Avira Exchange Security 11

Kurzanleitung





# Inhaltsverzeichnis

1. Installation der "Avira Exchange Security"	. 4
2. Lizenzierung	. 6
3. Anlegen neuer Email Filter	. 7
4. Konfiguration der Email Filter	. 9
<ul> <li>5. Informationsspeicher-Scan-Job</li> <li>5.1 Aktivierung des Informationsspeicher-Scan-Jobs</li> <li>5.2 Informationsspeicher-Scan manuell starten</li> </ul>	<b>14</b> 14 15
6. Quarantänen	16
7. Quarantänesammelbenachrichtigungen	18
<b>8. Update-Einstellungen</b> 8.1 Update via Proxy Server	<b>20</b> 21
<ul> <li>9. Jobvorschläge</li> <li>9.1 Zusatz im Betreff entfernen</li> <li>9.2 Unerwünschte Dateianhänge blocken</li> <li>9.3 Advanced Spamfiltering mit separaten Quarantänen</li> <li>9.4 Empfänger automatisch zur Whitelist hinzufügen</li> </ul>	24 24 24 26 28
9.5 Passwortgeschützte Archive	29

# **Allgemeine Informationen**

Alle für die Installation erforderlichen Installationspakete sowie die Produkthandbücher im PDF-Format finden Sie zum Download auf unserer Internetseite.

### Hinweis

Für die unterschiedlichen MS Exchange Systeme werden unterschiedliche Installationspakete angeboten! Bitte achten Sie darauf, dass Sie das richtige Installationspaket (Exchange 2000/2003 oder 2007) verwenden. Für Informationen über die Cluster-Installation wenden Sie sich bitte an den Avira-Support.

# Systemvoraussetzungen

Es ist zu beachten, dass vor jeglicher Installation von "Avira Exchange Security 11", die Mindestsystemvoraussetzungen erfüllt sein müssen.

### Betriebssysteme (32-Bit / 64-Bit)

- Windows Server 2003 (einschließlich der aktuellen Service Packs und Patches)
- Windows Server 2008 (einschließlich der aktuellen Service Packs und Patches)
- Windows Server 2008 R2 (einschließlich der aktuellen Service Packs und Patches)

## **MS Exchange Server**

- MS Exchange Server 2007 SP1 Update Rollup 4 (64-Bit) (oder höher, d.h. SP2/SP3 inkl. aller aktuellen Rollups)

### RAM

Exchange Empfehlung & zusätzlich 64 MB

## Festplatte

• Mindestens 400 MB für die Installation

### Sonstiges

- CD-ROM-Laufwerk oder Netzwerkzugriff
- Microsoft .NET Framework 3.5
- 100 MB für Ereignisprotokollierung empfohlen
- Internetzugang, für das Update von Engines (Scan- und Antispam-Engine)



• Benutzerberechtigungen: Im Active Directory angemeldeter Benutzer mit vollem Lesezugriff auf das Active Directory.

### Betriebssysteme für Avira Exchange Management Konsole

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows XP Professional
- Windows Vista
- Windows 7

# 1. Installation der "Avira Exchange Security"

Nachdem Sie das Installationspaket von "Avira Exchange Security" heruntergeladen haben, starten Sie dieses bitte auf Ihrem "Microsoft Exchange Mailserver".

Im Laufe der Installation erscheint ein Fenster, in dem Sie die zu installierenden Komponenten auswählen können. Achten Sie darauf, dass hier sowohl die Management-Konsole als auch die Serverkomponenten ausgewählt sind.

🙀 Avira Exchange Security - InstallShield Wizard	×
Angepasstes Setup Wählen Sie die zu installierenden Features aus.	<b>RAVIRA</b>
Klicken Sie auf ein Symbol in der Liste, um die Art der Feature-	Installation zu ändern.
Avira Exchange Security 11.1 Avira Exchange Security Managemen Online-Hilfe Benutzerhandbuch Avira Exchange Security Serverkomp Avira Exchange Security Serverkomp Mail-Transport-Grabber X V LDIF-Modus	Feature-Beschreibung Dieses Feature benötigt 19MB auf Ihrer Festplatte. Es sind 2 von 3 Subfeatures ausgewählt. Die Subfeatures erfordern 241MB auf Ihrer Festplatte.
Installieren nach:	
InstallShield	Andern Weiter > Abbrechen

Nach Auswahl der zu installierenden Komponenten werden Sie nach einer bestehenden Konfiguration gefragt.

Dieses Fenster ist nur dann interessant, wenn bereits eine ältere Installation von "AntiVir Exchange" im Einsatz war und nun ersetzt wurde.



Zur Auswahl stehen hier drei mögliche Auswahlfelder:

• Neue lokale Konfiguration anlegen

Diesen Punkt wählen Sie dann, wenn keine bisherige Konfiguration besteht, oder es sich um eine Erstinstallation handelt.

## • Bisherige Konfiguration beibehalten

Hier legen Sie bei einer erneuten Installation fest, dass die bereits hinterlegten Konfigurationen beibehalten werden sollen. Die Datei *ConfigData.xml* muss sich hierfür im Installationsverzeichnis von Avira Exchange Security befinden.

## Pfad zur Konfiguration manuell angeben

Sollte sich die Konfiguration in einem anderen Verzeichnis befinden, kann hier der genaue Pfad mit angegeben werden.

