat von einer dieser CAs hat signieren lassen, vertraut der Client automatisch diesem CA und der Authentifizierungsprozess wird fortgesetzt. Diese vorgegebene Liste ist nicht Kunden-spezifisch und kann sehr einfach über die Client-Software verteilt und aktualisiert werden.</p> <p>Wenn ein User nun individuelle Server-Zertifikate nutzen will, muss er einfach den oben erklärten Schritten folgen und die Server-Authentifizierung für die Agents aktivieren.</p> <p>Dies wird erreicht, in dem die Agents entsprechend konfiguriert werden, also im Konfigurationsdialog des Agents die Option „Server-Authentifizierung anfordern“ zu aktivieren.</p>
	<p>Automatische Synchronisierung mit ADS / LDAP</p>	<p>Die Vorgängerversion 2.4 der SMC hat eine manuelle Synchronisation der Sicherheitsumgebung mit ADS / LDAP ermöglicht.</p> <p>Die neue Version 2.5 kann jetzt die Sicherheitsumgebung automatisch mit ADS / LDAP synchronisieren.</p> <p>Beim Rechtsklick auf den Knoten Sicherheitsumgebung muss der Untereintrag „Synchronisierung planen“ gewählt werden. Es muss nur dem Assistenten gefolgt werden, um eine Aufgabe zu erstellen, die dem System sagt, wann es die SMC mit dem ADS / LDAP synchronisieren soll. Folgende Optionen sind möglich: einmal, stündlich, täglich, wöchentlich, monatlich, alle (Intervall zu definieren).</p> <p>Wenn einmal eine Aufgabe zur Synchronisation erstellt worden ist, wird diese im Knoten Sicherheitsumgebung aufgelistet. Wenn „Ansichten / Synchronisierungs-Tasks“</p>

		ausgewählt wird, werden diese Aufgaben separat in einer Ergebnisliste aufgeführt.
	Sicherheitsrichtlinien – automatische Installation der Produkte auf neuen PCs	<p>Wenn ein neuer Computer in eine bestehende Gruppe in der Vorgängerversion 2.4 eingefügt wurde, musste der User manuell sicherstellen, dass die richtigen Produkte auf diesem Knoten installiert werden.</p> <p>Die neue Version 2.5 bietet jetzt die Möglichkeit, ein solches Produkt automatisch zu installieren, wenn ein neuer Computer in die Sicherheitsumgebung oder in eine bestimmte Gruppe in der Sicherheitsumgebung eingefügt wird.</p> <p>Die Gruppe, für die eine solche Sicherheitsrichtlinie definiert werden soll, muss markiert werden und dann über einen Rechtsklick „Installation / Produkte“ gewählt werden. Zwei Optionen ermöglichen es, entweder die Einstellungen eines übergeordneten Knotens zu vererben oder es für diese bestimmte Gruppe zu aktivieren. Dann werden die Produkte aus einer Liste ausgewählt, die automatisch installiert werden sollen.</p> <p>Es kann auch sichergestellt werden, dass der Agent automatisch installiert wird, wenn er noch nicht auf dem Zielsystem installiert ist. Es gibt ebenfalls eine Option, automatisch Produkte zu deinstallieren, die nicht auf der Liste ausgewählt sind.</p>
	Internet Update Manager jetzt in die SMC GUI integriert	<p>Das Internet Update Manager-Interface ist jetzt in die Benutzeroberfläche des SMC Frontends integriert.</p> <p>Dies ist keine kosmetische Verbesserung, sondern bietet der SMC eine Reihe von nützlichen neuen Funktionalitäten.</p> <p>So können jetzt mehr als nur ein IUM Server zur SMC hinzugefügt und separat konfiguriert werden.</p> <p>Der Administrator kann dann hergehen und bestimmte IUM Server-Instanzen zu be-</p>

		<p>stimmten Nutzergruppen zuordnen, so dass diese ihre Updates von einem bestimmten IUM Server beziehen.</p> <p>Um dies zu tun, muss die entsprechende Gruppe markiert werden, aus dem Menü, das sich mit einem Rechtsklick öffnet „automatisches Update“ ausgewählt werden und dann der IUM aus dem Untermenü ausgewählt werden, der der Gruppe zugeordnet werden soll. In derselben Art und Weise kann eine Gruppe einem IUM Server, der als Update-Testserver konfiguriert worden ist, übertragen werden.</p> <p>Der IUM kann auch so eingestellt werden, dass er automatisch IUM Service Updates installiert und automatisch die angeschlossene SMC über neue Updates informiert.</p>
--	--	---

AVIRA ANTIVIR UNIX

Produkt	Funktion	Beschreibung
<p>Avira AntiVir Professional/Server (Unix)</p>	<p>Verschicken von SNMP Traps</p>	<p>SNMP Traps (Simple network management protocol) sind eine Möglichkeit, den Status des Systems und der Netzwerkdienste zu überwachen.</p> <p>Mit der neuen Version der Professional / Server wird der Guard in der Lage sein, SNMP Traps zu verschicken, so dass die Professional und Server mit großen Software-Management-Tools überwacht werden können.</p> <p>Traps werden in den folgenden Fällen versandt:</p> <ul style="list-style-type: none"> ▪ Änderung des Status des Guards ▪ Meldung, wenn der Guard nicht richtig gestartet oder neugestartet werden kann ▪ Meldung, wenn ein Teil der Software aktualisiert wurde (hier eingeschlossen VDFs) ▪ Viren-Alarme ▪ Wichtige Ergebnisse von Prüfläufen (optional) <p>Diese neue Funktionalität, SNMP Traps zu verschicken, ist nicht standardmäßig aktiviert, sondern muss von Nutzern entweder über die Kommandozeile oder über die entsprechenden Konfigurationsdateien (avguard und avscan) aktiviert</p>

		<p>werden.</p> <p>Bitte beachten:</p> <p>SNMP Traps können für On-Demand- und On-Access-Prüfläufe separate konfiguriert werden.</p> <p>SNMP Traps stehen für alle unterstützten Linux- und Solaris-Plattformen zur Verfügung.</p>
	<p>Scheduled Scanning</p>	<p>In der neuen Version ist es ebenfalls möglich, Prüfläufe zu planen und zu festgelegten Zeiten oder in festgelegten Intervallen automatisch durchführen zu lassen (sog. Scheduled scanning.)</p> <p>Diese Funktionalität nutzt eine interne Datenbank (die für das gesamte Produkt gültig ist), die alle geprüften Dateinamen (zusätzliche Information wie das Datum des Prüflaufes, eine interne Statusinformation, Prüfergebnisse oder ähnliches inbegriffen) in den Cachespeicher aufnimmt. Ein Prozess durchläuft die Verzeichnisstruktur und aktualisiert daraufhin die Datenbankeinträge.</p> <p>Die geplanten Prüfläufe nutzen diese Datenbank, um die Dateien, die gescannt werden können, zu priorisieren. Es ist auch möglich, den Scanvorgang zu stoppen und ihn an dem Punkt wieder neu zu starten, wo er angehalten wurde. Abfragen innerhalb der Prüfergebnisse, wie zum Beispiel Alarme oder ausgelöste Warnungen, können ebenfalls durchgeführt werden.</p> <p>Beide Scans können selbstverständlich auch über Cron Jobs geplant werden.</p> <p>Diese Funktionalität wird auch von der SMC unterstützt.</p>

	<p>Konfigurierbare Aktionen bei Warnmeldungen</p>	<p>In der Vorgängerversion konnte der Nutzer Alarmaktionen definieren und einige Einstellungen ändern, um zu definieren, ob ein Alarm ausgelöst werden soll oder nicht.</p> <p>Es wurden auch bestimmte Aktionen als Antwort auf bestimmte Ergebnisse beim Scannen von Archiven eingeführt, so dass der Anwender bei einer Warnmeldung z.B. definieren konnte, ob die Meldung ignoriert werden soll, ob der Alarm ausgelöst werden soll, die betreffende Datei geblockt werden soll oder ob eine komplette Aktionskette ausgeführt werden soll).</p> <p>Dieses neue Release verbesserte diese Funktionalität weiter und ermöglicht es jetzt, spezielle Aktionen für fast jedes Scan-Ergebnis festzulegen. Dies sind insbesondere:</p> <p>1) in der Kommandozeile:</p> <pre>--archive-max-size-action= --archive-max-recursion-action= --archive-max-ratio-action= --archive-max-count-action= --scan-incomplete-action= --archive-encrypted-action= --archive-multivolume-action= --archive-unsupported-action=</pre>
--	---	---