### Hinweis:

Der hier hinterlegte Pfad kann im Anschluss nicht mehr geändert werden!

te wählen Sie die Konfiguration	2015	
Neue lokale Konfiguration	anlegen	
C Bisherige Konfiguration be	eibehalten	
C Pfad zur Konfiguration ma	anuell angeben	
C:\Program Files (x8	6)\Avira\Avira Exchange Security\C	onfig\ConfigData.xml

In den weiteren Schritten werden Sie nun gebeten einige administrative Voreinstellungen festzulegen. Diese beinhalten eine Emailadresse des zuständigen Administrators und einen eventuell vorhandenen Proxyserver für das Internet Update.

Diese Einstellungen werden während der Installation im Programm hinterlegt, können aber auch im Anschluss in der Konfigurationsdatei *savapi.ini* angepasst werden.

# 2. Lizenzierung

Während der Installation wird die Lizenzdatei abgefragt und korrekt eingebunden. Bei einem späteren Lizenzwechsel gehen Sie bitte wie folgt vor:

- Kopieren Sie die Datei *HBEDV.key*, welche Sie per Email erhalten haben, in das Installationsverzeichnis von Avira Exchange. Hier wurde bereits ein Verzeichnis mit dem Namen "License" angelegt, in welchem die Datei abgelegt werden muss. Das Verzeichnis "License" enthält bereits eine Datei mit dem Namen *oem.lic*, welche sich auch weiterhin dort befinden muss
- Nachdem Sie die Lizenzdatei in das entsprechende Verzeichnis kopiert haben, ist ein Neustart des Dienstes "Avira Exchange Security Control" erforderlich. Während des Neustarts erhalten Sie einen Hinweis, dass der Dienst "Avira Exchange Security" ebenfalls neu gestartet wird, bitte bestätigen Sie dies mit Ja



Um zu prüfen, ob die Lizenzdatei richtig eingespielt wurde, starten Sie die "Avira Exchange Security Management Konsole" und öffnen dort den Bereich: "Avira Monitor". Öffnen Sie nun die Eigenschaften Ihres Servers, um im folgenden Fenster die Lizenzinformationen zu prüfen:

Eigenschaften
SERVER1
Server Information
Configuration Information
<ul> <li>File: C:\Program Files (x86)\Avira\AntiVir Exchange\Config\ConfigData.xml</li> <li>Filetime: 2013-03-11T14:46:07</li> <li>Schema: 11.1.1.0</li> <li>Status: Configuration successfully running since 2013-03-11T15:19:54</li> </ul>
License Information
License: Avira Exchange Security License     Customer: Test-license_Avira_Support_Department     Version: 11.1*     Server: SERVER1.meinefirma.local     Mode: FULL     State: VALID     Valid until: 2014-01-01
15 Scan Information
Scannerbill state: Unioaded
OK Abbrechen ((herrschmen)



Hier sehen Sie nun Ihre Lizenzinformationen, die Werte *Mode: FULL* und *State: VALID* zeigen, dass die Lizenz richtig ausgelesen wurde und gültig ist. Sollte dies nicht der Fall sein, kontrollieren Sie bitte mit Hilfe der Textdatei *lic\_info.txt*, ob Sie die richtige Lizenzdatei verwendet haben. Wenden Sie sich bitte ggf. an den Avira Support und senden Sie uns die Lizenzdatei zur Kontrolle zu.

# 3. Anlegen neuer Email Filter

Direkt nach der Installation ist das Produkt bereits vorkonfiguriert. Eingehende Emails werden schon auf Viren geprüft und bei einem Fund in die Quarantäne verschoben. Um die Email-Filterung zu erweitern und weitere Jobs einzubinden, können Sie die bereits mitgelieferten Jobvorlagen verwenden.

Hier finden Sie vorkonfigurierte Jobs, die den bereits aktiven Virenscanner um eine Spamfilterung, oder einen Content- / Attachement-Filter erweitern.



Um einen Job Ihrer Wahl für die Filterung zu aktivieren, ziehen Sie diesen einfach per *Drag&Drop* in die "Mail-Transport-Jobs". Dort kann dieser dann aktiviert bzw. konfiguriert werden.

### Hinweis:

Sollten Sie nicht sicher sein, welcher Filter für Sie der Richtige ist, empfehlen wir Ihnen den "Advanced Spam Filtering" Job, welcher bereits mehrere Filtermethoden beinhaltet und daher eine gute Erkennungsrate liefert.

# *CAVIRA*

Andere Jobs filtern den Inhalt der Emails z.B. anhand von Fingerprints. Als Fingerprint bezeichnen wir das Muster der jeweiligen Datei. Diese Muster werden entweder über die Dateiendung oder über ein Binärmuster der entsprechenden Datei klassifiziert.

Zum Beispiel: *Basis-Konfiguration > Utility-Einstellungen > Fingerprints > Images* 



Die einzelnen Dateimuster sind in Gruppen sortiert, so enthält z.B. die Gruppe Images eine Vielzahl bekannter Dateiendungen und Binärmuster.

Die Fingerprint-Gruppe "Images" wird nun einem Job zugeteilt. Dieser Job filtert eingehende Emails und überprüft, ob diese einen der genannten Fingerprints enthält.

Job Beispiel	Funktion
Blocke Bilddateien	Dieser Job greift auf die Fingerprint- Gruppe "Images" zu. Hier bekommt er die Information, was eine Bilddatei ist und woran er diese erkennen kann.
Blocke Videodateien	Das Prinzip der Fingerprints ist hier dasselbe wie bei den Bilddateien, le- diglich die Gruppe ist eine andere und damit sind auch die Dateimuster anders. Verwendete Gruppe: "Video"
Blocke Archive, außer ZIP-Dateien	Hier kommen zwei Filterrichtlinien zum Einsatz: die Fingerprint-Gruppe "Ar- chive", diese enthält alle bekannten Archivtypen und dient dem Job als Dateizuordnung. Der Fingerprint "Zip- Archive" ist jedoch in den Einstellungen dieses Jobs als Ausnahme deklariert.

# 4. Konfiguration der Email Filter

In Anbetracht dessen, dass die meisten Filter bereits vorkonfiguriert sind, ist eine Anpassung nicht zwingend erforderlich. Sollten Sie diese Standardeinstellungen nicht verwenden, können die Filter individuell angepasst werden.

Die Eigenschaften für die Konfiguration lassen sich mit einem Doppelklick auf den gewünschten Job öffnen.

#### Hinweis:

Der Zusatz [Avira checked], welcher im Betreff einer Email erscheint, wird durch den Job "Prüfen mit der Avira Scan Engine" hinzugefügt. Sollte dieser Zusatz nicht gewünscht sein, lässt er sich über die Eigenschaften des Jobs entfernen.

Zunächst ist jeder neue Job deaktiviert. Damit sie einen Job aktivieren, ändern Sie bitte die Einstellung im Reiter "Allgemeines" auf "Aktiv: **Ja"**.



Von der Grundeinstellung her wird jeder Job auf alle ein- und ausgehenden Emails angewandt. Um dies zu ändern und gegebenenfalls Black- / Whitelisten zu verwenden, wechseln Sie bitte in den Reiter "Adressen".



gemeines Adresse ▼ Emails an mehre	n   Bedingungen   Av	rira Scan Engine   Aktionen _ ch aufteilen
Absender/Empfäng	er Bedingungen:	E <u>r</u> weitert
Nachricht von:	Alle Absender/E	mpfänger 💌
A <u>d</u> ressiert an:	Alle Absender/E	mpfänger 💌

Über den Menüpunkt **Erweitert** ändert sich die Ansicht des Fensters und Sie haben nun die Möglichkeit, Adressen / Adresslisten als Ausnahme zu hinterlegen.

Eigenschaften von Prüfen mit der Avira Scan Engine	Eigenschaften von Prüfen mit der Avira Scan Engine
Allgemeines Adressen Bedingungen Avira Scan Engine Aktionen	Allgemeines Adressen Bedingungen Avira Scan Engine Aktionen
✓ Emails an mehrere Empfänger dynamisch aufteilen	Emails an mehrere Empfänger dynamisch aufteilen
Absender/Empfänger Bedingungen:	Absender/Empfänger Bedingungen:
Aktion wird ausgeführt	Aktion wird ausgeführt
bei folgenden "Absendern" (="from") Alle Absender/Empfänger	bei folgenden "Absendern" (="from") Alle Absender/Empfänger
gilt aber nicht für diese "Absender" Keine Adresse ausgewählt	gilt aber nicht für diese "Absender" Keine Adresse ausgewählt
und bei folgenden "Empfängern" (="to") Alle Absender/Empfänger	und bei folgenden "Empfängern" (="to") Alle Absender/Empfänger
gilt aber nicht für diese "Empfänger" Keine Adresse ausgewählt	gilt aber nicht für diese "Empfänger" Keine Adresse ausgewählt
OK         Abbrechen         Übernehmen	<u>DK</u> Abbrechen <u>Ü</u> bernehmen

Jede Email von extern oder an extern	Hier können Sie jedoch eigene
wird durch diesen Job überprüft.	Adressen oder Adresslisten
	hinzufügen, für welche der Job
	nicht gilt (z.B. eine Whitelist).

Wie bereits in der Bildbeschreibung zu erkennen ist, lassen sich die Adressbereiche anpassen. Durch einen einfachen Mausklick auf "Keine Adresse ausgewählt", im Bereich "gilt aber nicht für diese Absender", können Sie eine Adressliste hinzufügen.



Alle in dieser Adressliste hinterlegten Absender werden dann nicht mehr von diesem Job berücksichtigt, die Nachrichten kommen dann also in jedem Fall beim Empfänger an.

🛚 Adressen auswählen		_ 🗆 X
Adressen C Gruppen C Gruppen C Gruppen C Dynamische Gruppen C Dynamische Gruppen C Dynamische Gruppen C Gruppen C Gruppen Adressitien C G Avria Adressitien C Adressen C Adressen suchen	Eigene Adresslisten           Name         Email-Adresse           Ø Antispam: Blacklist         Ø Antispam: Newsletter Blacklist           Ø Antispam: Whitelist         Ø Antispam: Whitelist           Bearbeiten         Hinzufügen	
	Ausgewählte Adressen	
20	<u>QK</u> <u>Abbrechen</u>	

Falls Sie sich für eine der hier hinterlegten Listen entscheiden, ist unter Umständen eine Anpassung der Inhalte erforderlich.



Diese Anpassung kann im Anschluss über den Programmpunkt *Basis-Konfiguration* > *Allgemeine Einstellungen* > *Adresslisten* > *Antispam: Whitelist* durchgeführt werden.



Um festzulegen, was im Falle einer Klassifizierung als Spam/Virus durchgeführt werden soll, können Sie die Einstellungen im Bereich "Aktionen" anpassen. (*Richtlinien-Konfiguration > Mail-Transport-Jobs*) Hier haben Sie je nach Spam-Wahrschein-lichkeit unterschiedliche Möglichkeiten.