		<pre>--archive-header-malformed-action= --archive-bomb-action= --tagged-suspicious-action= --scan-timeout-action= --archive-procerror-action= --scan-aborted-action 2) für Einstellungsdateien ScanIncompleteAction ArchiveEncryptedAction ArchiveMultiVolumeAction ArchiveUnsupportedAction ArchiveHeaderMalformedAction ArchiveBombAction TaggedSuspiciousAction ScanTimeoutAction ArchiveProcErrorAction ScanAbortedAction Mögliche Aktionen sind: keine, umbenennen, löschen, in die Quarantäne ver-</pre>
--	--	--

		<p>schieben.</p> <p>Diese Funktionalität wird auch von der SMC unterstützt.</p>
	Verdächtige Dateien in die Quarantäne schieben	<p>Dateien, die von der heuristischen Erkennung als verdächtig markiert wurden, können jetzt in die Quarantäne verschoben werden.</p> <p>Siehe auch „Konfigurierbare Aktionen bei Warnmeldungen“</p>
	Ausnahmen bei On Access-Scans definieren	<p>Zum Release Q1 2009 wurden für On Demand Scans bereits PCRE-Ausnahmen eingefügt, während diese Funktionalität für den On Access-Scanner bislang gefehlt hat.</p> <p>Dies wurde jetzt ergänzt, so dass Nutzer jetzt auch hier Dateien vom Prüfen ausschließen können, basierend auf dem Dateinamen oder regular expressions oder einer Dateiendung wie beispielsweise .exe, .rar, .htm und so weiter.</p> <p>Ungültige Vorlagen werden abgelehnt und ausführliche Fehlermeldungen werden angezeigt.</p> <p>Die SMC unterstützt diese Funktionalität ebenfalls.</p>
	Professional / Server unterstützen jetzt die Run Modes des Avira Lizenzverfahrens	<p>Die Run Modes des Avira Lizenzierungsverfahrens werden jetzt unterstützt.</p> <p>Ebenso gibt es jetzt eine Begrenzung der Features abhängig von der Lizenz, besonders im Hinblick auf die Personal auf der einen Seite und Professional / Server auf der anderen Seite.</p>
	Begrenzung der Malware-Reports	<p>Es ist jetzt möglich, die Anzahl der Funde in einem Archiv oder einer Datei zu begrenzen. Wenn der dieser Grenzwert erreicht wird, wird eine Warnung ausge-</p>

	pro Archiv	löst und der Scan abgebrochen. Standardwert ist 100.
	Neueinführung der AVSCAN Authentifizierung / Kommunikation	Der Avscan-Authentifizierungsmechanismus, der im Q1-2009 Release implementiert wurde, fehleranfällig und nicht besonders sicher. Es wurde deswegen durch einen besseren Mechanismus ersetzt, der die Authentifizierung jetzt mit Unix Domain Sockets durchführt. Der Client erstellt ein Socket-File in seinem home directory. Die User-ID dieses Socket-Files wird genutzt, um den client zu authentifizieren.
	Produktspezifisches Installationsverzeichnis	Der Guard wird jetzt in das produktspezifische Installationsverzeichnis /usr/lib/antivir/guard installiert.
	Automatisches Produktupdate	Das SMC-Plug In für die Professional und Server unterstützt jetzt auch die Funktionalität der SMC, Produktupdates automatisch durchzuführen.
	Versionsinformation in den meisten Dateien	Da der Updater und andere Tools die Version von jedem Binary abrufen müssen, wurde die Versionsinformation zu jedem Binary und anderen Dateien, wie Dokumentation, Skripten, etc. hinzu gefügt.
	Ergänzte Integritätsprüfung des Programms	Jedes ausführbare Binary wird jetzt signiert und führt während des Startvorgangs eine Integritätsprüfung durch.