Eigenschaften von Prüfen auf Spam mit Avira Antispam 🔀	Niedrig X
Allgemeines Adressen Bedingungen Aktionen Server Details	Aktionen für niedrige Spam-Wahrscheinlichkeit:
Aktionen konfigurieren Spam-Wahrscheinlichkeit: Keine Zusatz im Betreff: Spam-Wahrscheinlichkeit: Niedrig [029] Miedrig Spam-Wahrscheinlichkeit: Mittel [3069] Mittel Spam-Wahrscheinlichkeit: Hoch [70100] Hoch	Standard:       Image: Antispam: Niedrig Mit Label: Spamkategorie: Niedrig ([VAR]spamvalue [/VAR])         Lösche Email       Absender/Empfänger zu Benutzerliste hinzufügen         Füge Zusatz im Betreff hinzu: [Spam- Wahrscheinlichkeit=[VAR]spamvalue:[/VAR]] am Anfang         Sende Benachrichtigung an Administrator         Sende Benachrichtigung an Alle Absender         Sende Benachrichtigung an Alle Empfänger
Erweiterte Konfiguration:          Definitive Kriterien       Kombinierte Kriterien         Schreibe Spam-Ergebnis in Exchange SCL Feld         Schreibe Spam-Ergebnis in Email-Header	Hinzufügen B C K Abbrechen Übernehmen

Der Reiter "Aktionen" ist für jeden Job separat zu konfigurieren. Änderungen sind immer nur für diesen einen Job wirksam.

# *CAVIRA*

Nachdem die Konfiguration abgeschlossen wurde, bestätigen Sie diese bitte zum Abschluss mit einem Klick auf **OK** und speichern Sie danach die Änderungen im Avira Exchange Security durch einen Klick auf das Diskettensymbol.

### Hinweis:

Ohne das Speichern der Änderungen werden diese nicht übernommen und sind daher wirkungslos. Dies gilt für alle Änderungen im Programm.

## • Definitive "Kein Spam" -Kriterien (Whitelist):

Beinhaltet Adressen aller bekannten Absender, die immer erlaubt sind und die eindeutig keinen Spam versenden. Dies sind im Prinzip alle regelmäßigen Kommunikationspartner und die Domänen von Kunden und Lieferanten. Je vollständiger diese Liste gehalten wird, desto weniger wird Ihr System mit unnötigen Prüfungen belastet.

## • Definitive "Spam-Kriterien" (Blacklist):

Beinhaltet Adressen aller Absender, die immer als Spam-Absender identifiziert werden. Die Standardkonfiguration enthält bereits eine Liste von bekannten Adressen. Sie können eigene zusätzliche Adressen definieren.

### • Kombinierte "Kein Spam" -Kriterien:

Die kombinierten Kriterien werden nur dann angewandt, wenn die definitiven Kriterien nicht zutreffend waren. Für die eigentliche Spam-Erkennung mit kombinierten Kriterien werden mehrere Analyse-Mechanismen (Kriterien-Untersuchungen) parallel durchgeführt und anschließend nach der Analyse der Email miteinander "verrechnet".

Zusätzlich ist hier eine Wortlistenerkennung für den Betreff und den Nachrichtentext hinterlegt. Die Wortlisten sind statisch, werden also nicht automatisch aktualisiert. Sie können diese Listen jedoch manuell anpassen. (*Richtlinien-Konfiguration > Mail-Transport-Jobs > Prüfen auf Spam mit Avira Antispam > Eigenschaften > Aktionen > Kombinierte Kriterien > Spam [Betreff]*)





# 5. Informationsspeicher-Scan-Job

Neben der Virenprüfung auf Transportebene (Email-Verkehr) ist Avira Exchange Security auch in der Lage, Daten im öffentlichen oder privaten Informationsspeicher von MS Exchange zu prüfen (z.B. Entwürfe). Dadurch dass der Informationsspeicher-Scan eine Servereinstellung ist, steht für jeden Server nur ein Informationsspeicher-Scan-Job zur Verfügung.

Grundsätzlich ist dieser Filter deaktiviert, er kann jedoch auf Wunsch aktiviert werden.

### Hinweis:

Nach dem Aktivieren/Deaktivieren des Informationsspeicher-Scan-Jobs kann es bis zu zwei Minuten dauern, bis der Exchange Store die Änderung registriert.

## 5.1 Aktivierung des Informationsspeicher-Scan-Jobs

Den Informationsspeicher-Scan-Job können Sie über folgenden Menüpunkt aktivieren: *Avira Exchange Security > Richtlinien-Konfiguration > Informationsspeicher-Jobs* > Doppelklick auf *Informationsspeicher auf Server.* 



genschaften von Allgemeines Opti	Informationsspeicher-S	can auf SERVER1	
Inform	Informationsspeicher-Scan auf SERVER1		
Aktiv:	© <u>J</u> a	C <u>N</u> ein	
Suche in diesen	Suche in diesen Informationsspeichern:		
Privater und Öff	entlicher Informationsspeiche	r T	
Virenprüfung:	C In Echtzeit (mit optionaler	Rescan-Zeitpunkten)	
	C Zeitgesteuert (Rescan in definierten Zeiträumen)		
Zeiträume für vo	Zeiträume für vollständigen Rescan:		
Name		Dauer	
Bearbeiten	n jedem Wochentagj	8 Stunden	
3	<u>o</u> k	<u>Abbrechen</u>	

In der Registerkarte "Allgemeines" aktivieren Sie mit **Ja** den Informationsspeicher-Scan. Mit Hilfe des Dropdown-Menüs können Sie auswählen, welcher der drei Informationsspeicher geprüft werden soll. (Privater Informationsspeicher/ Öffentlicher Informationsspeicher/Privater und Öffentlicher Informationsspeicher).

Zusätzlich haben Sie die Möglichkeit, den Suchlauf **In Echtzeit** oder **Zeitgesteuert** durchführen zu lassen. Bei der Auswahl einer zeitgesteuerte Virenprüfung, können Sie Zeiträume für die Virenprüfung festlegen.

Über die Registerkarten "Optionen", "Avira Scan Engine", "Aktionen" und "Details" können weitere Konfigurationen vorgenommen werden. Bestätigen Sie die Konfiguration mit einem Mausklick auf **Übernehmen** und anschließend auf **OK**.

## 5.2 Informationsspeicher-Scan manuell starten

Bei einen Start des Informationsspeicher-Scans werden sämtliche Elemente im Informationsspeicher erneut gescannt. Folglich kann die Prüfung zeit- und ressourcenintensiv sein. Es ist zu empfehlen einen manuellen Informationsspeicher-Scan zu Tagesrandzeiten durchzuführen.

Einen manuellen Scan können Sie im Menü Avia Exchange Security > Avira Monitor > Server > rechte Maustaste auf "Servername" > Eigenschaften > Informationsspeicher-Scan > Jetzt scannen durchführen.

# *CAVIRA*

# 6. Quarantänen

Avira Exchange Security verfügt über eine zentrale Quarantäne, welche über den Programmpunkt *Avira Monitor > Server > "Ihr Server" > Quarantänen* eingesehen werden kann. Nach der Installation sind im Produkt standardmäßig die wichtigsten Quarantänen vordefiniert. Ein Spamfilter überprüft die eingehenden Emails auf Viren und verschiebt sie bei einem Fund in die festgelegten Quarantänen. Zusätzlich zu den schon bekannten Quarantänen "Standard-Quarantäne" und "Infizierte Emails", sind zusätzlich folgende Quarantänen vordefiniert.

## • Informationsspeicher Quarantäne

Dies ist die Quarantäne des Informationsspeicher-Scanners und enthält Informationsspeicher-Dokumente. Im Allgemeinen handelt es sich bei diesen Dokumenten um Email-Anhänge oder um Elemente, die sich in öffentlichen Ordnern im Exchange befinden. In Abhängigkeit der Informationsspeicher-Job-Einstellungen sind die Dokumente

- virulent
- fehlerhaft (konnten nicht von der Avira Scan Engine geprüft werden)

## • Antispam: Niedrig

Diese Quarantäne enthält Emails der letzten Tage, die nur eine geringe Spamwahrscheinlichkeit aufweisen. Die Emails dieser Quarantäne müssen öfters überprüft werden. Bei Notwendigkeit muss der SPAM-Job angepasst werden. Zur Verbesserung der Klassifizierungsergebnisse, kann zum Beispiel der Spam-Absender Zur "Antispam: Blacklist" Adressenliste hinzugefügt werden.

## • Antispam: Mittel

In dieser Quarantäne befinden sich Emails der letzten Tage, die nicht eindeutig als "Spam" oder "NoSpam" klassifiziert werden konnten. Diese Quarantäne sollte regelmäßig nach falsch zugeordneten Emails ("False Positives") überprüft werden. Verwenden Sie hierzu die Quarantäne-Sammelbenachrichtigung, damit die Empfänger selbst ihre falsch zugeordneten Emails überprüfen.

Um die Anzahl der als "Mittel" eingestuften Emails so gering wie möglich zu halten, sollten Sie die Analyse dieser Emails in den SPAM-Jobeinstellungen berücksichtigen.

Zum Beispiel:

- Gewünschte Absender von Newslettern, in die "Antispam: Whitelist Newsletter" Adressenliste eintragen
- Ungewünschte Absender von Newslettern, in die "Antispam: Blacklist Newsletter" Adressenliste eintragen

### • Antispam: Hoch

Die Antispam Quarantäne "Hoch" enthält Emails der letzten Tage, die eine hohe Spamwahrscheinlichkeit aufweisen.



🔀 Avira Exchange Security		
Datei Aktion Ansicht ?		
🗇 🔿 🖄 🧟 📑 🔽 🖬		
Avira Exchange Security (*)     Sasis-Konfiguration     Migemeine Einstellungen	Name BADMAIL Antispam: Hoch	Anzahl Element 0 0
때 Proxyserver 같은 Adressisten 글 때 Vorlagen 같은 Avira Benachrichtigungen	Antispam: Mittel  Antispam: Niedrig  Infizierte Emails  Informationsspeicher-Quarantäne	0 0 0 0
Image: Avira Antispam Benachrichtigungen         Image: Informationsspeicher-Benachrichtigungen         Image: Rombinerte Benachrichtigungen         Image: Rombinerte Benachrichtistratistre Benachrichtistratistration	Standard-Quarantäne	0
Image: Server         Image: Server <t< td=""><td></td><td></td></t<>		
		<u> </u>

Sollte der Bedarf bestehen, eine weitere Quarantäne anzulegen, können Sie diese im Bereich *Basis-Konfiguration > Ordner > Quarantänen* anlegen.

Beachten Sie jedoch, dass die bereits vordefinierten Quarantänen den einzelnen Jobs zugeteilt wurden und dass hier eventuell weitere Änderungen erforderlich sind.



Um Ihre neu angelegte Quarantäne zu verwenden, muss diese in den gewünschten Jobs, im Reiter "Aktionen", hinterlegt werden.

# 7. Quarantänesammelbenachrichtigungen

Die Sammelbenachrichtigung gibt den Empfänger oder Gruppen eine Meldung über die Emails, welche in die Quarantäne gestellt worden sind. Alle benötigten Zusatzinformationen einer Meldung können über die Sammelbenachrichtigung konfiguriert werden.

Um die Funktion der Sammelbenachrichtigung zu nutzen, gehen Sie wie folgt vor.

 Schalten Sie zunächst den Quarantänezugriff frei: Basiskonfiguration > Avira Server > Doppelklick auf "Servername" > Quarantänenzugriff > Quarantänenzugriff per HTTP-Anfrage ermöglichen



 Wechseln Sie danach bitte wieder zu: Basiskonfiguration > Ordner > Quarantänen. Dort öffnen Sie die Eigenschaften der gewünschten Quarantäne mit einem Doppelklick. Im Reiter "Sammelbenachrichtigung" klicken Sie bitte auf Hinzufügen.



genschaften von An	tispam: Mittel	×
Allgemeines Sammell	benachrichtigungen Jobs Details	
Verwendete Quaran	täne-Sammelbenachrichtigungen:	
Name	Aktiv	
Empfängerbena 🐘	achrichtigung "Mittel" Nein	
<u>B</u> earbeiten I	Hinzufügen <u>E</u> ntfernen	
	<u>\</u>	
3	<u>O</u> K <u>A</u> bbrechen <u>Ü</u> b	ernehmen

In den Eigenschaften der Sammelbenachrichtigung können Sie zunächst festlegen, wer diese Benachrichtigung erhalten soll. Zusätzlich legen Sie hier einen Namen und die Inhalte fest.

enschaften von	Neue Quarantäne-Sammelbenachrichtigung		
Name:	Neue Quarantäne-Sammelbenachrichtigung		
Aktiv:	⊙ <u>J</u> a ⊂ <u>N</u> ein		
<u>V</u> orlage:	Quarantäne-Sammelbenachrichtigung 💌 😭		
Inhalte:	C Alle E <u>m</u> ails C Ne <u>u</u> e Emails		
	C Emails älter als 14 Tage		
Optionen:	<u>B</u> earbeitung:		
	nicht durch Avira Jobs bearbeiten		
2	OK Abbrechen Übernehme		

Im Reiter "Felder" legen Sie fest, welche Möglichkeiten der Empfänger haben soll.



### Hinweis:

Da der Quarantänezugriff zuvor auf HTTP eingestellt wurde, ist auch hier nur der HTTP-Zugriff möglich. Soll hier der Email-Zugriff verwendet werden, muss dies auch im Quarantänezugriff freigeschaltet werden.



Nachdem Sie die möglichen Aktionen festgelegt haben, fehlt zum Schluss nur noch der Zeitplan, nach welchem die Sammelbenachrichtigungen versendet werden.

Die Punkte "Zu White- / Blacklist hinzufügen", im Reiter "Felder" beziehen sich übrigens auf separate Adresslisten. Hier sind nicht die Listen im Bereich *Basis-Konfiguration > Allgemeine Einstellungen >Adresslisten* gemeint.

# 8. Update-Einstellungen

Die Einstellungen für das Update kann ab der Version 8 in der Oberfläche von Avira Exchange Security vorgenommen werden. Navigieren Sie nach *Basis-Konfiguration* > *Utility-Einstellungen*. Rufen Sie dort die Eigenschaften von "Avira Scan Engine" (Virensignaturen) bzw. von "Avira Spam Engine" (AntiSpam Signaturen) auf. Im Reiter "Update" ist der Punkt "Vordefinierte Werte für Update verwenden" ausgewählt. Dies bezeichnet die Avira Updateserver im Internet.



ualisiere Program ifigurationseinste	imdaten unter Vi Illungen:	erwendung folgende	er	
gemeine Einstel	lungen			
tervall:	60	Minuten		
eitüberschreitun	a: 600	Sekunden		
Administrator I	, bei erfolgreichen	Updates benachric	htigen	
'eitere Einstellun	gen			
Keine Update	durchführen			
Vordefinierte	Werte für Update	e verwenden		
C Update mit folgenden Einstellungen durchführen:				
C Lokales Update von (ohne Proxyserver):				
C Downloadserver (mit Proxyeinstellungen):				

Die relevanten Logdateien finden Sie unter folgenden Verzeichnissen:

### • Avira Spam Engine:

*C*:\*Programme* (x86)\*Avira*\*Avira* Exchange Security\*Bin*\*SPACE*\*Update*\*avupdate*. *log* 

### • Avira Scan Engine:

*C:\Programme (x86)\Avira\Avira Exchange Security\Bin\Savapi\Update\avupdate. log* 

## 8.1 Update via Proxy Server

Ebenfalls neu in der Version 8 ist die Möglichkeit, bei Bedarf einen Proxy über die Oberfläche von "Avira Exchange Security" konfigurieren zu können.

Die notwendige Konfiguration kann bzw. muss an verschiedenen Stellen vorgenommen werden.

Zuerst muss ein oder mehrere Proxy Server angeben werden. Navigieren Sie unter *Basis-Konfiguration > Allgemeine Einstellungen > Proxyserver* und erstellen einen neuen Eintrag.





Geben Sie in den Eigenschaften einen DNS-Namen bzw. IP-Adresse sowie Port und ggf. Benutzer und Passwort an.

Diesen Server geben Sie bitte unter *Basis-Konfiguration > Avira Server* in den Eigenschaften von ihrem Server an.



Somit haben Sie einen globalen Proxy Server definiert.



Damit ist dieser Proxy Server in den folgenden Modulen standardmäßig hinterlegt:

- Avira Scan Engine
- Avira Spam Engine

Diese Module finden Sie unter *Basis-Konfiguration* > *Utility-Einstellungen*.

Rufen Sie die Eigenschaften des jeweiligen Moduls auf und prüfen, ob dort die Einstellung "Proxyserver des Avira Servers" verwendet wird.

🞗 Avira Exchange Security		
Datei Aktion Ansicht ?		
🗢 🔿   🚈   X 🗐 🧟 🐟   🛽		
<ul> <li>Avira Exchange Security (*)</li> <li>Basis-Konfiguration</li> <li>Aligemeine Einstellungen</li> </ul>	Name     Avira Scan Engine	Aktiv Ja
Avira Server     Grdner     Grdner     Quarantänen     Gr Utilty-Einstellungen     Wortlisten     Wortlisten     Avira Scan Engine     Avira Spam Engine	Eigenschaften von Avira Scan Engine          Allgemeines       Returncodes       Update       Proxyserver       Jobs       Details         Proxyserver       auswählen:         ©       Keinen Proxyserver	×
	Eroxyserver des Avira Servers     Eenutzerdefinierten Proxyserver     Proxyserver augwähl Neuer Proxyserver	
E Server E Server1 E C Quarantänen		

#### Hinweis:

Sie haben die Möglichkeit, mehrere Proxy Server einzurichten und bei jedem Modul einen separaten Server anzugeben.

Setzen Sie in dem Fall bei dem Punkt "Benutzerdefinierten Proxyserver" einen Haken und wählen den entsprechenden Server in der Liste aus.

# 9. Jobvorschläge

# 9.1 Zusatz im Betreff entfernen

In der Standardkonfiguration fügt Avira Exchange im Betreff jeder Email den Zusatz [Avira checked] ein. Um diesen Zusatz zu ändern bzw. zu deaktivieren, muss jeder aktive Job separat konfiguriert werden (*Richtlinien-Konfiguration > Mail-Transport-Jobs*). Rufen Sie die Eigenschaften jedes Jobs auf und prüfen im Reiter "Allgemeines", ob der Zusatz im Betreff aktiviert ist.

Nachfolgend anhand des Jobs "Prüfen mit der Avira Scan Engine" gezeigt:



# 9.2 Unerwünschte Dateianhänge blocken

Um bestimmte Dateianhänge zu blocken, bietet Avira Exchange unter "Jobvorlagen" einige vorkonfigurierte Jobs. Diese werden in der Spalte "Jobtyp" als "Avira Attachment Filtering" bezeichnet.

Sie können diese vordefinierten Jobs benutzen oder einen neuen Job erstellen. Dazu muss man einen neuen Job anlegen (oder einen vorhandenen konfigurieren) und entsprechende Kriterien hinzufügen. Die Klassifizierung anhand von Fingerprints ist die beste Methode um Anhänge in Mails zu erkennen.

Navigieren Sie unter *Richtlinien-Konfiguration > Mail-Transport-Jobs* und legen Sie dort einen neuen Job an, in dem Fall "Avira Attachment Filtering". Die Eigenschaften des Jobs werden geöffnet und im Reiter "Fingerprints" können sowohl Bedingungen als auch Ausnahmen definiert werden.



gemeines   Adri Option:	essen   Bedingungen Fingerprints   Aktionen   Entpacke komprimierte Anhänge Archive <u>w</u> ählen	Serv_
ingerprint Bedi Aktion w	ngungen: ird ausgeführt ihang folgender Fingerprint	*
gilt aber Keine	richt für folgenden Fingerprint Fingerprints ausgewählt	
		*

Hier können Fingerprints geblockt werden (auch eine ganze Fingerprint Gruppe, z.B. Images) Zusätzlich können für bestimmt Fingerprints Ausnahmen gesetzt werden (z.B. alle Bilddateien außer JPEG)

Fingerprints auswählen		×
Alle Fingerprints	Ausgewählte Fingerprints:	
Fingerprints         Source         Alle Fingerprints         Source         Source	▲       Suspicious Attachments         Hinzufügen       Entfernen         Ausnahme(n):          ●       Hinzufügen         Entfernen	
<u>к</u>	Abbrechen	

Möchten Sie, dass der Absender über blockierte Anhänge informiert wird, aktivieren Sie bitte im Reiter "Aktionen" den Haken bei "Sende Absender: Verbotener Inhalt gefunden".

Empfehlenswert ist es auch, dass der Administrator nicht jedes Mal eine Mail bekommt wenn ein Anhang blockiert wurde. Entfernen Sie ggf. den entsprechenden Haken.

# *CAVIRA*

# 9.3 Advanced Spamfiltering mit separaten Quarantänen

#### Hinweis:

Bitte beachten Sie, dass nachfolgender Jobvorschlag in Avira Exchange Security als Job integriert ("Advanced Spamfiltering") und standardmäßig aktiviert ist.

Mit dem Job "Advanced Spamfiltering" kann man Spam in drei Kategorien unterteilen. Navigieren Sie dafür in der Avira Exchange Konsole unter *Basis-Konfiguration* > *Ordner* > *Quarantänen*.

- Antispam: Niedrig
- Antispam: Mittel
- Antispam: Hoch



Für jede Kategorie kann man einen separaten Quarantäneordner auswählen und eingehende Mails können somit in verschiedene Quarantäneordner abgelegt werden.

Anschließend muss noch der Job "Prüfen auf Spam mit Avira Antispam" unter *Richtlinien-Konfiguration > Mail-Transport-Jobs* entsprechend konfiguriert werden. In den Eigenschaften des Jobs unter dem Reiter "Aktionen" werden nun für alle drei Kategorien die zuvor erstellten Quarantänen festgelegt.





Aligemeines	Adressen	Bedingungen	Aktionen	Server Deta	ils
Aktioner	n konfigurieren	-			
Spam-W	/ahrscheinlich	keit: Keine			Trust .
Zusat	z im Betreff:		2 201		
Spam-w	anrscheinlich	keit: Miearig (t	J29]	NC-44-	1
Y .					
Spam-W	/ahrscheinlich	keit: Mittel [30	69]		
		12 2 2 2 1	a 19 3.	<u>M</u> ittel	
Spam-W	/ahrscheinlich	keit: Hoch [70	)100]		_
	- E12 - 124 - E12 -			<u>H</u> och	
Erweiterte	Konfiguration:				
Definiti	ve Kriterien	Kombinie	erte Kriterien	1	
	be Spam-Erge	hnis in Evcha	nge SCL Fe	 Id	
jornion	be opani Eige	bais in Empil I	landar		
Colori					

Jetzt konfigurieren Sie jede Kategorie (in dem Beispiel **Hoch**) und wählen den entsprechenden Quarantäneordner aus:

och X						
Aktic	nen für hohe Spam-Wahrscheinlichkeit:					
St	andard:					
2	Kopiere in Quarantäne: <u>Antispam: Hoch</u> Mit Label: <u>Spamkategorie: Hoch ([VAR]spamvalue</u> [/VAR])					
	Lösche Email					
	Absender/Empfänger zu Benutzerliste hinzufügen					
	Füge Zusatz im Betreff hinzu: [Spam- Wahrscheinlichkeit=[VAR]spamvalue;[/VAR]] am Anfang					
	Sende Absender: Spam gefunden an Administrator					
	Sende Benachrichtigung an Alle Absender					
	Sende <u>Empfänger: Spam gefunden</u> an Alle Empfänger					
	V					
	Hinzufügen					
3	<u>QK</u> <u>Abbrechen</u> <u>Ü</u> bernehmen					

Wiederholen Sie diesen Vorgang für die Kategorie Mittel sowie Niedrig.

#### Jobvorschläge

# *CAVIRA*

# 9.4 Empfänger automatisch zur Whitelist hinzufügen

Empfänger können Sie automatisch bei Versand einer Mail, zur Whitelist hinzufügen:

- Legen Sie einen neuen Job unter "Mail-Transport-Jobs" an: "Avira Antispam Email Address Filtering"
- Klicken Sie auf den Reiter "Aktionen" und setzen den Haken \*nur\* bei "Absender/Empfänger zur Benutzerliste Whitelist" hinzufügen.
- Schieben Sie den Job in "Mail-Transport-Jobs" auf den ersten Platz (rechte Maustaste auf Avira Antispam Email Address Filtering > Alle Aufgaben > An den Anfang)



Nun muss jeder nachfolgende Anti-Spam-Job so konfiguriert werden, dass der Job ignoriert wird wenn ein Absender in der Whitelist steht.

- Rufen Sie die Eigenschaften des entsprechenden Jobs auf und klicken Sie auf den Reiter "Bedingungen".
- Fügen Sie eine neue Bedingung hinzu: "...der Absender \*nicht\* in der Benutzerliste ,Whitelist' des Empfängers existiert"



Eigenschaften von Prüfen mit der Avira Scan Engine	🕫 Erweiterte Bedingungen
Allgemeines Adressen Bedingungen Avira Scan Engine Aktionen	Auswahl der Bedingungen für Emails:
QK         Abbrechen         Übernehmen	QK Abbrechen

Nun werden alle Empfänger automatisch in die Whitelist hinzugefügt und in den Anti-Spam-Jobs ignoriert.

## 9.5 Passwortgeschützte Archive

Passwortgeschützte Archive werden standardmäßig von Avira Exchange geblockt. Seit der Version 8 gibt es jedoch einen neuen Job: "Avira Protected Attachment Detection". Da der Job nicht automatisch aktiv ist, muss dieser erst einmal eingerichtet werden.

Richten Sie unter "Mail-Transport-Jobs" den oben erwähnten Job ein und verschieben diesen an die erste Stelle.





Nun können Sie diesen Job nach Belieben unter dem Reiter "Aktionen" konfigurieren und festlegen, was passieren soll, wenn eine Mail mit einem Passwort geschützten Archiv als Anhang eingeht.

Speichern Sie abschließend die durchgeführten Änderungen um diese zu aktivieren.

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 Operations GmbH & Co. KG nicht gestattet.

#### Ausgabe Q2-2013

Hier verwendete 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.



## live free.

 $\ensuremath{\mathbb{C}}$  2013 Avira Operations GmbH & Co. KG. Alle Rechte vorbehalten. Irrtümer und technische Änderungen vorbehalten.

Avira Operations GmbH & Co. KG Kaplaneiweg 1 88069 Tettnang Germany Telefon: +49 7542-500 0 Telefax: +49 7542-500 3000 www.avira.de